AMS/IP

Studies in Advanced Mathematics

S.-T. Yau, Series Editor

An Introduction to the Theory of Local Zeta Functions

Jun-ichi Igusa

American Mathematical Society • International Press

Selected Titles in This Series

14 **Jun-ichi Igusa,** An Introduction to the Theory of Local Zeta Functions, 2000

13 **Vasilios Alexiades and George Siopsis, Editors,** Trends in Mathematical Physics, 1999

12 **Sheng Gong,** The Bieberbach Conjecture, 1999

11 **Shinichi Mochizuki,** Foundations of p-adic Teichmüller Theory, 1999

10 **Duong H. Phong, Luc Vinet, and Shing-Tung Yau, Editors,** Mirror Symmetry III, 1999

9 **Shing-Tung Yau, Editor,** Mirror Symmetry I, 1998

8 **Jürgen Jost, Wilfrid Kendall, Umberto Mosco, Michael Röckner, and Karl-Theodor Sturm,** New Directions in Dirichlet Forms, 1998

7 **D. A. Buell and J. T. Teitelbaum, Editors,** Computational Perspectives on Number Theory, 1998

6 **Harold Levine,** Partial Differential Equations, 1997

5 **Qi-keng Lu, Stephen S.-T. Yau, and Anatoly Libgober, Editors,** Singularities and Complex Geometry, 1997

4 **Vyjayanthi Chari and Ivan B. Penkov, Editors,** Modular Interfaces: Modular Lie Algebras, Quantum Groups, and Lie Superalgebras, 1997

3 **Xia-Xi Ding and Tai-Ping Liu, Editors,** Nonlinear Evolutionary Partial Differential Equations, 1997

2.2 **William H. Kazez, Editor,** Geometric Topology, 1997

2.1 **William H. Kazez, Editor,** Geometric Topology, 1997

1 **B. Greene and S.-T. Yau, Editors,** Mirror Symmetry II, 1997

An Introduction to the Theory of Local Zeta Functions

https://doi.org/10.1090/amsip/014

AMS/IP Studies in Advanced Mathematics

Volume 14

An Introduction to the Theory of Local Zeta Functions

Jun-ichi Igusa

American Mathematical Society · International Press

Shing-Tung Yau, Managing Editor

2000 *Mathematics Subject Classification.* Primary 11Sxx, 11S40, 11Mxx, 11Gxx, 14Gxx.

Library of Congress Cataloging-in-Publication Data

Igusa, Jun-ichi, 1924–
An introduction to the theory of local zeta functions / Jun-ichi Igusa.
p. cm. — (AMS/IP studies in advanced mathematics, ISSN 1089-3288 ; v. 14)
Includes bibliographical references and index.
ISBN 0-8218-2015-X (hard cover; alk. paper)
ISBN 978-0-8218-2907-3 (soft cover; alk. paper)
1. Functions, Zeta. I. Title. II. Series.
QA351 .I38 2000
515′.56–dc21 99-087031

---

10 9 8 7 6 5 4 3 2 1 12 11 10 09 08 07

Contents

INTRODUCTION

Local zeta functions are relatively new mathematical objects. The first general theorems were proved from 1968 to 1973. Since then, especially during the last fifteen years, remarkable results have been obtained, allowing one to call the accumulation a "theory." Nevertheless, there remain several challenging problems whose solution will make the theory much richer. The purpose of this book is to introduce the readers to this theory. The book is written in such a way that it should be appropriate for those who have mastered the "basic courses" taught in America for first year graduate students. Assuming the reader has this background, nearly all material will be explained with detailed definitions and proofs. There are, however, two exceptions. We shall use *Hironaka's desingularization theorem* and the *functional equations of Weil's zeta functions* over finite fields. We shall explain these theorems by examples so that the readers can accept them with some understanding. The references are given primarily to indicate our indebtedness to the authors and not for the readers to consult.

Since local zeta functions are new, we shall define them briefly with details given in the text. If k is a number field, any completion of k is called a local field. Every local field K carries a Haar measure, and the rate of measure change under the multiplication by a in $K^\times = K\backslash\{0\}$ defines its absolute value $|a|_K$; it is completed by $|0|_K = 0$. If now $X = K^n$ for some $n \geq 1$, f is a K-valued non-constant polynomial function on X, and Φ is in the Schwartz-Bruhat space $\mathcal{S}(x)$ of X, then

$$Z_\Phi(s) = \int_X |f(x)|_K^s \Phi(x)\ dx, \qquad \mathrm{Re}(s) > 0$$

is called a local zeta function. If Φ is the standard function on X, i.e., $\exp(-\pi^t xx)$ for $K = \mathbb{R}$, $\exp(-2\pi^t x\bar{x})$ for $K = \mathbb{C}$, and the characteristic function of O_K^n for a p-adic field K with O_K as its maximal compact subring, then we drop the subscript Φ. Furthermore, we normalize the Haar measure dx on X so that $Z(s)$ tends to 1 as $s \to 0$. The set of $\omega_s(\cdot) = |\cdot|_K^s$ for all s in $\mathbb{C}$ forms the identity component

of the group $\Omega(K^\times)$ of all continuous homomorphisms ω from $K^\times$ to $\mathbb{C}^\times$. By replacing ω_s by ω we get a more general local zeta function $Z_\Phi(\omega)$. In view of the fact that $|\omega(\cdot)| = \omega_{\sigma(\omega)}(\cdot)$ for a unique $\sigma(\omega)$ in $\mathbb{R}$ satisfying $\sigma(\omega_s) = \mathrm{Re}(s)$, we define the right-half plane in $\Omega(K^\times)$ by $\sigma(\omega) > 0$. Then *the first general theorems* are as follows: $Z_\Phi(\omega)$, which is clearly holomorphic on the right-half plane, has a meromorphic continuation to the whole $\Omega(K^\times)$. Furthermore, in the p-adic case, if πO_K denotes the ideal of nonunits of O_K, then $Z_\Phi(\omega)$ is a rational function of $t = \omega(\pi)$. These results were obtained jointly by I. N. Bernstein and S. I. Gel'fand, independently by M. F. Atiyah, then by a different method by Bernstein, and in the p-adic case, by the author.

We shall now explain the *motivation*. In the archimedean case where $K = \mathbb{R}$ or $\mathbb{C}$, the general theorem was proposed as a problem by I. M. Gel'fand in 1954 and was discussed for some well-selected $f(x)$ in the first volume on generalized functions by I. M. Gel'fand and G. E. Shilov. The solution of the problem implies the existence of fundamental solutions for constant-coefficient differential equations. It appears that this situation served as a motivation of the work by Atiyah, Bernstein, and S. I. Gel'fand. On the other hand, we started differently. In the middle 60's, A. Weil showed that Siegel's main theorem on quadratic forms is a Poisson formula. More precisely, if k_A denotes the adele group of k and ψ a nontrivial character of k_A/k, then in the special case where the base space is one dimensional and

$$F_\Phi^*(i^*) = \int_{k_A^n} \psi(i^* f(x))\Phi(x)dx,$$

in which i^* is in k_A, $f(x)$ is a nondegenerate quadratic form on k^n, Φ is in $\mathcal{S}(k_A^n)$, dx is the Haar measure on k_A^n normalized as $\mathrm{vol}(k_A^n/k^n) = 1$, and $F_\Phi(i)$ is the inverse Fourier transform of $F_\Phi^*(i^*)$, then the Poisson formula takes the form

$$\sum_{i \in k} F_\Phi(i) = \sum_{i^* \in k} F_\Phi^*(i^*).$$

There is a condition $n > 4$ for the convergence of the series. Following Weil, we call the RHS, the right-hand side, the Eisenstein-Siegel series, and the identity itself with a modified LHS, the Siegel formula. Later, J. G. M. Mars proved the Siegel formula for a certain cubic form. Toward the end of 60's, we proved the Siegel formula for the Pfaffian and determined all cases where the Siegel formula might hold. However the proof of the convergence of the Eisenstein-Siegel series in general became a serious difficulty. In order to overcome this obstacle, we introduced $Z_\Phi(\omega)$ over K as above and showed that the general theorems on $Z_\Phi(\omega)$ can effectively be used to examine the convergence problem. In fact, it was shown to be sufficient to estimate $Z(\omega)$ for almost all p-adic completions K of k.

These were some of the developments up to the middle 70's. Before we start an explanation of later activities, we mention that the general theorems were proved by using Hironaka's theorem except for the second proof by Bernstein. In that proof he used the following remarkable fact: If $k_\circ$ is any field of characteristic 0 and $f(x)$ is in $k_\circ[x_1, \ldots, x_n]\backslash\{0\}$, where $x_1, \ldots, x_n$ are variables, then there exists

a differential operator P with coefficients in $k_\circ[s, x_1, \dots, x_n]$, where s is another variable, such that

$$Pf(x)^{s+1} = b_f(s)f(x)^s$$

for a monic polynomial $b_f(s)$. The $b_f(s)$, which is reserved for the one with the smallest degree, is called *Bernstein's polynomial* of $f(x)$. In the archimedean case, the above fact immediately implies the general theorem. In fact if $b_f(s) = \prod(s+\lambda)$, then

$$\prod_\lambda \Gamma(s+\lambda)^{-1} \cdot Z_\Phi(s)$$

becomes a holomorphic function on the whole s-plane. The proof via Hironaka's theorem shows that the poles of $Z_\Phi(s)$ are negative rational numbers. On the other hand, M. Sato developed his theory of prehomogeneous vector spaces in the middle 60's. Suppose that G is a connected reductive algebraic subgroup of $\mathrm{GL}_n(\mathbb{C})$ acting transitively on the complement of an irreducible hypersurface $f^{-1}(0)$ in $\mathbb{C}^n$ with $f(x)$ necessarily homogeneous of degree say d. Then without losing generality we can normalize G and $f(x)$ so that ${}^tG = \bar{G} = G$, $f(x)$ is in $\mathbb{R}[x_1, \dots, x_n]$ and further

$$f(\partial/\partial x)f(x)^{s+1} = b(s)f(x)^s$$

for a monic polynomial $b(s)$ of degree d called *Sato's b-function.* By definition $b_f(s)$ is a factor of $b(s)$. Actually they are equal. It can be seen, e.g., as follows: If $b(s) = \prod(s+\lambda)$, then $Z(s)$ has the form

$$\int_{\mathbb{C}^n} |f(x)|_{\mathbb{C}}^s \exp(-2\pi^t x\bar{x})\, dx = (2\pi)^{-ds} \cdot \prod_\lambda \left(\frac{\Gamma(s+\lambda)}{\Gamma(\lambda)}\right)$$

for $\mathrm{Re}(s) > 0$. This with the above results implies $b(s) = b_f(s)$. It also gives in the prehomogeneous case another proof to a general theorem of M. Kashiwara stating that all λ's in $b_f(s) = \prod(s+\lambda)$ are positive rational numbers.

Now in the p-adic case, what we did after the middle 70's was to compute $Z(\omega)$, especially $Z(s)$, for those $f(x)$ which might give the Siegel formulas. In compiling a list of $Z(s)$, we gradually became interested in patterns appearing in the shape of $Z(s)$ as a rational function of $t = \omega_s(\pi) = q^{-s}$, where $q = \mathrm{card}(O_K/\pi O_K)$. We therefore started a systematic computation of $Z(s)$ for a larger class of $f(x)$, especially for those $f(x)$ which appeared in Sato's theory, hoping to find conjectures on $Z(s)$. It did not take too long to find the first conjecture stating that if $f(x)$ is a homogeneous polynomial in $k[x_1, \dots, x_n]\backslash k$, where k is a number field as before, then

$$\deg_t(Z(s)) = -\deg(f)$$

for almost all K. We might emphasize the fact that this conjecture was not suggested by any existing theory, but it came from explicit computations. At any rate the conjecture was investigated by D. Meuser and proved as stated by J. Denef in the late 80's. In a similar manner, the ever-increasing list of explicitly computed $Z(s)$ suggested a new type of functional equations satisfied by $Z(s)$. This conjecture also became a theorem by Meuser and Denef in the early 90's. More precisely, the

new functional equation was derived from the functional equations of Weil's zeta functions over finite fields proved by A. Grothendieck. We shall devote the last chapter to a detailed explanation of their work.

We shall explain some problems on the denominator and the numerator of $Z(s)$ as a rational function of t. It is known for a general $f(x)$ that except for a power of t and the allowance of cancellation, the denominator of $Z(s)$ is of the form $\prod(1-q^{-a}t^b)$ for some positive integers a, b. Now in all known examples $b_f(-a/b) = 0$, i.e., the real parts of the poles of $Z(s)$ are zeros of $b_f(s)$, and the order of each pole is at most equal to the order of the corresponding zero. What it says is that $b_f(s)$ for some hidden reason describes the poles of $Z(s)$ also in the p-adic case. This is extremely remarkable in view of the fact that $b_f(s)$ does not play any direct role in that case. At any rate the problem is to convert the above experimental fact into a theorem. In the two variable case, i.e., if $n = 2$, the problem was settled by F. Loeser. Also in the prehomogeneous case, it was settled jointly by T. Kimura, F. Sato, and X.-W. Zhu, except for the information on the orders of poles stated above. In the general case, a solution seems to require a new theory.

Again, in the case of $f(x)$ appearing in Sato's theory, hence $d = \deg(f) = \deg(b_f)$, if $b > 1$ in some factors $1 - q^{-a}t^b$ of the denominator of $Z(s)$, then Denef's theorem suggests that $Z(s)$ might have a nonconstant numerator. By going through the list of $Z(s)$, we notice that certain cubic polynomials in t of the same type appear rather mysteriously in the numerators of $Z(s)$ for those $f(x)$ which do not have any apparent similarity. No hint to solve this mystery can be found in the complex case by the uniform simplicity of $Z(s)$ mentioned above, and a similarly explicit and general form of $Z(s)$ is not known in the real case. At any rate, no conjecture of any kind has been proposed on how to describe the numerator of $Z(s)$. We might finally make it clear that there are several important results, especially those by J. Denef, which we did not mention in this book. The reader can find most of them in Denef's Bourbaki seminar talk [11] and our expository paper [31].

The author would like to thank Professor S.-T. Yau for kindly inviting him to publish this book in the AMS-IP series. The author would also like to thank Professor M. M. Robinson for her effort to bring the manuscript into this final form. Finally, the author would like to gratefully acknowledge the invaluable assistance by his wife, Yoshie, for providing ideal working conditions for the last fifty years.

https://doi.org/10.1090/amsip/014/01

Chapter 1

Preliminaries

1.1 Review of some basic theorems

We shall assume that the reader is familiar with definitions and basic theorems on groups, rings, vector spaces, and modules in algebra. We shall review two theorems, among others, which we shall use later.

We shall assume, unless otherwise stated, that all rings are associative. If A is any ring with the unit element $1 \neq 0$, then we shall denote by $A^\times$ the group of units of A. If $\mathrm{M}_n(A)$ is the ring of $n \times n$ matrices with entries in A, then $\mathrm{M}_n(A)^\times$ will be denoted by $\mathrm{GL}_n(A)$. Suppose that A is commutative. Then an element a of A is called a zero divisor if $ab = 0$ for some $b \neq 0$ in A. If A has no zero divisor other than 0, then it is called an integral domain; and an element $a \neq 0$ of A is called irreducible if a is not in $A^\times$ and if $a = bc$ for b, c in A implies that either b or c is in $A^\times$. An integral domain is called a unique factorization ring if every $a \neq 0$ in A can be expressed uniquely, up to a permutation and elements of $A^\times$, as a product of irreducible elements. The classical examples are the ring $\mathbb{Z}$ of integers and the ring $F[x]$ of polynomials in one variable x with coefficients in a field F. In general, we have the following consequence of *Gauss' lemma*:

If A is a unique factorization ring and x is a variable, then $A[x]$ is also a unique factorization ring.

We might give some explanation. If we denote by F the quotient field of A, then every $f(x) \neq 0$ in $F[x]$ can be written as $f(x) = cf_\circ(x)$ with c in $F^\times$ and $f_\circ(x) \neq 0$ in $A[x]$ such that its coefficients are relatively prime. We call such an $f_\circ(x)$ primitive. According to the Gauss lemma, the product of primitive polynomials is primitive. Therefore if $f(x)$, $g(x)$ are primitive and $f(x) = g(x)h(x)$ with $h(x)$ in $F[x]$, then necessarily $h(x)$ is in $A[x]$ and primitive. This implies the above statement. The irreducible elements of $A[x]$ are irreducible elements of A and primitive polynomials which are irreducible in $F[x]$. At any rate, as a corollary we see that $F[x_1, \ldots, x_n]$, where $x_1, \ldots, x_n$ are variables, is a unique factorization ring.

We shall also use the following fact, which is sometimes called the "Principle of the irrelevance of algebraic inequalities":

Let F denote an infinite field and $f(x), g_1(x), \ldots, g_t(x)$ elements of the polynomial ring $F[x] = F[x_1, \ldots, x_n]$, in which $g_1(x) \neq 0, \ldots, g_t(x) \neq 0$. Suppose that $f(a) = 0$ for every $a = (a_1, \ldots, a_n)$ in F^n satisfying $g_1(a) \neq 0, \ldots, g_t(a) \neq 0$. Then $f(x) = 0$.

The proof is as follows. If we put $h(x) = f(x)g_1(x)\dots g_t(x)$, then by assumption, $h(a) = 0$ for every a in F^n. If we can show that this implies $h(x) = 0$, since $F[x]$ is an integral domain and $g_1(x) \neq 0, \dots, g_t(x) \neq 0$, we will have $f(x) = 0$. Suppose that $h(x) \neq 0$. Suppose further that $n = 1$. Then the number of zeros of $h(x)$ in F is at most equal to $\deg(h)$. Since F is an infinite field, we have a contradiction. We shall therefore assume that $n > 1$ and apply an induction on n. If we write

$$h(x) = c_0(x') + c_1(x')x_n + \dots$$

with $c_0(x')$, $c_1(x')$, ... in $F[x_1, \dots, x_{n-1}]$, then $c_i(x') \neq 0$ for some i by $h(x) \neq 0$. By induction, we can find $a' = (a_1, \dots, a_{n-1})$ in F^{n-1} satisfying $c_i(a') \neq 0$. Then $h(a', x_n) \neq 0$, hence $h(a', a_n) \neq 0$ for some a_n in F. We thus have a contradiction.

We shall assume that the reader is familiar with topological spaces, their compactness, continuous maps, etc., in general topology. We shall review some definitions and theorems.

A topological space is a nonempty set X equipped with a family of its subsets, called open, with the property that the family is closed under the taking of arbitrary union and finite intersection. The family then contains X and the empty set $\emptyset$. If Y is any nonempty subset of X, then Y will be considered as a topological space by the induced topology. The family of open sets in Y consists of intersections of Y and open sets in X. Complements of open sets are called closed. If A is any subset of X, the intersection $\overline{A}$ of all closed sets containing A is called the closure of A; it is the smallest closed set containing A. An open set containing a point is called its neighborhood. A topological space is called a Hausdorff space if any two distinct points have disjoint neighborhoods. A Hausdorff space X with the following property is called compact: If X is the union of open sets in a family I, then X is also the union of open sets in a suitable finite subfamily of I. Every nonempty closed set in a compact space is compact. The *Tychonoff theorem* states that the product space, i.e., the product set with the product topology, of any nonempty set of compact spaces is compact. A Hausdorff space is called locally compact if every point has a neighborhood with compact closure. The fields $\mathbb{R}$ and $\mathbb{C}$ of real and complex numbers with the usual topology are locally compact. A Hausdorff space is called normal if any two disjoint closed sets are contained in disjoint open sets. Every compact space is normal. If φ is an $\mathbb{R}$-valued function on any nonempty set X satisfying $\varphi(x) \geq \alpha$ for some α in $\mathbb{R}$ and for every x in X, we shall write $\varphi \geq \alpha$ and also $\alpha \leq \varphi$. If A, B are disjoint nonempty closed sets in a normal space X, there exists an $\mathbb{R}$-valued continuous function φ on X satisfying $0 \leq \varphi \leq 1$ such that $\varphi = 0$ on A, i.e., $\varphi(x) = 0$ for every x in A, and $\varphi = 1$ on B. This remarkable theorem is called *Urysohn's lemma*. We shall later use the following fact:

A Hausdorff space X is locally compact if and only if for every neighborhood U of any point a of X there exist an $\mathbb{R}$-valued continuous function φ on X satisfying $0 \leq \varphi \leq 1$ and a compact subset C of U containing a such that $\varphi = 0$ on $X \backslash C$ and $\varphi(a) = 1$.

We shall outline the proof. The if-part is clear. In fact, if O_φ denotes the set of all x in X where $\varphi(x) > 0$, then O_φ is a neighborhood of a with its closure contained in C, hence it is compact. Conversely, suppose that X is locally compact. Then

a has a neighborhood $U_\circ$ with compact closure. By replacing U by its intersection with $U_\circ$, we may assume that $\bar{U}$ is compact, hence normal. We choose disjoint open subsets V and W of $\bar{U}$ respectively containing a and $\bar{U}\backslash U$. Then V is open in U, hence also in X. By Urysohn's lemma there exists an $\mathbb{R}$-valued continuous function φ on $\bar{U}$ satisfying $0 \leq \varphi \leq 1$ such that $\varphi = 0$ on $\bar{U}\backslash V$ and $\varphi(a) = 1$. If we extend φ to X as $\varphi = 0$ on $X\backslash V$, then φ will have the required property with $\bar{V}$ as C.

We shall assume that the reader is familiar with routine theorems in complex analysis. We shall review a few basic facts, just to refresh reader's memory. If

$$P(z) = \sum_{n \geq 0} c_n (z-a)^n$$

is a power series with center a and coefficients $c_0, c_1, \ldots$ all in $\mathbb{C}$, then there exists $0 \leq r \leq \infty$, called the radius of convergence, such that $P(z)$ is convergent (resp. divergent) for every z in $\mathbb{C}$ satisfying $|z-a| < r$ (resp. $|z-a| > r$). Furthermore r is given by

$$r = \frac{1}{\limsup_{n\to\infty} |c_n|^{\frac{1}{n}}},$$

which is often called Cauchy-Hadamard's formula. As a consequence, if we define a power series $Q(z)$ by a termwise differentiation of $P(z)$ as

$$Q(z) = \sum_{n>0} n c_n (z-a)^{n-1},$$

then $Q(z)$ has the same radius of convergence as $P(z)$. Furthermore, the $\mathbb{C}$-valued function P on the disc $|z-a| < r$ defined by $P(z)$ is differentiable at every point of the disc and its derivative P' is given by the function Q defined by $Q(z)$. If D is any nonempty open subset of $\mathbb{C}$ and a is a point of D, we put $\partial D = \bar{D}\backslash D$ and denote by $\mathrm{dis}(a, \partial D)$ the distance from a to ∂D. We have $0 < \mathrm{dis}(a, \partial D) \leq \infty$. Suppose now that f is a $\mathbb{C}$-valued function on D with the following property: At every point a of D there exists a power series $P(z)$ with a radius of convergence $r > 0$ such that $f(z) = P(z)$ for every z in D satisfying $|z-a| < r$. Then we say that f is holomorphic on D. The above remark on P and Q shows that if f is holomorphic on D, then its derivative f' exists and is holomorphic on D. We call $P(z)$ the Taylor expansion of $f(z)$ at a. A standard criterion for f to be holomorphic on D is that f is differentiable at every point of D. In fact "Cauchy's theorem" holds for such an f, hence $f(z)$ can be expressed by "Cauchy's integral formula," and hence it can be expanded into a Taylor series. This line of argument implies that the above r satisfies $r \geq \mathrm{dis}(a, \partial D)$, and this fact supplies a basis for the holomorphic continuation of f. At any rate, the above criterion implies the following criterion, sometimes called *Morera's theorem*:

Let f denote a $\mathbb{C}$-valued continuous function on D such that its integral along any closed curve of finite length in D is 0. *Then f is holomorphic on D.*

In the application D usually has the property that it is connected and simply connected. Then Morera's theorem becomes the converse of Cauchy's theorem mentioned above. At any rate the proof is straightforward. We may assume that D

is connected. Choose a and z from D and join them by a curve C of finite length in D. Then, by assumption, the integral of f along C is independent of the choice of C, hence we may denote it by $F(z)$. In this way we get a well-defined function F on D with f as its derivative. Therefore F, hence also f, is holomorphic on D.

If a is a point of D and the function of z defined by $(z-a)^k f(z)$ becomes holomorphic on D for some $k > 0$, then a is called a pole of f. In such a case, $f(z)$ can be expanded into a Laurent series at a, which is similar to $P(z)$ above but with finitely many terms $c_n(z-a)^n$ for $n < 0$. Furthermore, the above mentioned Cauchy's integral formula implies that

$$c_n = \left(\frac{1}{2\pi i}\right) \int_{|z-a|=r_\circ} \frac{f(z)}{(z-a)^{n+1}}\ dz$$

for every n, in which $0 < r_\circ < \mathrm{dis}(a, \partial D)$ and the integral is from $\theta = 0$ to 2π after writing $z - a = r_\circ \exp(i\theta)$. We shall use meromorphic functions, meromorphic continuation, etc. later on.

We shall finally review two theorems in calculus and one theorem in analysis. The first one is called *Gauss' theorem*, and it is as follows:

Suppose that D is a bounded open subset of $\mathbb{R}^3$ such that $\partial D = \bar{D} \backslash D$ is piecewise smooth; let $f_1(x)$, $f_2(x)$, $f_3(x)$ denote continuously differentiable functions on $\bar{D}$. Then

$$\int_{\partial D} (f_1(x)dx_2dx_3 + f_2(x)dx_3dx_1 + f_3(x)dx_1dx_2) = \int_D (\frac{\partial f_1}{\partial x_1} + \frac{\partial f_2}{\partial x_2} + \frac{\partial f_3}{\partial x_3})\ dx_1dx_2dx_3.$$

Since D is assumed to be piecewise smooth, it has a "surface element" $d\sigma$. If $n = (n_1, n_2, n_3)$ denotes the outer normal unit vector at a smooth point of D and $f \cdot n = f_1n_1 + f_2n_2 + f_3n_3$, then the integrand on the LHS can be replaced by $(f \cdot n)\ d\sigma$. The second one is called *Fubini's theorem*, and it is as follows:

Suppose that $-\infty \leq a < b \leq \infty$, $-\infty \leq c < d \leq \infty$ and D consists of (x, y) satisfying $a < x < b$, $c < y < d$; let $f(x, y)$ denote a continuous function on D which is absolutely integrable on D, i.e., the integral of $|f(x, y)|$ over D is finite. Then

$$\int_D f(x,y)dxdy = \int_a^b \left(\int_c^d f(x,y)dy\right)dx = \int_c^d \left(\int_a^b f(x,y)dx\right)dy.$$

The third one is called *Lebesgue's theorem*, and it is as follows:

Suppose that D is defined by $a < x < b$ and $\{f_i(x)\}_i$ is a sequence of continuous functions on D which converges to a continuous function on D; suppose further that there exists an absolutely integrable function $\phi(x)$ on D satisfying $|f_i(x)| \leq \phi(x)$ for all i and all x in D. Then

$$\lim_{i\to\infty} \int_D f_i(x)\ dx = \int_D (\lim_{i\to\infty} f_i(x))\ dx.$$

We have formulated the above theorems rather restrictively so that the integrals become those familiar in calculus. Actually, the third theorem is proved in analysis

for a convergent sequence of Lebesgue integrable functions. In our later applications we more or less keep the restrictions on functions, but the domains of integration will become multidimensional. We shall use Lebesgue's theorem to shorten the proof, i.e., to avoid longer and artificial argument.

1.2 Noetherian rings

We shall summarize basic theorems on noetherian rings. Although some of them may be included in the first course on algebra, we shall give outlines of standard proofs to all of them.

A *noetherian ring* A is a commutative ring with the unit element 1 in which every ideal has a finite ideal basis. Equivalently, every strictly increasing sequence of ideals is finite. In the following, we shall explicitly state it if this condition is used. If $\mathfrak{a}$, $\mathfrak{b}$ are ideals of A, then $\mathfrak{ab}$ denotes the set of finite sums of ab for all a in $\mathfrak{a}$ and b in $\mathfrak{b}$; by definition $\mathfrak{ab}$ is an ideal of A. If $\mathfrak{a}$ is an ideal of A, then its root $r(\mathfrak{a})$ consists of all a in A such that its image in the factor ring $A/\mathfrak{a}$ is nilpotent, i.e., a^e is in $\mathfrak{a}$ for some positive integer e depending on a. We see that $r(\mathfrak{a})$ is an ideal of A, $r(r(\mathfrak{a})) = r(\mathfrak{a})$, and the operation "$r$" is monotone, i.e., preserves the inclusion relation, and commutes with the taking of finite intersection. Furthermore, if A is a noetherian ring, hence $r(\mathfrak{a})$ has a finite ideal basis, a suitable power $r(\mathfrak{a})^e$ of $r(\mathfrak{a})$ is contained in $\mathfrak{a}$. We say that an ideal $\mathfrak{p}$ of A is prime if $A/\mathfrak{p}$ is an integral domain, i.e., if $\mathfrak{p} \neq A$ and ab in $\mathfrak{p}$, a not in $\mathfrak{p}$ imply b in $\mathfrak{p}$. We say that an ideal $\mathfrak{q}$ of A is primary if $A/\mathfrak{q} \neq 0$ and every zero divisor of $A/\mathfrak{q}$ is nilpotent, i.e., if $\mathfrak{q} \neq A$ and ab in $\mathfrak{q}$, a not in $\mathfrak{q}$ imply b in $r(\mathfrak{q})$. In that case, we see that $r(\mathfrak{q})$ is a prime ideal. Clearly every prime ideal is a primary ideal. If $\mathfrak{a}$ is an ideal of A and E is a subset of A, then we denote by $\mathfrak{a} : E$ the set of all a in A such that ab is in $\mathfrak{a}$ for all b in E. We observe that $\mathfrak{a} : E$ is an ideal of A. Furthermore, the operation "$\cdot : E$" clearly commutes with the taking of finite intersection. We shall often use the following fact: namely, if an ideal $\mathfrak{a}$ is not contained in $r(\mathfrak{q})$ for a primary ideal $\mathfrak{q}$, i.e., $r(\mathfrak{a})$ is not contained in $r(\mathfrak{q})$, then $\mathfrak{q} : \mathfrak{a} = \mathfrak{q}$.

Lemma 1.2.1 *Let $\mathfrak{a}$ denote an ideal of a noetherian ring A which is different from A and meet-irreducible in the sense that it cannot be expressed as an intersection of two ideals of A both strictly containing $\mathfrak{a}$. Then $\mathfrak{a}$ is a primary ideal.*

Proof. We shall assume that $\mathfrak{a}$ is not primary and derive a contradiction. Since $\mathfrak{a} \neq A$ is already assumed, we will have the situation that ab in $\mathfrak{a}$, a not in $\mathfrak{a}$, and b not in $r(\mathfrak{a})$. Since the sequence $\mathfrak{a} : b$, $\mathfrak{a} : b^2, \ldots$ is increasing, we will have $\mathfrak{a} : b^k = \mathfrak{a} : b^{k+1}$ for some positive integer k. Then both $\mathfrak{a}_1 = Ab^k + \mathfrak{a}$ and $\mathfrak{a}_2 = Aa + \mathfrak{a}$ strictly contain $\mathfrak{a}$. If x is in $\mathfrak{a}_1$, then $x = cb^k + d$ for some c in A and d in $\mathfrak{a}$. If x is also in $\mathfrak{a}_2$, since ab is in $\mathfrak{a}$, we see that bx is in $\mathfrak{a}$. Then c is in $\mathfrak{a} : b^{k+1} = \mathfrak{a} : b^k$, hence x is in $\mathfrak{a}$. Therefore $\mathfrak{a}$ is the intersection of $\mathfrak{a}_1$ and $\mathfrak{a}_2$, hence $\mathfrak{a}$ is not meet-irreducible.

In a noetherian ring A every ideal $\mathfrak{a}$ can be expressed as an intersection of a finite number of meet-irreducible ideals. Otherwise, starting from $\mathfrak{a}$ we can construct an infinite sequence of strictly increasing ideals in A. On the other hand if $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$ are primary ideals of A satisfying $r(\mathfrak{q}_i) = \mathfrak{p}$ for all i and $t > 0$, then their intersection $\mathfrak{q}$ is

a primary ideal and $r(\mathfrak{q}) = \mathfrak{p}$. Therefore, by Lemma 1 every ideal $\mathfrak{a}$ can be expressed as an intersection of primary ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$ with distinct $r(\mathfrak{q}_1), \ldots, r(\mathfrak{q}_t)$. If no $\mathfrak{q}_i$ is redundant, then for the sake of simplicity we call such an expression a *minimal representation* of $\mathfrak{a}$. We shall only use the following uniqueness theorem:

Theorem 1.2.1 *If $\mathfrak{a}$ is an ideal of a noetherian ring A and*

$$\mathfrak{a} = \bigcap_{1 \le i \le t} \mathfrak{q}_i$$

is a minimal representation of $\mathfrak{a}$, then the set $\{r(\mathfrak{q}_1), \ldots, r(\mathfrak{q}_t)\}$ is uniquely determined by $\mathfrak{a}$.

Proof. If $t = 0$, i.e., $\mathfrak{a} = A$, then the theorem holds trivially. Suppose that $\mathfrak{a}$ has another minimal representation as an intersection of primary ideals $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_s$ and assume by induction that $\min(s, t) > 0$. Since the situation is symmetric, we may assume that $\mathfrak{p} = r(\mathfrak{q}_t)$ is maximal among $r(\mathfrak{q}_i), r(\mathfrak{q}'_j)$ for all i, j. Then $\mathfrak{p}$ is among $r(\mathfrak{q}'_1), \ldots, r(\mathfrak{q}'_s)$. Otherwise we will have

$$\mathfrak{a} : \mathfrak{q}_t = \bigcap_{1 \le i < t} \mathfrak{q}_i = \bigcap_{1 \le j \le s} \mathfrak{q}'_j = \mathfrak{a},$$

hence $\mathfrak{q}_t$ is redundant. This is a contradiction. Therefore we may assume that $r(\mathfrak{q}'_s) = \mathfrak{p}$. Then we get

$$\mathfrak{a} : \mathfrak{q}_t\mathfrak{q}'_s = \bigcap_{1 \le i < t} \mathfrak{q}_i = \bigcap_{1 \le j < s} \mathfrak{q}'_j$$

We observe that they are minimal representations of the LHS. Therefore, by induction the two sets $\{r(\mathfrak{q}_1), \ldots, r(\mathfrak{q}_{t-1})\}$ and $\{r(\mathfrak{q}'_1), \ldots, r(\mathfrak{q}'_{s-1})\}$ are the same.

We shall use the operation S^{-1} by a *multiplicative subset* S of A, i.e., a multiplicatively closed subset containing 1, but only in the case where S is free from zero divisors. In that case, $S^{-1}A$ simply consists of a/s for all a in A and s in S with the convention that $a/s = a'/s'$ if and only if $s'a = sa'$. We convert $S^{-1}A$ into a ring as in the special case where $A = \mathbb{Z}$ and S is the set of positive integers. Then $S^{-1}A$ becomes a commutative ring with $1/1$ as its unit element and A can be identified with its subring under the correspondence $a \mapsto a/1$. If $\mathfrak{a}$ is an ideal of A, then $S^{-1}\mathfrak{a}$ is defined as the set of a/s for all a in $\mathfrak{a}$ and s in S. Then $S^{-1}\mathfrak{a}$ becomes an ideal of $S^{-1}A$. We observe that the operation $\mathfrak{a} \mapsto S^{-1}\mathfrak{a}$ is monotone and commutes with the taking of finite intersection. Furthermore, if $\mathfrak{a}^*$ is an ideal of $S^{-1}A$, then $A \cap \mathfrak{a}^*$ is an ideal of A and $\mathfrak{a}^* = S^{-1}(A \cap \mathfrak{a}^*)$ because $a/s = (1/s)(a/1)$ for every a/s in $\mathfrak{a}^*$ with $a = a/1$ in $A \cap \mathfrak{a}^*$. Therefore if $\mathfrak{a}^*_1, \mathfrak{a}^*_2, \ldots$ form a strictly increasing sequence of ideals of $S^{-1}A$, then $A \cap \mathfrak{a}^*_1, A \cap \mathfrak{a}^*_2, \ldots$ form a strictly increasing sequence of ideals of A. This implies that $S^{-1}A$ is noetherian if A is noetherian.

Lemma 1.2.2 *Let $\mathfrak{q}$ denote a primary ideal of A. If $\mathfrak{q}$ and S are disjoint, then $S^{-1}\mathfrak{q}$ is a primary ideal of $S^{-1}A$, $r(S^{-1}\mathfrak{q}) = S^{-1}r(\mathfrak{q})$, and $A \cap S^{-1}\mathfrak{q} = \mathfrak{q}$. If $\mathfrak{q}$ and S intersect, then $S^{-1}\mathfrak{q} = S^{-1}A$.*

Proof. Since the second part is clear, we shall only prove the first part. If $\mathfrak{q}$ and S are disjoint, then clearly $S^{-1}\mathfrak{q} \neq S^{-1}A$ and $A \cap S^{-1}\mathfrak{q} = \mathfrak{q}$ because $r(\mathfrak{q})$ and S are also disjoint. Furthermore, if a/s for a in A and s in S is in $S^{-1}\mathfrak{q}$, then a is in $\mathfrak{q}$. In fact, if $a/s = a'/s'$ with a' in $\mathfrak{q}$ and s' in S, then $s'a = sa'$ is in $\mathfrak{q}$ and s' is not in $r(\mathfrak{q})$, hence a is in $\mathfrak{q}$. This implies $r(S^{-1}\mathfrak{q}) = S^{-1}r(\mathfrak{q})$. We shall show that $S^{-1}\mathfrak{q}$ is a primary ideal of $S^{-1}A$. If $(a/s)(a'/s')$ is in $S^{-1}\mathfrak{q}$ with a/s not in $S^{-1}\mathfrak{q}$, then aa' is in $\mathfrak{q}$ with a not in $\mathfrak{q}$, hence a'/s' is in $S^{-1}r(\mathfrak{q}) = r(S^{-1}\mathfrak{q})$.

Proposition 1.2.1 *In Theorem 1.2.1 suppose that $\mathfrak{q}_i$ and S are disjoint for $i \leq r$ but not for $i > r$. Then*

$$S^{-1}\mathfrak{a} = \bigcap_{1 \leq i \leq r} S^{-1}\mathfrak{q}_i$$

is a minimal representation of $S^{-1}\mathfrak{a}$ in $S^{-1}A$.

Proof. This follows immediately from Lemma 1.2.2 except for the fact that none of $S^{-1}\mathfrak{q}_1, \ldots, S^{-1}\mathfrak{q}_r$ is redundant. If we denote by $\mathfrak{a}'$ the intersection of $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$, then by Lemma 1.2.2 we get $A \cap S^{-1}\mathfrak{a}' = \mathfrak{a}'$. Therefore, if, e.g., $S^{-1}\mathfrak{q}_r$ is redundant, we will have

$$\mathfrak{a}' = A \cap S^{-1}\mathfrak{a}' = \bigcap_{1 \leq i < r} \mathfrak{q}_i,$$

hence $\mathfrak{q}_r$ becomes redundant in the minimal representation of $\mathfrak{a}$. This is a contradiction.

We say that an ideal $\mathfrak{m}$ of A is maximal if $\mathfrak{m}$ is maximal in the set of all ideals of A different from A. In that case, $Aa + \mathfrak{m} = A$ for every a in A not in $\mathfrak{m}$, hence $A/\mathfrak{m}$ is a field, and hence $\mathfrak{m}$ is a prime ideal. We say that A is a *local ring* if the set of all nonunits of A forms its maximal ideal. If $\mathfrak{p}$ is a prime ideal of A such that $S = A \backslash \mathfrak{p}$ is free from zero divisors, then Lemma 1.2.2 shows that $S^{-1}A$ is a local ring with $S^{-1}\mathfrak{p}$ as its maximal ideal. At any rate, if A is a local ring with $\mathfrak{m}$ as its maximal ideal, then every element of $1 + \mathfrak{m}$ is a unit of A.

Theorem 1.2.2 *Let $\mathfrak{m}$ denote an ideal of A with the property that every element of $1+\mathfrak{m}$ is a unit of A and M a finitely generated A-module, i.e., $M = Ax_1 + \ldots + Ax_n$ for some $x_1, \ldots, x_n$ in M, satisfying $\mathfrak{m}M = M$. Then $M = 0$. Furthermore, if A is a noetherian ring, then the intersection of all powers of $\mathfrak{m}$ is 0.*

Proof. We shall prove the first part. Suppose that $M \neq 0$ and express M as in the theorem with the smallest n necessarily positive. Then x_n is in $M = \mathfrak{m}M$, hence $x_n = a_1x_1 + \ldots + a_nx_n$ with a_i in $\mathfrak{m}$ for all i. This implies $(1 - a_n)x_n = a_1x_1 + \ldots + a_{n-1}x_{n-1}$. Since $1 - a_n$ is a unit of A by assumption, we see that x_n is in $Ax_1 + \ldots + Ax_{n-1}$, hence $M = Ax_1 + \ldots + Ax_{n-1}$. This contradicts the minimality of n.

We shall prove the second part. We denote the intersection of all powers of $\mathfrak{m}$ by $\mathfrak{n}$. Then $\mathfrak{n}$ is an ideal of A, hence a finitely generated A-module. By the first part we have only to show that $\mathfrak{m}\mathfrak{n} = \mathfrak{n}$. Since $\mathfrak{m}\mathfrak{n}$ is contained in $\mathfrak{n}$, we shall show that $\mathfrak{n}$ is contained in $\mathfrak{m}\mathfrak{n}$. Let

$$\mathfrak{m}\mathfrak{n} = \bigcap_{1 \leq i \leq t} \mathfrak{q}_i$$

denote a minimal representation of $\mathfrak{mn}$. Then $\mathfrak{mn}$ is contained in $\mathfrak{q}_i$, hence $\mathfrak{n}$ is contained in $\mathfrak{q}_i : \mathfrak{m}$ for all i. If $\mathfrak{m}$ is not contained in $r(\mathfrak{q}_i)$, then $\mathfrak{n}$ is contained in $\mathfrak{q}_i : \mathfrak{m} = \mathfrak{q}_i$. On the other hand if $\mathfrak{m}$ is contained in $r(\mathfrak{q}_i)$, then $\mathfrak{m}^e$ is contained in $\mathfrak{q}_i$ for some e, hence $\mathfrak{n}$ is contained in $\mathfrak{q}_i$. Therefore, $\mathfrak{n}$ is contained in all $\mathfrak{q}_i$, hence in $\mathfrak{mn}$.

The second part, i.e., the fact that the intersection of all powers of $\mathfrak{m}$ is 0, is due to W. Krull [36]. We might mention that the first part, i.e., the fact that $\mathfrak{m}M = M$ implies $M = 0$, is sometimes called Nakayama's lemma. It has the following useful corollary:

Corollary 1.2.1 *Let A denote a local ring with $\mathfrak{m}$ as its maximal ideal and M a finitely generated A-module; for every a, x respectively in A, M denote by $\bar{a}$, $\bar{x}$ their images in $A/\mathfrak{m}$, $M/\mathfrak{m}M$ and convert $M/\mathfrak{m}M$ into a vector space over $A/\mathfrak{m}$ as $\bar{a}\bar{x} = \overline{ax}$. Then $M = Ax_1 + \ldots + Ax_n$ if and only if $\bar{x}_1, \ldots, \bar{x}_n$ span $M/\mathfrak{m}M$ over $A/\mathfrak{m}$.*

Proof. Since the other part is clear, we shall prove the if-part. We observe that $M/\mathfrak{m}M = (A/\mathfrak{m})\bar{x}_1 + \ldots + (A/\mathfrak{m})\bar{x}_n$ can be rewritten as $M = (Ax_1 + \ldots + Ax_n) + \mathfrak{m}M$. If we put $N = M/(Ax_1 + \ldots + Ax_n)$, then N is a finitely generated A-module and $\mathfrak{m}N = N$, hence $N = 0$.

1.3 Hilbert's theorems

It is a well-known historical fact that D. Hilbert put a period to the classical theory of invariants by his monumental paper [19]. We shall explain three important theorems in that paper with proof. We shall start with the following lemma:

Lemma 1.3.1 . *Let A denote a noetherian ring, M a finitely generated A-module, and N any A-submodule of M. Then N is also finitely generated.*

Proof. If we express M as $M = Ax_1 + \ldots + Ax_n$, then the Lemma holds trivially for $n = 0$. Therefore we shall assume that $n > 0$ and apply an induction on n. If we denote by N' the intersection of N and $M' = Ax_1 + \ldots + Ax_{n-1}$, then N' is finitely generated by induction. If we denote by $\mathfrak{a} = (M' + N) : x_n$ the set of all a in A such that ax_n is in $M' + N$, then $\mathfrak{a}$ is an ideal of A. We choose a finite ideal basis $\{a_1, \ldots, a_t\}$ for $\mathfrak{a}$ and write $a_i x_n = x_i' + y_i$ with x_i' in M' and y_i in N for all i. If we put $N'' = Ay_1 + \ldots + Ay_t$, then we have only to show that $N = N' + N''$. Since $N' + N''$ is contained in N, we shall show that every element x of N is in $N' + N''$. If we write $x = x' + ax_n$ with x' in M' and a in A, then a is in $\mathfrak{a}$, hence $a = b_1 a_1 + \ldots + b_t a_t$ for some $b_1, \ldots, b_t$ in A. Then $x - (b_1 y_1 + \ldots + b_t y_t)$ is in N', hence x is in $N' + N''$.

Lemma 1.3.2 *If A is a noetherian ring and x is a variable, then the polynomial ring $A[x]$ is also a noetherian ring.*

Proof. We take any ideal $\mathfrak{A}$ of $A[x]$ and show that $\mathfrak{A}$ has a finite ideal basis. We shall exclude the trivial case where $\mathfrak{A} = 0$ and denote by $\mathfrak{a}$ the set of coefficients of

the highest powers of x which occur in elements of $\mathfrak{A}$. If ax^m, bx^n are the highest terms of elements of $\mathfrak{A}$ and $m \geq n$, then $x^{m-n} \cdot bx^n = bx^m$ is also the higest term of an element of $\mathfrak{A}$. Therefore if a, b are in $\mathfrak{a}$, then $a+b$ is in $\mathfrak{a}$ and ca for any c in A is clearly in $\mathfrak{a}$. This shows that $\mathfrak{a}$ is an ideal of A. We choose $g_1(x), \ldots, g_s(x)$ from $\mathfrak{A}$ such that the coefficients of the highest powers of x which occur in them form an ideal basis for $\mathfrak{a}$. By the same adjustment as above, we may assume that x^n for some $n > 0$ is the highest power of x which occurs in all of them. We denote by $\mathfrak{A}'$ the intersection of $\mathfrak{A}$ and $A + Ax + \ldots + Ax^{n-1}$ and put $\mathfrak{A}'' = A[x]g_1(x) + \ldots + A[x]g_s(x)$. We shall show that $\mathfrak{A} = \mathfrak{A}' + \mathfrak{A}''$. Since $\mathfrak{A}$ contains $\mathfrak{A}' + \mathfrak{A}''$, we have only to show that $\mathfrak{A}$ is contained in $\mathfrak{A}' + \mathfrak{A}''$. Take any $f(x)$ from $\mathfrak{A}$ and put $\deg(f) = m$. If $m < n$, then $f(x)$ is in $\mathfrak{A}'$. Therefore we shall assume that $m \geq n$ and apply an induction on m. By the choice of $g_1(x), \ldots, g_s(x)$ we can find $a_1, \ldots, a_s$ in A such that for

$$f'(x) = f(x) - \sum_{1 \leq i \leq s} a_i x^{m-n} g_i(x)$$

we have $\deg(f') < m$. Then by induction $f'(x)$, hence also $f(x)$, is in $\mathfrak{A}' + \mathfrak{A}''$. The rest of the proof is as follows.

Since $\mathfrak{A}'$ is an A-submodule of the finitely generated A-module $A + Ax + \ldots + Ax^{n-1}$, by Lemma 1.3.1 it is finitely generated. Therefore $\mathfrak{A}' = Af_1(x) + \ldots + Af_r(x)$ for some $f_1(x), \ldots, f_r(x)$ in $\mathfrak{A}$. This implies

$$\mathfrak{A} = \sum_{1 \leq i \leq r} A[x]f_i(x) + \sum_{1 \leq j \leq s} A[x]g_j(x).$$

If K is an arbitrary field, then 0 and K are the only ideals of K, hence it is a noetherian ring. Therefore by using Lemmas 1.3.1 and 1.3.2 we get *Hilbert's basis theorem*, which we state as follows:

Theorem 1.3.1 *Let A denote the polynomial ring $K[x_1, \ldots, x_n]$, where K is a field and $x_1, \ldots, x_n$ are variables, M a finitely generated A-module, and N any A-submodule of M. Then N is also finitely generated. In particular, every ideal of A has a finite ideal basis.*

We shall next explain Hilbert's Nullstellensatz. We shall start with its shallow generalization for a better understanding. Since we shall not use this result, we just outline its proof. Let A denote any commutative ring with the unit element. Then a nilpotent element of A is clearly contained in every prime ideal of A. The converse is true and the proof is quite simple. Consider the polynomial ring $A[x]$ as in Lemma 1.3.2 and take any a from the intersection of all prime ideals of A. Then $1 - ax$ is a unit of $A[x]$. Otherwise $1 - ax$ is contained in a maximal ideal, hence a prime ideal, say, $\mathfrak{P}$ of $A[x]$. This is clear if A, hence $A[x]$, is a noetherian ring. In the general case, we have only to use Zorn's lemma. At any rate, if $\mathfrak{p}$ denotes the intersection of A and $\mathfrak{P}$, then $\mathfrak{p}$ is a prime ideal of A, hence $\mathfrak{p}$ contains a. Then $\mathfrak{P}$ contains $(1 - ax) + ax = 1$, a contradiction. Therefore $(1 - ax)f(x) = 1$ for some $f(x)$ in $A[x]$, and this implies $a^{n+1} = 0$ if $\deg(f) = n$. The above result implies that for any ideal $\mathfrak{a}$ of A, its root $r(\mathfrak{a})$ is the intersection of all prime ideals of A

which contain $\mathfrak{a}$. Hilbert's Nullstellensatz is similar to the above statement. We shall state and prove it after the following lemma:

Lemma 1.3.3 *Let $\mathfrak{m}$ denote any maximal ideal of the polynomial ring $K[x] = K[x_1, \dots, x_n]$. Then the images of $x_1, \dots, x_n$ in $K[x]/\mathfrak{m}$ are all algebraic over K.*

Proof. We denote the image of x_i in $K[x]/\mathfrak{m}$ by x_i', assume that they are not all algebraic over K, and derive a contradiction. After a permutation we may assume that $y_i = x_i'$ for $i \leq r$ are algebraically independent over K and x_i' for $i > r$ are algebraic over $K(y)$, where $y = (y_1, \dots, y_r)$. We choose $d(y) \neq 0$ from $K[y]$ so that if we denote $d(y)x_i'$ for $i > r$ by $z_1, \dots, z_s$, then they become zeros of monic polynomials with coefficients in $K[y]$ of respective degrees say $n_1, \dots, n_s$. Since $K[x'] = K[x_1', \dots, x_n']$ is a field, $d(y)^{-1}$ is in $K[x']$, hence $K[x'] = K[d(y)^{-1}, y, z]$, where $z = (z_1, \dots, z_s)$. Furthermore if we put $N = n_1 \cdots n_s$ and denote $z_1^{e_1} \cdots z_s^{e_s}$, where $0 \leq e_i < n_i$ for all i, by $w_1, \dots, w_N$, then we will have $K[y, z] = K[y]w_1 + \dots + K[y]w_N$. On the other hand, for some $y' = (y_1', \dots, y_r')$ with y_i' algebraic over K we have $d(y') \neq 0$. We can take y' from K^r if K is infinite. If we denote by $\mathfrak{p}$ the kernel of the homomorphism $K[y] \to K[y']$ defined by $y_i \mapsto y_i'$, then $\mathfrak{p}$ is a prime ideal of $K[y]$ not containing $d(y)$ and $\mathfrak{p} \neq 0$ by $r > 0$, hence $K[x']\mathfrak{p} = K[x']$. We put $S = K[y]\backslash\mathfrak{p}$, $A = S^{-1}K[y]$, and $M = S^{-1}K[y, z]$. Then A is a local ring with $S^{-1}\mathfrak{p}$ as its maximal ideal and $M = K[x'] = Aw_1 + \dots + Aw_N$. Furthermore, $(S^{-1}\mathfrak{p})M = M$. This implies the contradiction $M = 0$ by Theorem 1.2.2.

Now *Hilbert's Nullstellensatz* is a consequence of Lemma 1.3.3 and the fact that $r(\mathfrak{a})$ for any ideal $\mathfrak{a}$ of $K[x]$ is the intersection of all maximal ideals of $K[x]$ which contain $\mathfrak{a}$. The classical statement is as follows:

Theorem 1.3.2 *Let $f(x), f_1(x), \dots, f_r(x)$ denote elements of the polynomial ring $K[x] = K[x_1, \dots, x_n]$ and Ω any algebraically closed extension of K such that $f(a) = 0$ for every $a = (a_1, \dots, a_n)$ in Ω^n satisfying $f_i(a) = 0$ for all i. Then there exists a positive integer e and $a_1(x), \dots, a_r(x)$ in $K[x]$ such that*

$$f(x)^e = \sum_{1 \leq i \leq r} a_i(x) f_i(x).$$

Proof. We exclude the trivial case where $f(x) = 0$, introduce a new variable y, and denote by $\mathfrak{a}$ the ideal of $K[x, y]$ generated by $f_1(x), \dots, f_r(x)$, $1 - f(x)y$. Then Lemma 1.3.3 and the assumption imply that $\mathfrak{a}$ is not contained in any maximal ideal of $K[x, y]$, hence $\mathfrak{a} = K[x, y]$, and hence

$$1 = \sum_{1 \leq i \leq r} a_i(x, y) f_i(x) + a(x, y)(1 - f(x)y)$$

for some $a_1(x, y), \dots, a_r(x, y), a(x, y)$ in $K[x, y]$. If $y^{e_\circ}$ is the highest power of y which occurs in $a_1(x, y), \dots, a_r(x, y)$ and $e = e_\circ + 1$, then by replacing y by $1/f(x)$, we get the relation in the theorem with $a_i(x) = f(x)^e a_i(x, 1/f(x))$ in $K[x]$ for all i.

Finally, we shall explain Hilbert's theorem on his characteristic functions. Hilbert's original proof depends on the theory of syzygies. Another proof by B. L.

van der Waerden depends on ideal theory. We shall explain the proof by M. Nagata [44] which seems to be the simplest known proof. We shall start with the following well-known lemma, in which $\mathbb{N}$ denotes the set of nonnegative integers:

Lemma 1.3.4 *Let $\chi(t)$ denote a polynomial of degree d in one variable t with coefficients in a field of characteristic 0 such that $\chi(r)$ is in $\mathbb{Z}$ for all large r in $\mathbb{N}$. Then $\chi(t)$ is necessarily of the form*

$$\chi(t) = \sum_{0 \le i \le d} a_i \binom{t}{i}, \qquad \binom{t}{i} = t(t-1)\dots(t-i+1)/i!$$

with $a_0, a_1, \dots, a_d$ in $\mathbb{Z}$.

Proof. Since the highest degree term of $\binom{t}{i}$ is $t^i/i!$, we can uniquely write $\chi(t)$ as in the lemma with $a_0, a_1, \dots, a_d$ in the field. Since they are clearly in $\mathbb{Z}$ for $d = 0$, we shall assume that $d > 0$ and apply an induction on d. If we put $\sigma(t) = \chi(t+1) - \chi(t)$, then $\deg(\sigma) = d - 1$ and $\sigma(r)$ is in $\mathbb{Z}$ for all large r. Therefore if we write

$$\sigma(t) = \sum_{0 \le i < d} b_i \binom{t}{i},$$

then $b_0, b_1, \dots, b_{d-1}$ are in $\mathbb{Z}$ by induction. On the other hand

$$\chi(t+1) - \chi(t) = \sum_{0 \le i < d} a_{i+1} \binom{t}{i},$$

hence $a_1 = b_0, a_2 = b_1, \dots, a_d = b_{d-1}$ are in $\mathbb{Z}$. Then

$$a_0 = \chi(r) - \sum_{0 < i \le d} a_i \binom{r}{i}$$

with $\chi(r)$ in $\mathbb{Z}$ for all large r shows that a_0 is also in $\mathbb{Z}$.

We take the polynomial ring $A = K[x_1, \dots, x_n]$ as before and denote by A_r its subspace consisting of homogeneous polynomials of degree r for all r. Then A becomes the direct sum of $A_0 = K, A_1, A_2, \dots$ satisfying $A_i A_j \subset A_{i+j}$ for all i, j. Such an A, with A_0 just a subring of A in general, is called a *graded ring*. If an A-module M is a direct sum of its additive subgroups $M_0, M_1, M_2, \dots$ satisfying $A_i M_j \subset M_{i+j}$ for all i, j, then it is called a *graded A-module*. If N is an A-submodule of M such that it becomes the direct sum of $N_r = N \cap M_r$ for all r, then automatically $A_i N_j \subset N_{i+j}$ for all i, j; such an N is called a graded A-submodule of M. In that case, the factor module M/N becomes a graded A-module with $(M/N)_r = M_r/N_r$ for all r. We observe that A itself is a graded A-module; we call its graded A-submodule a *homogeneous ideal* of A. If M is any graded A-module, we put

$$F_r(M) = \sum_{i \le r} M_i = M_0 + M_1 + \dots + M_r$$

for all r. The *Hilbert characteristic function*, abbreviated as Hf, is the polynomial $\chi(M, t)$ of t in the following theorem:

Theorem 1.3.3 *If A is the polynomial ring $K[x_1, \dots, x_n]$ and M is a finitely generated graded A-module, then there exists a polynomial $\chi(M,t)$ of degree at most n satisfying*

$$\dim_K(F_r(M)) = \chi(M,r)$$

for all large r.

Proof. If $\chi(M,t)$ exists, then we say that M has an Hf. To be proved is that every finitely generated graded A-module M has an Hf. We observe that if M has an Hf and $M^{\#}$ is a new graded A-module defined as $(M^{\#})_r = M_{r+r_\circ}$ for some fixed $r_\circ$ and for all r, then $M^{\#}$ also has an Hf and $\chi(M,t)$, $\chi(M^{\#},t)$ have the same degree. Furthermore, if M' is a graded A-submodule of M and if both M' and M/M' have Hf's, then M has $\chi(M',t) + \chi(M/M',t)$ as its Hf. In particular, if $\deg(\chi(M',t)), \deg(\chi(M/M',t)) \le n$, then $\deg(\chi(M,t)) \le n$. After these remarks we write $M = Af_1 + \ldots + Af_m$. We may assume that each f_i is in M_{r_i} for some r_i. If $m = 0$, hence $M = 0$, then M has 0 as its Hf. Furthermore, if we can show that every M with $m = 1$ has an Hf, then by induction $M' = Af_1 + \ldots + Af_{m-1}$ and $M'' = M/M'$ will have Hf's, hence M has an Hf. Therefore, we have only to show that $M = Af_1$ has an Hf and $\deg(\chi(M,t)) \le n$.

If we denote by $\mathfrak{a}$ the kernel of the A-homomorphism from A to M defined by $a \mapsto af_1$, then $\mathfrak{a}$ is a homogeneous ideal of A and $(A/\mathfrak{a})_r$ becomes K-isomorphic to M_{r+r_1}, i.e., $(A/\mathfrak{a})_r$ is mapped K-linearly and bijectively to M_{r+r_1}, for all r. Therefore, if $A/\mathfrak{a}$ has an Hf, so does M. Furthermore, since

$$\dim_K(F_r(A/\mathfrak{a})) \le \dim_K(F_r(A)) = \binom{n+r}{n},$$

we will have $\deg(\chi(M,t)) \le n$. Consider the set Σ of all homogeneous ideals $\mathfrak{a}$ of A, different from A, with the property that $A/\mathfrak{a}$ does not have an Hf. We have only to derive a contradiction assuming that Σ is not empty. We choose any $\mathfrak{a}$ which is maximal in Σ. Then $\mathfrak{a}_1$ is strictly contained in A_1 for otherwise $\mathfrak{a}$ becomes $A_1 + A_2 + \ldots$ and $A/\mathfrak{a}$ will have 1 as its Hf. Therefore, we can choose f from $A_1 \backslash \mathfrak{a}_1$. Then the homogeneous ideal $Af + \mathfrak{a}$ strictly contains $\mathfrak{a}$, hence $A/(Af + \mathfrak{a})$ has an Hf, and hence $\sigma(t) = \chi(A/(Af + \mathfrak{a}), t)$ is defined. We observe that $\mathfrak{a} : f$ is a homogeneous ideal of A containing $\mathfrak{a}$ and that the correspondence $a \mapsto af$ gives rise to a K-isomorphism from $A_r/(\mathfrak{a} : f)_r$ to $(Af + \mathfrak{a})_{r+1}/\mathfrak{a}_{r+1}$ for every r. A simple computation of dimensions then shows that

$$\dim_K(F_{r+1}(A/\mathfrak{a})) - \dim_K(F_r(A/(\mathfrak{a} : f))) = \dim_K(F_{r+1}(A/(Af + \mathfrak{a})))$$

for every r, and the RHS is equal to $\sigma(r+1)$ for all large r. If $\mathfrak{a} : f = \mathfrak{a}$, then we see, as in the proof of Lemma 1.3.4, that $A/\mathfrak{a}$ has an Hf, which is not the case. Therefore $\mathfrak{a} : f$ strictly contains $\mathfrak{a}$, hence $A/(\mathfrak{a} : f)$ has an Hf, and then $A/\mathfrak{a}$ also has an Hf. This is a contradiction.

We remark that if $\mathfrak{a}$ is any homogeneous ideal of $A = K[x_1, \dots, x_n]$, different from 0, then in

$$\chi(\mathfrak{a}, t) = \sum_{0 \le i \le n} a_i \binom{t}{i}$$

we always have $a_n = 1$. In fact $\mathfrak{a} \neq 0$ implies $\mathfrak{a}_{r_\circ} \neq 0$ for some $r_\circ$. If $f \neq 0$ is in $\mathfrak{a}_{r_\circ}$, then $A_r f \subset \mathfrak{a}_{r+r_\circ} \subset A_{r+r_\circ}$, hence

$$\dim_K(A_r) = \dim_K(A_r f) \leq \dim_K(\mathfrak{a}_{r+r_\circ}) \leq \dim_K(A_{r+r_\circ})$$

for every r. This implies the above assertion.

https://doi.org/10.1090/amsip/014/02

Chapter 2

Implicit function theorems and K-analytic manifolds

2.1 Implicit function theorem

We shall prove an implicit function theorem over an arbitrary complete field K using *calculus of limits*. This method was discovered by A. Cauchy in the case where $K = \mathbb{C}$ to prove general existence theorems. The fact that it can be applied to prove similar theorems over an arbitrary complete field K was pointed out, possibly for the first time, in [21]. At any rate, since Cauchy's calculus of limits is very seldom taught in any graduate course, we shall give all the details to the proof.

We shall denote by K a field with an absolute value $|\cdot|_K$. This means that $|\cdot|_K$ is an $\mathbb{R}$-valued function on K satisfying the following conditions:

AV 1. $|a|_K \geq 0$ for all a in K and $|a|_K = 0$ if and only if $a = 0$.

AV 2. $|ab|_K = |a|_K|b|_K$ for all a, b in K.

AV 3. $|a + b|_K \leq |a|_K + |b|_K$ also for all a, b in K.

We shall exclude the trivial case where $\mathrm{Im}(K^\times)$, the image of $K^\times$ under $|\cdot|_K$, is $\{1\}$. Then $\mathrm{Im}(K^\times)$ contains a sequence $\{r_i\}_i = \{r_1, r_2, \dots\}$ which tends to 0. If for any b in K we take the family of subsets of K defined by $|a - b|_K < r_i$ for $i = 1, 2, \dots$ as a base of open sets containing b, then K becomes a Hausdorff space. Furthermore the algebraic operations in K are continuous. If $a = (a_1, \dots, a_n)$ is in K^n, we put

$$\|a\| = \max(|a_1|_K, \dots, |a_n|_K).$$

Then in K^n with the product topology the family of subsets defined by $\|a\|_K < r_i$ for $i = 1, 2, \dots$ forms a base of open sets containing 0. We shall later replace $|\cdot|_K$ by $|\cdot|_K^\rho$ for some $\rho > 0$, e.g., in the case where $K = \mathbb{C}$. If we do this, the new absolute value ceases to satisfy AV 3 and yet it defines the same topology on K.

We shall assume in most cases that K is complete. This means that every Cauchy sequence in K , i.e., a sequence satisfying Cauchy's criterion of convergence, is convergent. Explicitly stated, if $a_1, a_2, \dots$ are elements of K and $|a_i - a_j|_K$ tends to 0 as i, j tend to ∞, then there exists an element a of K, necessarily unique, such that $|a_i - a|_K$ tends to 0 as i tends to ∞. If K is any field with an absolute value $|\cdot|_K$, the set of Cauchy sequences in K forms a commutative ring with the unit element under the termwise addition and multiplication. In this ring the set of all null sequences, i.e., sequences which tend to 0, forms a maximal ideal. We denote

the corresponding factor ring by K^*. If a^* is an element of K^* represented by a Cauchy sequence $\{a_i\}_i$, then the sequence $\{|a_i|_K\}_i$ in $\mathbb{R}$ has a limit which depends only on a^*. If we denote this limit by $|a^*|_{K^*}$, then $|\cdot|_{K^*}$ gives an absolute value on K^* and K^* becomes a complete field. If to every a in K we associate the element of K^* represented by the sequence all terms of which are a, then we get an injective homomorphism from K to K^*. If we identify K with its image in K^*, then $|\cdot|_{K^*}$ restricts to $|\cdot|_K$ on K and K is dense in K^*, i.e., K^* becomes the closure of K. The field K^* is called the completion of K. The completion of $\mathbb{Q}$ by the usual absolute value on $\mathbb{Q}$ is $\mathbb{R}$. If p is a prime number, then every a in $\mathbb{Q}^\times$ can be written uniquely as $a = p^e b$ for some e in $\mathbb{Z}$ and b in $\mathbb{Q}^\times$ with its denominator and numerator both not divisible by p. If we put

$$|a|_p = p^{-e}, \qquad |0|_p = 0,$$

then $|\cdot|_p$ gives an absolute value on $\mathbb{Q}$ and the corresponding completion of $\mathbb{Q}$ is the Hensel p-adic field $\mathbb{Q}_p$.

If A is a commutative ring with the unit element, in particular if A is a field K, and if $i = (i_1, \ldots, i_n)$ is in $\mathbb{N}^n$, $x = (x_1, \ldots, x_n)$ where $x_1, \ldots, x_n$ are variables, and c_i is in A for all i, then we shall write

$$\sum c_i x^i = \sum_{i_1,\ldots,i_n} c_{i_1\ldots i_n} x_1^{i_1} \cdots x_n^{i_n}.$$

The set $A[[x_1, \ldots, x_n]]$ of all such formal power series forms a commutative ring. If K is a complete field, basic properties of sequences and infinite series for $K = \mathbb{R}$, which one learns in calculus, remain valid for K. If a series in $K[[x]] = K[[x_1, \ldots, x_n]]$ is convergent at every a in K^n satisfying $\|a\| < r$ for some $r > 0$, then it is called a convergent power series. The set $K\langle\langle x\rangle\rangle = K\langle\langle x_1, \ldots, x_n\rangle\rangle$ of all such convergent power series forms a subring of $K[[x]]$. If for $\sum c_i x^i$ in $K[[x]]$ and $\sum c_i^\circ x^i$ in $\mathbb{R}\langle\langle x\rangle\rangle$ we have $|c_i|_K \leq c_i^\circ$ for all i, then we shall write

$$\sum c_i x^i << \sum c_i^\circ x^i$$

and call $\sum c_i^\circ x^i$ a *dominant series* for $\sum c_i x^i$.

Lemma 2.1.1 *A formal power series is a convergent power series if and only if it has a dominant series.*

Proof. Since the if-part is straightforward, we shall prove the only-if part. Suppose that $\sum c_i x^i$ is a convergent power series, i.e., $\sum c_i a^i$ is convergent for every a in K^n satisfying $||a|| < r$ for some $r > 0$. Choose $0 < r_\circ < r$ from $\mathrm{Im}(K^\times)$. Then for every a in K^n satisfying $||a|| \leq r_\circ$ we have

$$|c_i a^i|_K \leq |c_i|_K r_\circ^{|i|}, \qquad |i| = i_1 + \ldots + i_n.$$

Furthermore $|c_i|_K r_\circ^{|i|}$ tends to 0 as $|i|$ tends to ∞, hence it is bounded by some $M > 0$. It is then clear that

$$\sum c_i x^i << \sum \left(\frac{M}{r_\circ^{|i|}}\right) x^i.$$

We observe that if $F(y)$ is in $A[[y_1, \dots, y_m]]$ and $f_i(x)$ is in $A[[x_1, \dots, x_n]]$ satisfying $f_i(0) = 0$ for $1 \leq i \leq m$ for some m, n, then $F(f(x)) = F(f_1(x), \dots, f_m(x))$ is clearly in $A[[x_1, \dots, x_n]]$. If $A = K$ is a complete field and $F(y)$, $f_i(x)$ are convergent power series for all i, then $F(f(x))$ is a convergent power series.

Lemma 2.1.2 *If $F(x, y)$ is an element of $K[[x, y]] = K[[x, y_1, \dots, y_m]]$, it can be written uniquely as*

$$F(x, y) = F(x, 0) + \sum_{1 \leq k \leq m} H_k(x, y_1, \dots, y_k) y_k$$

with $H_k(x, y_1, \dots, y_k)$ in $K[[x, y_1, \dots, y_k]]$ for $1 \leq k \leq m$. If further $F(x, y)$ is a convergent power series, then every $H_k(x, y_1, \dots, y_k)$ is a convergent power series.

Proof. Firstly, the uniqueness is clear. Since the lemma holds trivially for $m = 0$, we shall assume that $m > 0$ and apply an induction on m. We have

$$F(x, y) = F(x, y_1, \dots, y_{m-1}, 0) + H_m(x, y) y_m$$

with $H_m(x, y)$ in $K[[x, y]]$. Furthermore if $F(x, y) << F^\circ(x, y)$ and

$$F^\circ(x, y) = F^\circ(x, y_1, \dots, y_{m-1}, 0) + H_m^\circ(x, y) y_m,$$

then $F(x, y_1, \dots, y_{m-1}, 0) << F^\circ(x, y_1, \dots, y_{m-1}, 0)$ and $H_m(x, y) << H_m^\circ(x, y)$. Therefore we have only to apply an induction to $F(x, y_1, \dots, y_{m-1}, 0)$.

As a consequence, if $G(x, y)$ is an element of $K[[x, y]]$ (resp. $K\langle\langle x, y\rangle\rangle$) of the form $G(x, y) = \sum c_{ij} x^i y^j$ with $c_{00} = 0$ and $c_{0j} = 0$ for $|j| = 1$ and if $z_1, \dots, z_m$ are variables, then

$$G(x, y + z) = G(x, y) + \sum_{1 \leq k \leq m} H_k(x, y, z) z_k$$

with $H_k(x, y, z)$ in $K[[x, y, z]]$ (resp. $K\langle\langle x, y, z\rangle\rangle$) free from $z_{k+1}, \cdots, z_m$. Since $G(0, z) = H_1(0, 0, z) z_1 + \dots + H_m(0, 0, z) z_m$, we have $H_k(0, 0, 0) = 0$ for all k.

All termwise partial derivatives of a convergent power series are convergent power series. More precisely if

$$\sum c_i x^i << \sum c_i^\circ x^i,$$

then

$$\partial(\sum c_i x^i)/\partial x_j << \partial(\sum c_i^\circ x^i)/\partial x_j$$

for all j. In fact, we have $|i_j c_i|_K \leq i_j c_i^\circ$ for every i and the RHS is a convergent power series.

Lemma 2.1.3 *Suppose that*

$$f(x) = \sum c_i x^i << \sum \left(\frac{M}{r^{|i|}}\right) x^i$$

for some $M, r > 0$ and U is the neighborhood of 0 in K^n defined by $\|a\| < r$; denote by f the K-valued function on U defined by $a \mapsto f(a)$. Then $f = 0$ implies $f(x) = 0$. Furthermore partial derivatives of f are the functions on U obtained from the corresponding termwise partial derivatives of $f(x)$. In particular f is continuous.

Proof. We shall prove the first part, i.e., $f = 0$ implies $f(x) = 0$. This can be done by using the principle of the irrelevance of algebraic inequalities in Chapter 1.1 or directly as follows. Suppose first that $n = 1$ and

$$f(x) = \sum_{i \geq k} c_i x^i, \qquad c_k \neq 0$$

for some $k \geq 0$. If a is in $K^\times$ and $|a|_K < r$, then

$$\frac{f(a)}{a^k} = c_k + \sum_{i>k} c_i a^{i-k} = 0, \qquad \Big|\sum_{i>k} c_i a^{i-k}\Big|_K \leq \frac{M|a|_K}{r^k(r - |a|_K)}.$$

We know that $\mathrm{Im}(K^\times)$ contains a null sequence in $\mathbb{R}$. Therefore we can choose a above so that the RHS becomes less than $|c_k|_K$. We then have a contradiction. Suppose next that $n > 1$ and

$$f(x) = f(x', x_n) = \sum_{i \geq k} f_i(x') x_n^i, \qquad f_k(x') \neq 0,$$

in which $f_i(x')$ are all in $K[[x_1, \ldots, x_{n-1}]]$. Then they are convergent at every a' in K^{n-1} satisfying $\|a'\| < r$, where $\|\cdot\|$ is relative to K^{n-1}. Since $f_k(x') \neq 0$, by induction we can find a' such that $f_k(a') \neq 0$. Then $f(a', x_n) \neq 0$, hence $f(a', a_n) \neq 0$ for some a_n in K satisfying $|a_n|_K < r$, and hence $f \neq 0$. This is a contradiction.

We shall prove the second part. As in calculus, we may assume that $n = 1$. Take a from K, h from $K^\times$ satisfying $|a|_K + |h|_K < r$. Then we have

$$\Big|\frac{f(a+h) - f(a)}{h} - \sum i c_i a^{i-1}\Big|_K \leq \frac{Mr|h|_K}{(r - |a|_K - |h|_K)(r - |a|_K)^2}.$$

If $|h|_K$ tends to 0, the RHS, hence also the LHS, tends to 0.

Theorem 2.1.1 *(i) Let K denote an arbitrary field and assume for some m, n that every $F_i(x, y)$ in $F(x, y) = (F_1(x, y), \ldots, F_m(x, y))$ is in $K[[x, y]] = K[[x_1, \ldots, x_n, y_1, \ldots, y_m]]$ satisfying $F_i(0, 0) = 0$ and further*

$$\partial(F_1, \ldots, F_m)/\partial(y_1, \ldots, y_m)(0, 0) \neq 0,$$

in which $\partial(F_1, \ldots, F_m)/\partial(y_1, \ldots, y_m)$ is the jacobian, i.e., the determinant of the square matrix of degree m with $\partial F_i/\partial y_j$ as its (i, j)-entry. Then there exists a unique $f(x) = (f_1(x), \ldots, f_m(x))$ with every $f_i(x)$ in $K[[x]] = K[[x_1, \ldots, x_n]]$ satisfying $f_i(0) = 0$ and further $F(x, f(x)) = 0$, i.e., $F_i(x, f(x)) = 0$ for all i.
(ii) In the above situation, if K is a complete field and if every $F_i(x, y)$ is a convergent power series, then every $f_i(x)$ is also a convergent power series. Furthermore if a is near 0 in K^n, then $f(a)$ is near 0 in K^m and $F(a, f(a)) = 0$, and if (a, b) is near $(0, 0)$ in $K^n \times K^m$ and $F(a, b) = 0$, then $b = f(a)$.

Proof of (i). If we write

$$F_i(x,y) = \sum_{1\le j\le m} a_{ij}y_j - G_i(x,y), \qquad G_i(x,y) = \sum_{|j|+|k|>0} c_{ijk}x^j y^k$$

with a_{ij}, c_{ijk} in K, in which $c_{i0k} = 0$ for $|k| = 1$, then $a_{ij} = (\partial F_i/\partial y_j)(0,0)$ for all i, j. The square matrix a with a_{ij} as its (i,j)-entry is in $\mathrm{GL}_m(K)$ by assumption. We observe that $f(x)$ satisfying $F(x, f(x)) = 0$ is not affected by any invertible K-linear transformation of entries of $F(x,y)$. Therefore, after multiplying a^{-1} to $F(x,y)$, regarded as a column vector, we may assume that $a_{ij} = \delta_{ij}$, i.e., $a_{ii} = 1$ and $a_{ij} = 0$ for $i \neq j$. After this adjustment we write

$$f_i(x) = \sum_{|j|>0} d_{ij}x^j$$

with unknown coefficients d_{ij} in K. Since $F(x, f(x)) = 0$ can be rewritten as

$$f_i(x) = \sum_{|j|+|k|>0} c_{ijk}x^j f(x)^k$$

for all i, if we denote by $f_{ip}(x)$ the homogeneous part of degree p in $f_i(x)$, then $F(x, f(x)) = 0$ becomes equivalent to

$$f_{ip}(x) = \sum c_{ijk}x^j \left(\prod_{1\le\alpha\le m} \prod_{1\le\beta\le k_\alpha} f_{\alpha\ p_{\alpha\beta}}(x) \right),$$

in which $\sum k_\alpha = |k|$ and

$$(*) \qquad |j| + \sum_{1\le\alpha\le m} \sum_{1\le\beta\le k_\alpha} p_{\alpha\beta} = p, \qquad p_{\alpha\beta} > 0,$$

in particular $|j| + |k| \le p$, for $p = 1, 2, 3, \ldots$. Since $c_{i0k} = 0$ for $|k| = 1$, if $p = 1$, then

$$f_{i1}(x) = \sum_{|j|=1} c_{ij0}x^j.$$

Furthermore, if $p > 1$, then in $(*)$ we have $p_{\alpha\beta} < p$ for $c_{ijk} \neq 0$. In fact if $p_{\alpha\beta} \ge p$, hence $p_{\alpha\beta} = p$, for some α, β, then $j = 0$, $k_\alpha = 1$, and $k_{\alpha'} = 0$ for $\alpha' \neq \alpha$. This implies $|k| = 1$ and $c_{ijk} = c_{i0k} = 0$. We have thus shown that $f_{i1}(x)$ is as above and $f_{ip}(x)$ for $p > 1$ is determined by $f_{i'p'}(x)$ for $p' < p$. Therefore $f_i(x)$ is uniquely determined by an induction on p.

Proof of (ii). We start with an additional observation still in the case where K is an arbitrary field. The above proof shows that $d_{ij} = c_{ij0}$ for $|j| = 1$ and that d_{ij} for $|j| = p > 1$ is a polynomial in $c_{i'j'k'}$ and $d_{i''j''}$ for $|j'| + |k'| \le p$ and $|j''| < p$ with coefficients in $\mathbb{N}$. Therefore, again by an induction on p, we see that

$$d_{ij} = P_{ij}(c_{i'j'k'}),$$

in which P_{ij} is a polynomial in $c_{i'j'k'}$ for $|j'|+|k'| \leq p$ with coefficients in $\mathbb{N}$.

Suppose now that K is a complete field and $F_i(x,y)$ is in $K\langle\langle x,y\rangle\rangle$. Then by Lemma 2.1.1 we will have

$$\begin{aligned} G_i(x,y) &<< \sum_{|j|+|k|>0}{}' \left(\frac{M}{r^{|j|+|k|}}\right) x^j y^k \\ &<< \sum_{p+q>0}{}'' \left(\frac{M}{r^{p+q}}\right) (x_1+\ldots+x_n)^p (y_1+\ldots+y_m)^q \end{aligned}$$

for some $M, r > 0$, in which $\sum'$ (resp. $\sum''$) indicates the restriction $|k| > 1$ for $j = 0$ (resp. $q > 1$ for $p = 0$). If we denote the last power series by $G_i^\circ(x,y)$ and put

$$F_i^\circ(x,y) = y_i - G_i^\circ(x,y), \qquad G_i^\circ(x,y) = \sum_{|j|+|k|>0} c_{ijk}^\circ x^j y^k,$$

then $|c_{ijk}|_K \leq c_{ijk}^\circ$ for all i,j,k and by (i) we have a unique $f_i^\circ(x) = (f_1^\circ(x),\ldots,f_n^\circ(x))$ in $\mathbb{R}[[x]]$ satisfying $f_i^\circ(0) = 0$ and $F^\circ(x, f^\circ(x)) = 0$. Furthermore

$$f_i^\circ(x) = \sum_{|j|>0} d_{ij}^\circ x^j, \qquad d_{ij}^\circ = P_{ij}(c_{i'j'k'}^\circ)$$

with the same polynomial P_{ij} as before. Since the coefficients of P_{ij} are in $\mathbb{N}$, therefore, we get

$$|d_{ij}|_K = |P_{ij}(c_{i'j'k'})|_K \leq P_{ij}(|c_{i'j'k'}|_K) \leq P_{ij}(c_{i'j'k'}^\circ) = d_{ij}^\circ$$

for all i,j. If, for a moment, we accept the fact that $f_i^\circ(x)$ is in $\mathbb{R}\langle\langle x\rangle\rangle$, then by definition $f_i(x) << f_i^\circ(x)$ for all i. Therefore the formal identity $F(x,f(x)) = 0$ implies $F(a,f(a)) = 0$ for all a near 0 in K^n.

We shall show that if (a,b) is near $(0,0)$ in $K^n \times K^m$ and $F(a,b) = 0$, then $b = f(a)$. If $y_1',\ldots,y_m'$ are other variables, then by the remark after Lemma 2.1.2 we can write

$$G_i(x,y) - G_i(x,y') = \sum_{1\leq j\leq m} H_{ij}(x,y,y')(y_j - y_j')$$

with $H_{ij}(x,y,y')$ in $K\langle\langle x,y,y'\rangle\rangle$ satisfying $H_{ij}(0,0,0) = 0$ for all i,j. Furthermore,

$$b_i - f_i(a) = G_i(a,b) - G_i(a,f(a)) = \sum_{1\leq j\leq m} H_{ij}(a,b,f(a))(b_j - f_j(a)),$$

hence

$$\sum_{1\leq j\leq m} (\delta_{ij} - H_{ij}(a,b,f(a)))(b_j - f_j(a)) = 0$$

for all i. Since $H_{ij}(a,b,b')$ depends continuously on (a,b,b') near $(0,0,0)$ in $K^n \times K^m \times K^m$ by Lemma 2.1.3 and $H_{ij}(0,0,0) = 0$, the coefficient-matrix is invertible for (a,b) near $(0,0)$, hence $b = f(a)$.

Finally, we shall show that $f_i^\circ(x)$ is in $\mathbb{R}\langle\langle x\rangle\rangle$. If we put $X = x_1 + \ldots + x_n$ and $Y = y_1 + \ldots + y_m$, then we have

$$G_i^\circ(x,y) = \frac{M}{(1-X/r)(1-Y/r)} - M(1+Y/r),$$

hence $F^\circ(x,y) = 0$ if and only if $y_1 = \ldots = y_m = Y/m$ and

$$\left(\frac{M}{r^2} + \frac{1}{mr}\right) Y^2 - \frac{Y}{m} + \frac{MX}{(r-X)} = 0.$$

This equation in Y has a unique solution in $\mathbb{R}\langle\langle X\rangle\rangle$ which becomes 0 for $X = 0$. This clearly implies that $f_i^\circ(x)$ is in $\mathbb{R}\langle\langle x\rangle\rangle$.

Corollary 2.1.1 *(i) If $g_i(x)$ in $K[[x]]$, where K is an arbitrary field, satisfies $g_i(0) = 0$ for $1 \le i \le n$ and*

$$\partial(g_1, \ldots, g_n)/\partial(x_1, \ldots, x_n)(0) \neq 0,$$

then there exists a unique $f(x) = (f_1(x), \ldots, f_n(x))$ with $f_i(x)$ in $K[[x]]$ satisfying $f_i(0) = 0$ for all i and $g(f(x)) = x$. (ii) In the above situation, if K is a complete field and $g_i(x)$ is in $K\langle\langle x\rangle\rangle$, then $f_i(x)$ is also in $K\langle\langle x\rangle\rangle$ for all i. Furthermore if b is near 0 in K^n and $a = g(b)$, then a is also near 0 in K^n and $b = f(a)$. Therefore $y = f(x)$ gives rise to a bicontinuous map from a small neighborhood of 0 in K^n to another.

This follows immediately from Theorem 2.1.1. We have only to take $F_i(x,y) = x_i - g_i(y)$ for $1 \le i \le m = n$.

Corollary 2.1.2 *If $g(0) \neq 0$ for $g(x)$ in $K[[x]]$, then $1/g(x)$ can be expressed uniquely as an element of $K[[x]]$; if further $g(x)$ is in $K\langle\langle x\rangle\rangle$, then $1/g(x)$ is also in $K\langle\langle x\rangle\rangle$.*

We may assume that $g(0) = 1$. Then we have only to apply Theorem 2.1.1 to $F(x,y) = g(x)(1+y) - 1$ for $m = 1$. We also mention that if $\mathrm{char}(K)$ does not divide a positive integer m and if the m-th power map is surjective on $K^\times$, then the m-th power map is also surjective on $K[[x]]^\times$. In fact if $g(x)$ is any element of $K[[x]]$ with $g(0) \neq 0$, then $a^m = g(0)$ for some a in $K^\times$. This time we apply Theorem 2.1.1 to $F(x,y) = (a+y)^m - g(x)$.

2.2 Implicit function theorem (non-archimedean case)

We say that an absolute value $|\cdot|_K$ on a field K is *non-archimedean* if, instead of AV 3, it satisfies the following stronger condition:

AV 3′. $|a+b|_K \le \max(|a|_K, |b|_K)$ for all a, b in K.

In such a case if we put

$$O_K = \{a \in K;\ |a|_K \leq 1\},$$

then O_K forms a subring of K and the group of units $O_K^\times$ of O_K is given by

$$O_K^\times = \{a \in K;\ |a|_K = 1\}.$$

We shall assume that $\mathrm{Im}(K^\times)$, the image of $K^\times$ under $|\cdot|_K$, is discrete in $\mathbb{R}^\times$. This condition is equivalent to the ideal of nonunits of O_K being principal, i.e., of the form πO_K for some π in O_K. We shall sometimes write π_K instead of π to avoid any confusion. We keep in mind that π is unique up to a factor in $O_K^\times$, hence $|\pi|_K$ does not depend on the choice of π. At any rate, if a, b are in K and $a - b$ is in $\pi^e O_K$ for some e in $\mathbb{Z}$, mostly for $e > 0$, then we shall write $a \equiv b \bmod \pi^e$. If c is in O_K, then $c \not\equiv 0 \bmod \pi$ means that c is in $O_K^\times$.

We know that a non-archimedean absolute value is characterized by the condition that $|n1|_K \leq 1$ for all n in $\mathbb{N}$. We might as well recall its simple proof. If $|n1|_K \leq 1$ for all n in $\mathbb{N}$, then

$$(|a+b|_K)^n \leq (n+1)\max(|a|_K, |b|_K)^n$$

for all a, b in K, and this implies AV $3'$ above as $n \to \infty$. In particular $\mathbb{Q}_p$ is a complete non-archimedean field. This implies, e.g., by Proposition 11.6.1, that every extension of $\mathbb{Q}_p$ of finite degree is also such a field.

We shall assume that K is a complete non-archimedean field. Then a series in K is convergent if and only if the sequence obtained by replacing each term by its absolute value forms a null sequence in $\mathbb{R}$. If A is a subring of K, then we shall denote by $A\langle\langle x\rangle\rangle$ the intersection of $A[[x]] = A[[x_1, \ldots, x_n]]$ and $K\langle\langle x\rangle\rangle = K\langle\langle x_1, \ldots, x_n\rangle\rangle$. We say that $f(x) = \sum c_i x^i$ in $K[[x]]$ is a *special restricted power series*, abbreviated as SRP, if $f(0) = 0$, i.e., $c_0 = 0$, and

$$c_i \equiv 0 \bmod \pi^{|i|-1}, \qquad |i| = i_1 + \ldots + i_n$$

for all $i \neq 0$ in $\mathbb{N}^n$. This clearly implies that $f(x)$ is in $O_K[[x]]$. Furthermore $f(x)$ is convergent at every a in O_K^n. In fact, we have

$$|c_i a^i|_K \leq |c_i|_K \leq (|\pi|_K)^{|i|-1}$$

and the RHS tends to 0 as $|i| \to \infty$. Therefore $f(a) = \sum c_i a^i$ is convergent and $f(a)$ is in O_K. We introduce the notation

$$P^\#(x) = \pi P(\pi^{-1}x) = \pi P(\pi^{-1}x_1, \ldots, \pi^{-1}x_n)$$

for every $P(x)$ in $K[[x]]$ satisfying $P(0) = 0$. Then clearly $P(x)$ is an SRP in $x_1, \ldots, x_n$ if and only if $P^\#(x)$ is in $O_K[[x]]$. Furthermore if $F(y)$ is an SRP in $y_1, \ldots, y_m$ and all entries of $f(x) = (f_1(x), \ldots, f_m(x))$ are SRP's in $x_1, \ldots, x_n$, then $F(f(x))$ is also an SRP in $x_1, \ldots, x_n$. This can be proved, e.g., as follows. If we put $G(x) = F(f(x))$, then $G(0) = 0$ and $G^\#(x) = F^\#(f^\#(x))$, in which $f^\#(x) = (f_1^\#(x), \ldots, f_m^\#(x))$. Since $F^\#(y)$ is in $O_K[[y]]$ and all entries of $f^\#(x)$ are in $O_K[[x]]$, clearly $G^\#(x)$ is in $O_K[[x]]$, hence $G(x)$ is an SRP in $x_1, \ldots, x_n$.

We shall now go back to Theorem 2.1.1. In (i) below the field K need not be complete:

Theorem 2.2.1 *(i) If $F_i(x,y)$ is in $O_K[[x,y]]$ and $F_i(0,0)=0$ for all i and further*

$$\partial(F_1,\dots,F_m)/\partial(y_1,\dots,y_m)(0,0)\not\equiv 0 \bmod \pi,$$

then every $f_i(x)$ in the unique solution $f(x)=(f_1(x),\dots,f_m(x))$ of $F(x,f(x))=0$ satisfying $f_i(0)=0$ is in $O_K[[x]]$. (ii) If every $F_i(x,y)$ is an SRP in $x_1,\dots,x_n,y_1,\dots,y_m$, then every $f_i(x)$ is an SRP in $x_1,\dots,x_n$. Furthermore if a is in O_K^n, then $f(a)$ is in O_K^m and $F(a,f(a))=0$, and if (a,b) in $O_K^n\times O_K^m$ satisfies $F(a,b)=0$, then $b=f(a)$.

Proof of (i). If, as in the proof of Theorem 2.1.1, we write

$$F_i(x,y)=\sum_{1\le j\le m} a_{ij}y_j - G_i(x,y), \qquad G_i(x,y)=\sum_{|j|+|k|>0} c_{ijk}x^jy^k$$

with a_{ij}, c_{ijk} in O_K this time, in which $c_{i0k}=0$ for $|k|=1$, then the square matrix a with a_{ij} as its (i,j)-entry is in $\mathrm{GL}_m(O_K)$ by assumption. Therefore, after the normalization $a_{ij}=\delta_{ij}$ by multiplying a^{-1} to $F(x,y)$, the new c_{ijk} is still in O_K for all i,j,k. Since

$$f_i(x)=\sum_{|j|>0} d_{ij}x^j, \qquad d_{ij}=P_{ij}(c_{i'j'k'}),$$

in which the coefficients of the polynomial P_{ij} are in $\mathbb{N}$, we see that $f_i(x)$ is in $O_K[[x]]$ for all i.

Proof of (ii). We observe that the normalization $a_{ij}=\delta_{ij}$ does not affect the assumption that $F_i(x,y)$ is an SRP in $x_1,\dots,x_n,y_1,\dots,y_m$ for all i. Therefore $F_i^{\#}(x,y)=\pi F_i(\pi^{-1}x,\pi^{-1}y)$ is in $O_K[[x,y]]$ and $F_i^{\#}(0,0)=0$ for all i, and further

$$\partial(F_1^{\#},\cdots,F_m^{\#})/\partial(y_1,\cdots,y_m)(0,0)=1.$$

Therefore if $g(x)=(g_1(x),\cdots,g_m(x))$, where $g_i(0)=0$, is the unique solution of $F^{\#}(x,g(x))=0$, then every $g_i(x)$ is in $O_K[[x]]$ by what we have shown. On the other hand, $F(x,f(x))=0$ implies $F^{\#}(x,f^{\#}(x))=0$, in which $f_i^{\#}(0)=0$ for all i. Therefore by the uniqueness we get $f_i^{\#}(x)=g_i(x)$, hence $f_i(x)$ is an SRP in $x_1,\cdots,x_n$ for all i. In particular if a is in O_K^n, then $f(a)$ is in O_K^m and the formal identity $F(x,f(x))=0$ implies $F(a,f(a))=0$.

We shall show that if (a,b) in $O_K^n\times O_K^m$ satisfies $F(a,b)=0$, then $b=f(a)$. We observe that the LHS of

$$G_i(x,y)-G_i(x,y')=\sum_{i\le j\le m} H_{ij}(x,y,y')(y_j-y'_j)$$

in the proof of Theorem 2.1.1 (ii) is an SRP in the entries of x,y,y', and it starts from the degree 2 part. Therefore the remark after Lemma 2.1.2 shows that $\pi^{-1}H_{ij}(x,y,y')$ is also an SRP in the same variables. Now since $F(a,b)=0$ implies

$$\sum_{1\le j\le m}(\delta_{ij}-H_{ij}(a,b,f(a)))(b_j-f_j(a))=0$$

for all i with the coefficient-matrix in $\mathrm{GL}_m(K)$, in fact in $\mathrm{GL}_m(O_K)$ because its determinant is in $1+\pi O_K$, we see that $b=f(a)$.

Theorem 2.2.1 has a corollary similar to that of Theorem 2.1.1. We shall use the same notation as in that corollary.

Corollary 2.2.1 *(i) If $g_i(x)$ is in $O_K[[x]]$ and $g_i(0)=0$ for all i and further*

$$\partial(g_1,\dots,g_n)/\partial(x_1,\dots,x_n) \not\equiv 0 \bmod \pi,$$

then every $f_i(x)$ in the unique solution of $g(f(x))=x$ satisfying $f_i(0)=0$ is also in $O_K[[x]]$. (ii) If every $g_i(x)$ is an SRP in $x_1,\dots,x_n$, then every $f_i(x)$ is also an SRP in the same variables, and $y=f(x)$ gives rise to a bicontinuous map from O_K^n to itself

2.3 Weierstrass preparation theorem

In general if $f(x)$ is an element of $A[[x]]=A[[x_1,\dots,x_n]]$, where A is any commutative ring with the unit element, and if the homogeneous part $f_p(x)$ of $f(x)$ of degree p satisfies $f_p(x)=0$ for all $p<r$ and for some r in $\mathbb{N}$, then we shall write $f(x)=f_r(x)+\dots$. If further $f_r(x)\neq 0$, then r and $f_r(x)$ are called respectively the *leading degree* and the *leading form* of $f(x)$. If $g_s(x)$ is the leading form of a similar element $g(x)$ of $A[[x]]$ and if $f_r(x)g_s(x)\neq 0$, then it is the leading form of $f(x)g(x)$. This implies that if A is an integral domain, then $A[[x]]$ is also an integral domain.

We shall explain an immediate consequence of Theorem 2.1.1. If $F(x,y)$ is in $K[[x,y]]=K[[x_1,\dots,x_n,y]]$ satisfying $F(0,0)=0$ and $c=(\partial F/\partial y)(0,0)\neq 0$, i.e., cy is the leading form of $F(0,y)$, then there exists a unique $f(x)$ in $K[[x]]$ satisfying $f(0)=0$ and $F(x,f(x))=0$. If we put $z=y-f(x)$, we will have $F(x,y)=F(x,f(x)+z)=zE_0(x,z)$ with $E_0(x,z)$ in $K[[x,z]]$. This implies

$$F(x,y)=E(x,y)(y-f(x)),$$

in which $E(x,y)=E_0(x,y-f(x))$ is in $K[[x,y]]$ and $E(0,0)=c$. Furthermore if $F(x,y)$ is a convergent power series, then $f(x)$ and $E(x,y)$ are also convergent power series. The *Weierstrass preparation theorem* is a generalization of this fact, and it is as follows:

Theorem 2.3.1 *If $F(x,y)$ is in $K[[x,y]]=K[[x_1,\dots,x_n,y]]$ and has the property that $F(0,y)$ is different from 0 and has cy^m for some $m>0$ as its leading form, then $F(x,y)$ can be written uniquely as*

$$F(x,y)=E(x,y)(y^m+a_1(x)y^{m-1}+\dots+a_m(x)),$$

in which $E(x,y)$ is in $K[[x,y]]$ with $E(0,0)\neq 0$ and $a_1(x),\dots,a_m(x)$ are in $K[[x]]$, hence necessarily $a_i(0)=0$ for all i and $E(0,0)=c$. Furthermore if $F(x,y)$ is a convergent power series, then $a_1(x),\dots,a_m(x)$ and $E(x,y)$ are also convergent power series.

Proof. We shall first show that we indeed have $a_i(0) = 0$ for all i and $E(0,0) = c$. Suppose that $a_{m-i}(0) = 0$ for all $i < k$ and for some $k < m$. Then we will have

$$cy^m + \ldots = (E(0,0) + \ldots)(a_{m-k}(0)y^k + \ldots + a_1(0)y^{m-1} + y^m).$$

By comparing the coefficients of y^k on both sides we get $0 = E(0,0)a_{m-k}(0)$, hence $a_{m-k}(0) = 0$. Therefore by induction we get $a_i(0) = 0$ for all i. Then by comparing the coefficients of y^m on both sides we get $c = E(0,0)$.

After dividing $F(x,y)$ and $E(x,y)$ by c, we may assume that $c = 1$. Since $E(x,y)$ is a unit of $K[[x,y]]$ by Corollary 2.1.2, we replace it by its inverse say $H(x,y)$. Also we replace $F(x,y)$ by $y^m - G(x,y)$. Then the equation to be solved becomes

$$(y^m - G(x,y))H(x,y) = y^m + a_1(x)y^{m-1} + \ldots + a_m(x).$$

We express $G(x,y)$, $H(x,y)$ as power series in y as

$$G(x,y) = \sum_{i\geq 0} g_i(x)y^i, \qquad H(x,y) = \sum_{i\geq 0} h_i(x)y^i$$

and denote the homogeneous parts of $g_i(x), h_i(x)$ of degree j by $g_{ij}(x)$, $h_{ij}(x)$ for all j. The condition that y^m is the leading form of $F(0,y)$ then becomes

$$g_{i0}(x) = g_i(0) = 0$$

for all $i \leq m$. Furthermore if we compare the coefficients of y^{k+m} on both sides of the above equation, we get

$$h_k(x) - \sum_{0\leq i\leq k+m} g_{k+m-i}(x)\, h_i(x) = \delta_0(k)$$

for all k, and for each k this can be replaced by

$$h_{kl}(x) - \sum_{0\leq i\leq k+m} \sum_{0\leq j\leq l} g_{k+m-i,l-j}(x)\, h_{ij}(x) = \delta_0(k)\, \delta_0(l)$$

for all l. In the above, $\delta_0(k)$ is the function taking the value 1 at $k = 0$ and 0 elsewhere. If we incorporate the fact that $g_{i0}(x) = 0$ for all $i \leq m$, then we finally get

$$(*) \qquad h_{kl}(x) = \delta_0(k)\delta_0(l) + \sum_{0\leq i<k} g_{k+mi,0}(x)h_{il}(x) + \sum_{0\leq i\leq k+m} \sum_{0\leq j<l} g_{k+m-i,l-j}(x)h_{ij}(x)$$

for all k, l. If now we introduce a function ϕ on $\mathbb{N}^2$ as $\phi(i,j) = \alpha i + \beta j$ with α, β in $\mathbb{R}$, then the condition that both $\phi(k-1,l)$ and $\phi(k+m,l-1)$ are less than $\phi(k,l)$ becomes $0 < \alpha m < \beta$. This condition is satisfied by $\alpha = 1$, $\beta = m+1$. We shall use the so-normalized ϕ. We observe that $(*)$ permits us to determine $h_{kl}(x)$ by an

induction on $\phi(k,l)$ for all k,l starting with $h_{00}(x)=1$. Hence $H(x,y)$ and also $a_1(x),\ldots,a_m(x)$ are uniquely derternined. We have thus shown that a solution by formal power series exists and is unique.

We shall show that if $G(x,y)$ is a convergent power series, then the unique $H(x,y)$ is also a convergent power series. As we have seen in section 2.1, if we choose M, $r>0$ suitably, then we will have

$$G(x,y) << G^\circ(x,y) = \sum{}' \left(\frac{M}{r^{p+q}}\right)(x_1+\ldots+x_n)^p y^q,$$

in which the summation is over $\mathbb{N}^2$ and $\sum'$ indicates the restriction $q>m$ for $p=0$. We shall show that the unique $H^\circ(x,y)$ for $G^\circ(x,y)$ gives a dominant series for $H(x,y)$. We shall first make $H^\circ(x,y)$ explicit. If we write

$$G^\circ(x,y) = \sum_{i,j\geq 0} g^\circ_{ij}(x)\left(\frac{y}{r}\right)^i,$$

we will have

$$g^\circ_{ij}(x) = M\left(\frac{x_1+\ldots+x_n}{r}\right)^j$$

with the exception that $g^\circ_{i0}(x)=0$ for all $i\leq m$. Therefore by $(*)$ we get

$$H(x,y) << H^\circ(x,y) = \sum_{i,j\geq 0} h^\circ_{ij}(x)\left(\frac{y}{r}\right)^i,$$

in which

$$\begin{aligned} h^\circ_{kl}(x) &= \delta_0(k)\,\delta_0(l) \\ &+ \left(\frac{M}{r^m}\right)\Big\{\sum_{0\leq i<k} h^\circ_{il}(x) + \sum_{0\leq i\leq k+m}\sum_{0\leq j<l}\left(\frac{x_1+\ldots+x_n}{r}\right)^{l-j} h^\circ_{ij}(x)\Big\} \end{aligned}$$

for all k,l. If we put $\rho = M/r^m$ and $X=(x_1+\ldots+x_n)/r$, then we see by an induction on $\phi(k,l)$ that $h^\circ_{kl}(x) = a_{kl}X^l$, in which

$$(**) \qquad a_{kl} = \delta_0(k)\delta_0(l) + \rho\Big(\sum_{0\leq i<k} a_{il} + \sum_{0\leq i\leq k+m}\sum_{0\leq j<l} a_{ij}\Big)$$

for all k,l. If we put $Y=y/r$, then we have only to show that

$$H^\circ(x,y) = \sum_{i,j\geq 0} a_{ij}X^jY^i$$

is a convergent power series in X,Y.

We shall show that

$$0<a_{kl}\leq \alpha^k\beta^l,$$

in which $\alpha = 2\rho + 1$, $\beta = \alpha^{m+1} + 1$, for all k, l. Since $\phi(k,l) = 0$ implies $k = l = 0$ and since $a_{00} = 1$ by $(**)$, we shall assume that $\phi(k,l) > 0$ and apply an induction on $\phi(k,l)$. Then by $(**)$ we will have

$$\begin{aligned} 0 < a_{kl} \leq \quad & \rho \quad \Big(\sum_{0 \leq i < k} \alpha^i \beta^l + \sum_{0 \leq i \leq k+m} \sum_{0 \leq j < l} \alpha^i \beta^j \Big) \\ = \quad & \frac{1}{2}\big\{(\alpha^k - 1)\beta^l + (\alpha^k - \alpha^{-m-1})(\beta^l - 1)\big\} < \alpha^k \beta^l. \end{aligned}$$

The induction is thus complete. Therefore the series $\sum a_{ij} X^j Y^i$ is convergent for $|X| < \beta^{-1}$ and $|Y| < \alpha^{-1}$.

The rest of the proof is straightforward. If $F(x,y)$ is a convergent power series, so is $G(x,y) = y^m - F(x,y)$, hence also $H(x,y)$ by what we have shown. Since $H(0,0) = 1$, the inverse $E(x,y)$ of $H(x,y)$ is a convergent power series. Also

$$a_1(x)y^{m-1} + \cdots + a_m(x) = F(x,y)H(x,y) - y^m$$

is a convergent power series. If we replace y by distinct c_i in K with small $|c_i|_K$ for $i = 1, \ldots, m$, we get m convergent power series $b_1(x), \ldots, b_m(x)$, and they are K-linear combinations of $a_1(x), \ldots, a_m(x)$. Since up to sign the determinant of the coefficient-matrix is the product of $c_i - c_j$ for all $i < j$, it is different from 0. Therefore $a_1(x), \ldots, a_m(x)$ become K-linear combinations of $b_1(x), \ldots, b_m(x)$, hence they are also convergent power series.

In the case where $K = \mathbb{C}$ the usual proof of Weierstrass' preparation theorem is by Cauchy's integral formula. The proof by Cauchy's calculus of limits is due to H. Späth [53]. At any rate any monic polynomial

$$y^m + a_1(x)y^{m-1} + \ldots + a_m(x),$$

in which the coefficients $a_1(x), \ldots, a_m(x)$ are power series satisfying $a_i(0) = 0$ for all i, is called a *Weierstrass polynomial.*

Corollary 2.3.1 *The ring $K\langle\langle x\rangle\rangle = K\langle\langle x_1, \ldots, x_n\rangle\rangle$ of convergent power series is a unique factorization ring.*

Proof. We put $A_n = K\langle\langle x_1, \ldots, x_n\rangle\rangle$ and denote the leading degree of any $f(x)$ in $A_n \backslash \{0\}$ by $\mathrm{ldeg}(f)$. Then $f(x) = g(x)h(x)$ with $f(x), g(x), h(x)$ in $A_n \backslash \{0\}$ implies $\mathrm{ldeg}(f) = \mathrm{ldeg}(g) + \mathrm{ldeg}(h)$ and $f(x)$ is a unit of A_n if and only if $\mathrm{ldeg}(f) = 0$. Therefore we see that every $f(x)$ in $A_n \backslash \{0\}$ can be expressed as a product of irreducible elements with the number of factors at most equal to $\mathrm{ldeg}(f)$. The problem is to show that the product-decomposition is unique up to a unit. We observe that if $f(x)$ is in $A_1 \backslash \{0\}$, then up to a unit $f(x)$ is equal to x_1^e with $e = \mathrm{ldeg}(f)$. This shows that A_1 is a unique factorization ring. We shall therefore assume that $n > 1$ and apply an induction on n. We take $a(x), b(x), p(x)$ from $A_n \backslash \{0\}$ such that $p(x)$ is irreducible and divides the product $a(x)b(x)$. We have only to show that $p(x)$ then divides either $a(x)$ or $b(x)$. In doing so we may apply any automorphism to A_n

If g is an element of $\mathrm{GL}_n(K)$ with g_{ij} as its (i,j)-entry, then the correspondence $x_i \mapsto y_i = \sum g_{ij}x_j$ gives rise to a K-automorphism of A_n. If $f(x)$ is any element of $A_n\backslash\{0\}$ with $f_m(x)$ as its leading form, since every complete field is infinite, we will have $f_m(a) \neq 0$ for some a in $K^n\backslash\{0\}$. We can then find g in $\mathrm{GL}_n(K)$ with a as its last column. In fact if the k-th entry of a is different from 0, we can take $e_1, \ldots, e_{k-1}, e_{k+1}, \ldots, e_n$, where $e_1 = {}^t(1, 0, \ldots, 0)$, etc., as the first, ..., the $(n-1)$-th columns of g. If in $f(y) = f(gx)$ we put $x_i = 0$ for all $i < n$, then we get $cx_n^m + \ldots$ with $c = f_m(a) \neq 0$. By applying the above observation to $a(x)b(x)p(x)$ as $f(x)$, we may assume that $a(0, x_n)b(0, x_n)p(0, x_n) \neq 0$. Then by Theorem 2.3.1 we may further assume that $a(x)$, $b(x)$, $p(x)$ are Weierstrass polynomials in $B_n = A_{n-1}[x_n]$. We know by induction and by a consequence of Gauss' lemma that B_n is a unique factorization ring. Furthermore a Weierstrass polynomial in B_n is a unit of A_n if and only if it is 1; that a Weierstrass polynomial is irreducible in A_n if and only if it is irreducible in B_n. Therefore $p(x)$ divides either $a(x)$ or $b(x)$.

We remark that if K is any infinite field, the above proof is applicable without any change to $K[[x]] = K[[x_1, \ldots, x_n]]$, hence it is also a unique factorization ring. We might mention that both $K[[x]]$ and $K\langle\langle x\rangle\rangle$ are noetherian rings, and the idea of the proof for $K[[x]]$ is as follows. If $\mathfrak{A}$ is any ideal of $K[[x]]$, then the leading forms of elements of $\mathfrak{A}\backslash\{0\}$ generate an ideal $\mathfrak{a}$ of $K[x]$. If we choose a finite subset I of $\mathfrak{A}\backslash\{0\}$ such that the set of leading forms of its elements forms an ideal basis for $\mathfrak{a}$, then I forms an ideal basis for $\mathfrak{A}$.

2.4 K-analytic manifolds and differential forms

There are two ways to define real-analytic manifolds, one non-intrinsically by "charts" and another intrinsically by "sheaves." The fact is that if K is any complete field, then K-analytic manifolds can be defined in the same way as in the case where $K = \mathbb{R}$. For the sake of completeness, we shall review some basic definitions.

If $x = (x_1, \ldots, x_n)$, where $x_1, \ldots, x_n$ are variables or letters, then by the usual practice x will also be considered as a variable point of K^n. Suppose that U is a nonempty open subset of K^n and $f : U \to K$ is a map. If at every point $a = (a_1, \ldots, a_n)$ of U there exists an element $f_a(x)$ of $K\langle\langle x - a\rangle\rangle = K\langle\langle x_1 - a_1, \ldots, x_n - a_n\rangle\rangle$ such that $f(x) = f_a(x)$ for any variable point x near a, then f is called a K-analytic function on U. As we have seen in section 2.1, such an f is differentiable and all its partial derivatives are K-analytic functions on U. Suppose that U is as above and $f : U \to K^m$ is a map. If every f_i in $f = (f_1, \ldots, f_m)$ are K-analytic functions on U, then f is called a K-analytic map. Let X denote a Hausdorff space and n a fixed nonnegative integer. Then a pair (U, ϕ_U), where U is a nonempty open subset of X and ϕ_U is a bicontinuous map from U to an open subset $\phi_U(U)$ of K^n, is called a chart. Furthermore $\phi_U(x) = (x_1, \ldots, x_n)$ for a variable point x of U are called local coordinates of x. A set of charts $\{(U, \phi_U)\}$ is called an atlas if the union of all U is X and for every U, U' such that $U \cap U' \neq \emptyset$ the map

$$\phi_{U'} \circ \phi_U^{-1} : \phi_U(U \cap U') \to \phi_{U'}(U' \cap U)$$

is K-analytic. Two atlases are considered to be equivalent if their union is also

an atlas. This is an equivalence relation and any equivalence class is called an n-dimensional K-analytic structure on X. If $\{(U, \phi_U)\}$ is an atlas in the equivalence class, we say that X is an n-dimensional K-analytic manifold defined by $\{(U, \phi_U)\}$ or simply an *n-dimensional K-analytic manifold*, and we write $n = \dim(X)$. We observe that every nonempty open subset U of K^n is an n-dimensional K-analytic manifold defined by the atlas consisting of one chart (U, ϕ_U), in which ϕ_U is the inclusion map $U \to K^n$.

Suppose that X, Y are K-analytic manifolds respectively defined by $\{(U, \phi_U)\}$, $\{(V, \psi_V)\}$ and $f : X \to Y$ is a map. If for every U, V such that $U \cap f^{-1}(V) \neq \emptyset$, where $f^{-1}(V)$ is the preimage of V under f, the map

$$\psi_V \circ f \circ \phi_U^{-1} : \phi_U(U \cap f^{-1}(V)) \to K^{\dim(Y)}$$

is K-analytic, then f is called a *K-analytic map*. The K-analyticity of f defined above does not depend on the choice of atlases. We shall not repeat this kind of remark. If $f : X \to Y$, $g : Y \to Z$ are K-analytic maps of K-analytic manifolds, the composite map $g \circ f : X \to Z$ is K-analytic. If $f : X \to K$ is a K-analytic map, it is called a K-analytic function on X. If f is a K-analytic function on X such that $f(a) \neq 0$ at every a in X, then Corollary 2.1.2 shows that $1/f$ is also a K-analytic function on X. If (U, ϕ_U) is a chart on X and $\phi_U(x) = (x_1, \ldots, x_n)$ as above, and f is a K-analytic function on X, then we shall denote $\partial(f \circ \phi_U^{-1})/\partial x_i$ simply by $\partial f/\partial x_i$ for $1 \leq i \leq n$.

If X, Y are K-analytic manifolds respectively defined by $\{(U, \phi_U)\}$, $\{(V, \psi_V)\}$, then $\{(U \times V, \phi_U \times \psi_V)\}$, where $(\phi_U \times \psi_V)(x, y) = (\phi_U(x), \psi_V(y))$ for every (x, y) in $U \times V$, gives an atlas on the product space $X \times Y$. Therefore $X \times Y$ becomes a K-analytic manifold with $\dim(X \times Y) = \dim(X) + \dim(Y)$. We call $X \times Y$ the product manifold of X and Y. Suppose that X is a K-analytic manifold defined by $\{(U, \phi_U)\}$ and Y is a nonempty open subset of X. If for every $U' = Y \cap U \neq \emptyset$ we put $\phi_{U'} = \phi_U \big| U'$, the restriction of ϕ_U to U', then $\{(U', \phi_{U'})\}$ gives an atlas on Y. Therefore Y becomes a K-analytic manifold with $\dim(Y) = \dim(X)$. We call Y an open submanifold of X. Suppose that Y is a nonempty closed subset of an n-dimensional K-analytic manifold X and $0 < p \leq n$ such that an atlas $\{(U, \phi_U)\}$ defining X can be chosen with the following property: If $\phi_U(x) = (x_1, \ldots, x_n)$ and $U' = Y \cap U \neq \emptyset$, then there exist K-analytic functions $F_1, \ldots, F_p$ on U such that firstly U' becomes the set of all x in U satisfying $F_1(x) = \ldots = F_p(x) = 0$ and secondly $\partial(F_1, \ldots, F_p)/\partial(x_1, \ldots, x_p)(a) \neq 0$ at every a in U'. Then by Corollary 2.1.1-(ii) the correspondence $x \mapsto (F_1(x), \ldots, F_p(x), x_{p+1}, \ldots, x_n)$ gives a K-bianalytic map from a neighborhood of a in U to its image in K^n. It follows from this fact that if we denote by V the intersection of such a neighborhood of a and Y, and put $\psi_V(x) = (x_{p+1}, \ldots, x_n)$ for every x in V, then $\{(V, \psi_V)\}$ for all V and for each U above gives an atlas on Y. Therefore Y becomes a K-analytic manifold with $\dim(Y) = n - p$. We call Y a closed submanifold of X, $p = \dim(X) - \dim(Y)$ the codimension of Y in X, and denote p by $\mathrm{codim}_X(Y)$.

We shall define K-analytic differential forms on a K-analytic manifold X. If U, V are neighborhoods of an arbitrary point a of X and f, g are K-analytic functions respectively on U, V such that $f \big| W = g \big| W$ for some neighborhood W of a contained

in U, V, then we say that f, g are equivalent. If we denote by $\mathcal{O}_{X,a}$, or simply by $\mathcal{O}_a$, the set of such equivalence classes, then $\mathcal{O}_a$ becomes a commutative ring containing K. We shall use the same notation for f and its equivalence class. We observe that $f(a)$ is well defined for every f in $\mathcal{O}_a$ and $\mathcal{O}_a$ is a local ring with its maximal ideal $\mathfrak{m}_a$ defined by $f(a) = 0$. Furthermore if (U, ϕ_U) is a chart with U containing a and $\phi_U(x) = (x_1, \dots, x_n)$ as before, then $\mathfrak{m}_a$ has $x_1 - x_1(a), \dots, x_n - x_n(a)$ as its ideal basis, and $\mathcal{O}_a$ becomes isomorphic to $K\langle\langle x - x(a)\rangle\rangle$. We shall use $\mathcal{O}_a$ to define the tangent space $T_a(X)$ of X at a. In order to make the definition accessible, we recall the following fact in calculus.

If $a = (a_1, \dots, a_n)$ is a point of $\mathbb{R}^n$ and $v = (v_1, \dots, v_n)$ is a vector in $\mathbb{R}^n$, then the derivative in the direction v of a differentiable function f at a is defined as

$$\Big(\frac{df(a+tv)}{dt}\Big)(0) = \sum_{1\le i\le n} \big(\frac{\partial f}{\partial x_i}\big)(a)v_i.$$

If we denote the LHS by ∂f, then the operation ∂ is $\mathbb{R}$-linear and

$$(*) \qquad \partial(fg) = (\partial f)g(a) + f(a)(\partial g)$$

for all differentiable functions f, g at a. Furthermore the vector v can be recovered from such a ∂ as $v = (\partial x_1, \dots, \partial x_n)$.

We now define $T_a(X)$ as the vector space over K of K-linear maps $\partial : \mathcal{O}_a \to K$ satisfying $(*)$ for all f, g in $\mathcal{O}_a$ and denote its dual space by $\Omega_a(X)$. We recall that for any vector space E over a field K, its dual space E^* is the vector space over K of all K-linear maps v^* from E to K; we write $v^*(v) = [v, v^*]$ for every v, v^* in V, V^*. We shall show in the present case that $\Omega_a(X)$ can be identified with the factor space $\mathfrak{m}_a/\mathfrak{m}_a^2$ as $[\partial, f + \mathfrak{m}_a^2] = \partial f$ for all ∂ in $T_a(X)$ and f in $\mathfrak{m}_a$. If for any f in $\mathcal{O}_a$ we denote by $(df)_a$ the image of $f - f(a)$ in $\mathfrak{m}_a/\mathfrak{m}_a^2$, then ∂f clearly depends only on ∂ and $(df)_a$. Furthermore if $\phi_U(x) = (x_1, \dots, x_n)$, then $(dx_1)_a, \dots, (dx_n)_a$ form a K-basis for $\mathfrak{m}_a/\mathfrak{m}_a^2$ and $(df)_a$ can be written uniquely as

$$(df)_a = \sum_{1\le i\le n} \big(\frac{\partial f}{\partial x_i}\big)(a)(dx_i)_a.$$

Therefore we have only to observe that the correspondence $f \mapsto (\partial f/\partial x_i)(a)$ defines an element $(\partial/\partial x_i)_a$ of $T_a(X)$ and

$$\partial = \sum_{1\le i\le n} \big(\frac{\partial}{\partial x_i}\big)_a \partial x_i, \qquad \big[\big(\frac{\partial}{\partial x_i}\big)_a, (dx_j)_a\big] = \delta_{ij}$$

for all ∂ in $T_a(X)$ and all i, j. We observe that if $(df_1)_a, \dots, (df_n)_a$ for $f_1, \dots, f_n$ in $\mathcal{O}_a$ are linearly independent, then by Corollary 2.1.1-(ii) there exists a neighborhood V of a in U such that $\psi_V = (f_1, \dots, f_n)$ gives a K-bianalytic map from V to an open subset of K^n. Therefore the addition of (V, ψ_V) to the given atlas $\{(U, \phi_U)\}$ on X will produce an equivalent atlas. We shall apply such a process whenever it becomes necessary. We call $(f_1, \dots, f_n)$ local coordinates of X around a.

We shall use the Grassmann or the exterior algebra of a vector space. We shall briefly recall its definition. In general, if A is a vector space over an arbitrary field K equipped with a K-bilinear multiplication $A \times A \to A$, then A is called a K-algebra. We shall consider, for the time being, only associative K-algebras each with the unit element. If E is a vector space over K, assumed to be finite dimensional, then the exterior algebra $\bigwedge(E)$ of E is the K-algebra generated by E with $v^2 = 0$ for every v in E as its "defining relation." A more precise definition is as follows. If E, E' are vector spaces over K, their tensor product $E \otimes E'$ is the vector space over K with a K-bilinear map $(v, v') \mapsto v \otimes v'$ from $E \times E'$ to $E \otimes E'$ such that $E \otimes E'$ is spanned by the image and $\dim_K(E \otimes E') = \dim_K(E) \dim_K(E')$. If we choose K-bases for E, E', the set of formal products of their members forms a K-basis for $E \otimes E'$. This fact can be used as a non-intrinsic definition of $E \otimes E'$. At any rate, if we denote by $T(E)$ the direct sum of $K, E, E \otimes E$, ... and define a product in $T(E)$ by $\otimes$, then $T(E)$ becomes a K-algebra, and it is called the tensor algebra of E. If $I(E)$ denotes the two-sided ideal of $T(E)$ generated by $v \otimes v$ for all v in E, then $\bigwedge(E)$ is the factor ring $T(E)/I(E)$. If $v_1, \ldots, v_p$ are elements of E, the image of $v_1 \otimes \ldots \otimes v_p$ in $\bigwedge(E)$ is denoted by $v_1 \wedge \ldots \wedge v_p$ and the K-span of such elements by $\bigwedge^p(E)$. We have

$$v \wedge v = 0, \qquad v \wedge v' + v' \wedge v = 0$$

for every v, v' in E. As a vector space $\bigwedge(E)$ is the direct sum of $\bigwedge^p(E)$ for $0 \leq p \leq n$ if $\dim_K(E) = n$, hence $\dim_K(\bigwedge(E)) = 2^n$.

If now we take $\Omega_a(X)$ as E and if $\phi_U(x) = (x_1, \ldots, x_n)$ with U containing a, then we get

$$\bigwedge^p(\Omega_a(X)) = \sum_{i_1 < \ldots < i_p} K\,(dx_{i_1})_a \wedge \ldots \wedge (dx_{i_p})_a;$$

we shall denote it by $\Omega_a^p(X)$ for $0 \leq p \leq n$. We say that α is a differential form of degree p on X if $\alpha(a)$ is in $\Omega_a^p(X)$ for every a in X. If we replace a by a variable point x of U, then we write dx_i, etc. instead of $(dx_i)_x$, etc. A differential form α of degree p on X has a local expression

$$\alpha(x) = \sum_{i_1 < \ldots < i_p} f_{U,i_1 \ldots i_p}(x)\, dx_{i_1} \wedge \ldots \wedge dx_{i_p},$$

in which $f_{U,i_1 \ldots i_p}$ are K-valued functions on U. If they are all K-analytic functions on U for every U, we say that α is a *K-analytic differential form* of degree p on X. In particular, if f is any K-analytic function on X, then df is a K-analytic differential form of degree 1 on X.

If $f : X \to Y$ is a K-analytic map of K-analytic manifolds and β is a K-analytic differential form of degree p on Y, then we get a similar differential form $(\delta f)^*(\beta)$ on X as follows. If a is any point of X and $f(a) = b$, then a K-linear map $\delta_a f : T_a(X) \to T_b(Y)$ is defined as $(\delta_a f)(\partial)(g) = \partial(g \circ f)$ for all g in $\mathcal{O}_{Y,b}$ and its dual map $(\delta_a f)^* : \Omega_b(Y) \to \Omega_a(X)$ is given by

$$(\delta_a f)^*(g + \mathfrak{m}_b^2) = g \circ f + \mathfrak{m}_a^2$$

for all g in $\mathfrak{m}_b$. We observe that $(\delta_a f)^*$ uniquely extends to a K-algebra homomorphism $\bigwedge(\Omega_b(Y)) \to \bigwedge(\Omega_a(X))$. If we write δf instead of $\delta_x f$, then we have

$$(\delta f)^*(\sum g\, dg_1 \wedge \ldots \wedge dg_p) = \sum (g \circ f)\, d(g_1 \circ f) \wedge \ldots \wedge d(g_p \circ f)$$

for all K-analytic functions $g, g_1, \ldots, g_p$ on Y or on its open submanifolds. Therefore if (U, ϕ_U), (V, ψ_V) are charts on X, Y with $\phi_U(x) = (x_1, \ldots, x_n), \psi_V(y) = (y_1, \ldots, y_m)$ satisfying $U' = U \cap f^{-1}(V) \neq \emptyset$ so that

$$\beta(y) = \sum_{j_1 < \ldots < j_p} g_{V,j_1 \ldots j_p}(y)\, dy_{j_1} \wedge \ldots \wedge dy_{j_p}$$

with K-analytic functions $g_{V,j_1 \ldots j_p}$ on V, then we have

$$(\delta f)^*(\beta)(x) = \sum_{j_1 < \cdots < j_p} (g_{V,j_1 \cdots j_p} \circ f)(x)\, d(y_{j_1} \circ f) \wedge \cdots \wedge d(y_{j_p} \circ f)$$

on U'. We shall sometimes write f^* instead of $(\delta f)^*$. In the special case where $\dim(X) = \dim(Y) = p = n$, if we put $g_V = g_{V,1 \ldots n}$, then we simply have

$$f^*(\beta)(x) = g_V(f(x)) \frac{\partial(y_1, \cdots, y_n)}{\partial(x_1, \ldots, x_n)} \cdot dx_1 \wedge \cdots \wedge dx_n.$$

2.5 Critical sets and critical values

Let K denote any complete field and $f : X \to Y$ a K-analytic map of K-analytic manifolds; for every a in X and $b = f(a)$ let $\delta_a f : T_a(X) \to T_b(Y)$, $(\delta_a f)^* : \Omega_b(Y) \to \Omega_a(X)$ denote the corresponding dual K-linear maps. Then a is called a *critical point* of f if $\delta_a f$ is not surjective, i.e., if $(\delta_a f)^*$ is not injective. The set C_f of all critical points of f is called the *critical set* of f. We shall consider the special case where $Y = K$, hence f is a K-analytic function on X. In that case we see that a is a critical point of f if and only if $\delta_a f = 0$, i.e., $(df)_a = 0$. If a is a critical point of f, then $f(a)$ is called a *critical value* of f. We shall denote by V_f the set of all critical values of f. The critical set C_f is an important geometric object associated with f. In the following we shall examine V_f in the case where f is a polynomial function on a vector space X over K. We shall start with a generalization of $T_a(X)$.

Let L denote an extension, i.e., an extension field, of any field F, R a commutative F-algebra, and θ an F-algebra homomorphism from R to L; let $\mathrm{Der}_F(R, L)$ denote the set of all F-linear maps ∂ from R to L satisfying

$$\partial(ab) = (\partial a)(\theta b) + (\theta a)(\partial b)$$

for every a, b in R. Then $\mathrm{Der}_F(R, L)$ forms a vector space over L. We observe that $T_a(X)$ can be written as $\mathrm{Der}_K(\mathcal{O}_a, K)$ with $\theta\varphi = \varphi(a)$ for every φ in $\mathcal{O}_a$. If now θ is injective and S is a multiplicative subset of R free from zero so that θ extends uniquely to $S^{-1}R$, then every ∂ in $\mathrm{Der}_F(R, L)$ extends also uniquely to an element $\partial^\#$ of $\mathrm{Der}_F(S^{-1}R, L)$ as

$$\partial^\#(\frac{a}{b}) = \frac{(\partial a)(\theta b) - (\theta a)(\partial b)}{(\theta b)^2}$$

for every a in R and b in S. The correspondence $\partial \mapsto \partial^{\#}$ gives an L-linear bijection from $\mathrm{Der}_F(R, L)$ to $\mathrm{Der}_F(S^{-1}R, L)$. Therefore we shall denote $\partial^{\#}$ simply by ∂. In particular if R is a finitely generated integral domain over F, i.e., of the form $F[x] = F[x_1, \ldots, x_n]$ with $F(x)$ as its quotient field, we get an L-linear bijection from $\mathrm{Der}_F(F[x], L)$ to $\mathrm{Der}_F(F(x), L)$. We shall make $\mathrm{Der}_F(F[x], L)$ explicit.

We introduce variables $t_1, \ldots, t_n$, put $F[t] = F[t_1, \ldots, t_n]$, and choose an ideal basis I for the kernel of the F-algebra homomorphism $F[t] \to F[x]$ defined by $t_i \mapsto x_i$ for $1 \leq i \leq n$. If $f(t)$ is arbitrary in $F[t]$, $\theta x = a$, i.e., $\theta x_i = a_i$ for all i, and ∂ is in $\mathrm{Der}_F(F[x], L)$, then

$$(*) \qquad \partial f(x) = \sum_{1 \leq j \leq n} \left(\frac{\partial f}{\partial t_j}\right)(a) v_j,$$

in which $v_j = \partial x_j$ for $1 \leq j \leq n$. In particular

$$\partial f_i(x) = \sum_{1 \leq j \leq n} \left(\frac{\partial f_i}{\partial t_j}\right)(a)\, v_j = 0$$

for every $f_i(t)$ in I. Conversely if $v_1, \ldots, v_n$ are elements of L satisfying the above condition, then we can easily verify that $\partial f(x)$ is well defined by $(*)$ and ∂ gives an element of $\mathrm{Der}_F(F[x], L)$.

Lemma 2.5.1 *Let $x_1, \ldots, x_n$ denote elements of an extension field L of a field F such that $x_1, \ldots, x_d$ are algebraically independent over F and $F(x) = F(x_1, \ldots, x_n)$ is separably algebraic over $F(x') = F(x_1, \ldots, x_d)$; define $Der_F(F[x], L)$ by using the inclusion map of $F[x]$ in L as θ. Then the correspondence $\partial \mapsto (\partial x_1, \ldots, \partial x_d)$ gives an L-linear bijection from $Der_F(F[x], L)$ to L^d.*

Proof. Since $F(x)$ is separably algebraic over $F(x')$, we can write $F(x) = F(x', y)$ with y satisfying $f_\circ(y) = 0$ for a unique irreducible monic polynomial $f_\circ(t)$ in $F(x')[t]$, where t is a variable. Since y is a simple root of $f_\circ(t)$, we have $(df_\circ/dt)(y) \neq 0$. By multiplying a common denominator of the coefficients, we can convert $f_\circ(t)$ into a primitive polynomial $f_1(x', t)$ in $F[x'][t] = F[x', t]$. Then by a consequence of Gauss' lemma the kernel of the F-algebra homomorphism $F[x', t] \to F[x', y]$ defined by $x' \mapsto x', t \mapsto y$ is the principal ideal generated by $f_1(x', t)$. Therefore if we denote the coordinates on L^{d+1} by $v_1, \ldots, v_{d+1}$, then by our previous observation the correspondence $\partial \mapsto (\partial x_1, \ldots, \partial x_d, \partial y)$ gives an L-linear bijection from $\mathrm{Der}_F(F[x', y], L)$ to the subspace of L^{d+1} defined by

$$\sum_{1 \leq i \leq d} \left(\frac{\partial f_1}{\partial x_i}\right)(x', y)\, v_i + \left(\frac{\partial f_1}{\partial t}\right)(x', y)\, v_{d+1} = 0,$$

in which $(\partial f_1/\partial t)(x', y) \neq 0$. Since $F(x', y) = F(x)$, we also know that $\mathrm{Der}_F(F[x', y], L)$, $\mathrm{Der}_F(F(x), L)$, $\mathrm{Der}_F(F[x], L)$ all have the same dimension as vector spaces over L. Therefore the correspondence $\partial \mapsto (\partial x_1, \ldots, \partial x_d)$ gives an L-linear bijection from $\mathrm{Der}_F(F[x], L)$ to L^d.

Theorem 2.5.1 *Let F denote a field with $\mathrm{char}(F) = 0$ and $f(t)$ any element of the polynomial ring $F[t] = F[t_1, \ldots, t_n]$; define C_f as the set of all a in F^n satisfying $(\partial f/\partial t_1)(a) = \ldots = (\partial f/\partial t_n)(a) = 0$ and V_f as the set of $f(a)$ for all a in C_f. Then V_f is a finite subset of F.*

Proof. If L is any extension of F, then C_f, V_f can be defined relative to L and they respectively contain the original C_f, V_f. Therefore by extending F we may assume for our purpose that it is algebraically closed. We consider the ideal $\mathfrak{a}$ of $F[t]$ generated by $\partial f/\partial t_1, \ldots, \partial f/\partial t_n$ and take its minimal representation as an intersection of primary ideals:

$$\mathfrak{a} = \sum_{1 \le i \le n} F[t]\,(\frac{\partial f}{\partial t_i}) = \bigcap_{1 \le j \le r} \mathfrak{q}_j.$$

If $r = 0$, hence $\mathfrak{a} = F[t]$, we see that C_f and V_f are empty sets. Therefore we shall assume that $r > 0$, choose $\mathfrak{q} = \mathfrak{q}_j$ and put $\mathfrak{p} = r(\mathfrak{q})$. If we denote by x_i the image of t_i in $F[t]/\mathfrak{p}$, then $F[x] = F[x_1, \ldots, x_n]$ is an integral domain and $(\partial f/\partial t_i)(x) = 0$ for $1 \le i \le n$. We shall show that $x_0 = f(x)$ is in F.

If x_0 is not in F, since F is algebraically closed, it is transcendental over F. Therefore we may assume after a permutation that $x_0, x_1, \ldots, x_d$ for some $d \ge 0$ are algebraically independent over F and $F(x) = F(x_0, x)$ is algebraic, necessarily separable by $\mathrm{char}(F) = 0$, over $F(x_0, x_1, \ldots, x_d)$. Then by Lemma 2.5.1 there exists an element ∂ of $\mathrm{Der}_F(F[x], F(x))$ so that ∂x_0 takes any preassigned value in $F(x)$. On the other hand $x_0 = f(x)$ implies

$$\partial x_0 = \sum_{1 \le i \le n} (\frac{\partial f}{\partial t_i})(x)\,\partial x_i = 0.$$

We thus have a contradiction.

We now take any point $a = (a_1, \ldots, a_n)$ of C_f. Then $t_1 - a_1, \ldots, t_n - a_n$ generate a maximal ideal $\mathfrak{m}$ of $F[t]$ which contains $\mathfrak{a}$. Since the product of $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ is contained in $\mathfrak{a}$, hence in $\mathfrak{m}$, some $\mathfrak{q} = \mathfrak{q}_j$ is contained in $\mathfrak{m}$. Then $\mathfrak{p} = r(\mathfrak{q})$ is contained in $\mathfrak{m}$. Therefore, in the above notation, we get an F-algebra homomorphism $F[x] \to F[a] = F$ as $x_i \mapsto a_i$ for $1 \le i \le n$. Since $x_0 = f(x)$ is in F, this implies $x_0 = f(a)$. Since the number of x_0 is at most equal to r, we get $\mathrm{card}(V_f) \le r$ including the case where $r = 0$.

In the above theorem if we drop the assumption that $\mathrm{char}(F) = 0$, then it becomes false. In fact if $\mathrm{char}(F) = p > 0$ and $f(t) = t_1^p + \ldots + t_n^p$, then $C_f = F^n$. Therefore if F is algebraically closed, then $V_f = F$, which is infinite. On the other hand, if $f(t)$ is homogeneous, then V_f is either an empty set or $\{0\}$ provided that p does not divide $\deg(f)$. This follows immediately from the classical Euler identity

$$\sum_{1 \le i \le n} t_i(\frac{\partial f}{\partial t_i}) = \deg(f) f(t)$$

valid for any homogeneous polynomial $f(t)$.

https://doi.org/10.1090/amsip/014/03

Chapter 3

Hironaka's desingularization theorem

3.1 Monoidal transformations

Hironaka's desingularization is achieved by successive monoidal transformations; they have been known in algebraic geometry for a long time. We just mention O. Zariski's paper [62] which contains a rigorous definition of a general monoidal transformation and its basic properties. We shall explain a monoidal transformation with smooth center following A. Borel and J.-P. Serre [4]. We fix a complete field K and start with a definition of the projective space $P_n(K)$.

We regard two points of $K^{n+1}\backslash\{0\}$ to be equivalent if they differ by a scalar factor in $K^\times$ and denote the set of all equivalence classes by $P_n(K)$. If t is a point of $P_n(K)$, therefore, it is represented by some $(t_1, \dots, t_{n+1})$ in $K^{n+1}\backslash\{0\}$, called the homogeneous coordinates of t. The condition $t_i \neq 0$ on t is independent of the choice of its homogeneous coordinates and defines a subset U_i of $P_n(K)$ for $1 \leq i \leq n+1$. If t is in U_i, then a map $\phi : U_i \to K^n$ is well defined as

$$\phi_i(t) = \left(\frac{t_1}{t_i}, \cdots, \frac{t_{i-1}}{t_i}, \frac{t_{i+1}}{t_i}, \cdots, \frac{t_{n+1}}{t_i}\right).$$

We observe that ϕ_i is a bijection. We shall make the map

$$\phi_j \circ \phi_i^{-1} : \phi_i(U_i \cap U_j) \to \phi_j(U_j \cap U_i)$$

for $i \neq j$ explicit. After a permutation we may assume that $i = 1$ and $j = 2$. Then we will have

$$\phi_1(U_1 \cap U_2) = \phi_2(U_2 \cap U_1) = K^\times \times K^{n-1}.$$

Furthermore if we put $\phi_1(t) = (u_1, \dots, u_n)$, $\phi_2(t) = (v_1, \dots, v_n)$, then $\phi_2 \circ \phi_1^{-1} : K^\times \times K^{n-1} \to K^\times \times K^{n-1}$ is given by

$$(*) \qquad (v_1, v_2, \dots, v_n) = \left(\frac{1}{u_1}, \frac{u_2}{u_1}, \dots, \frac{u_n}{u_1}\right),$$

hence $u_1 = 1/v_1$, $u_2 = v_2/v_1$, $\dots$, $u_n = v_n/v_1$. Therefore the map $\phi_2 \circ \phi_1^{-1}$ is K-bianalytic. In particular if we topologize U_i by the condition that ϕ_i is bicontinuous, then U_i and U_j induce the same topology on $U_i \cap U_j$. We call a subset U of $P_n(K)$

open if and only if $U \cap U_i$ is open in U_i for all i. Then $P_n(K)$ becomes a Hausdorff space. Furthermore, again by $(*)$, we see that $\{(U_i, f_i)\}$ gives an atlas on $P_n(K)$, hence $P_n(K)$ becomes an n-dimensional K-analytic manifold. We keep in mind that the map $K^{n+1}\backslash\{0\} \to P_n(K)$ defined by $(t_1, \dots, t_{n+1}) \mapsto t$ is K-analytic, hence continuous, and its restriction to the subset defined by $\max(|t_1|_K, \dots, |t_{n+1}|_K) = 1$ is surjective.

We now take an n-dimensional K-analytic manifold X and a closed submanifold C with $p = \operatorname{codim}_X(C) \geq 2$, and define the *monoidal transformation* $f : X^\# \to X$ *with center* C. It will have the following properties: Firstly $X^\#$ is also an n-dimensional K-analytic manifold; secondly f is a K-analytic map which induces a K-bianalytic map $X^\#\backslash f^{-1}(C) \to X\backslash C$, where the preimage $f^{-1}(C)$ of C under f is a closed submanifold of $X^\#$ of codimension 1, called the *exceptional divisor* of f; thirdly $f^{-1}(a)$ for every a in C is a closed submanifold of $X^\#$ which is K-bianalytic to $P_{p-1}(K)$. In particular f is surjective. In the special case where C is a point f is often called the *quadratic transformation* with center C.

We take an atlas $\{(U, \phi_U)\}$ on X with $\phi_U(x) = (x_1, \dots, x_n)$ such that if $U \cap C \neq \emptyset$, then it consists of all x in U satisfying $x_1 = \dots = x_p = 0$. We then define for each U an n-dimensional K-analytic manifold $U^\#$ equipped with a K-analytic surjection $f_U : U^\# \to U$ and piece them together to get $X^\#$ and $f : X^\# \to X$ as $f\big|U^\# = f_U$. If $U \cap C = \emptyset$, we simply take $U^\# = U$ and $f_U = \mathrm{id}_U$, the identity map of U. If $U \cap C \neq \emptyset$, then $U^\#$ is the closed subset of $U \times P_{p-1}(K)$ defined as follows: It consists of all (x, t) satisfying $x_i t_j - x_j t_i = 0$ for $1 \leq i < j \leq p$, in which $(t_1, \dots, t_p)$ are the homogeneous coordinates of t. We put $f_U(x, t) = x$. By definition if x is not in C, then t has $(x_1, \dots, x_p)$ as its homogeneous coordinates and $f_U^{-1}(x)$ consists of the single point (x, t) for that t. On the other hand if x is in C, then $f_U^{-1}(x) = x \times P_{p-1}(K)$. After this simple observation, we shall examine $U^\#$ more closely.

We take the open covering of $P_{p-1}(K)$ by V_i defined by $t_i \neq 0$ and introduce local coordinates of t in V_i as

$$(u_1, \dots, u_{p-1}) = \left(\frac{t_1}{t_i}, \dots, \frac{t_{i-1}}{t_i}, \frac{t_{i+1}}{t_i}, \dots, \frac{t_p}{t_i}\right)$$

for $1 \leq i \leq p$. Then we can easily see that $U_i^\# = U^\# \cap (U \times V_i)$ is defined by

$$(**) \qquad x_j = x_i u_j \quad (1 \leq j < i), \qquad x_j = x_i u_{j-1} \quad (i < j \leq p).$$

Therefore if we denote by W_i the image of $\phi_U(U)$ in K^{n-p+1} under the projection $(x_1, \dots, x_n) \mapsto (x_i, x_{p+1}, \dots, x_n)$, then

$$\phi^\#(x, t) = (x_i, x_{p+1}, \dots, x_n, u_1, \dots, u_{p-1})$$

gives a bicontinuous map from $U_i^\#$ to an open subset $\phi_i^\#(U_i^\#)$ of $W_i \times K^{p-1}$. We shall examine $\phi_j^\# \circ (\phi_i^\#)^{-1}$ for $i \neq j$. After a permutation we may assume that $i = 1$ and $j = 2$. Then we will have

$$\phi_1^\#(U_1^\# \cap U_2^\#) \subset W_1 \times K^\times \times K^{p-2}, \qquad \phi_2^\#(U_2^\# \cap U_1^\#) \subset W_2 \times K^\times \times K^{p-2}.$$

Furthermore if $(u_1, \dots, u_{p-1})$ and $(v_1, \dots, v_{p-1})$ are the local coordinates of t respectively in V_1 and V_2, then

$$\phi_2^{\#} \circ (\phi_1^{\#})^{-1} : \phi_1^{\#}(U_1^{\#} \cap U_2^{\#}) \to \phi_2^{\#}(U_2^{\#} \cap U_1^{\#})$$

is given by

$$(x_1, x_{p+1}, \dots, x_n, u_1, u_2, \dots, u_{p-1}) \mapsto \big(x_1 u_1, x_{p+1}, \dots, x_n, \ \frac{1}{u_1}, \frac{u_2}{u_1}, \dots, \frac{u_{p-1}}{u_1}\big).$$

Therefore it is clearly K-analytic. We have thus shown that $\{(U_i^{\#}, f_i^{\#})\}$ gives an atlas on $U^{\#}$, hence it becomes an n-dimensional K-analytic manifold. Also we see by $(**)$ that the map $f_U : U^{\#} \to U$ is K-analytic. Furthermore $f_U^{-1}(U \cap C)$ becomes a closed submanifold of $U^{\#}$ of codimension 1 because we see by $(**)$ that it is defined in each $U_i^{\#}$ by $x_i = 0$. Finally f_U maps $U^{\#} \backslash f_U^{-1}(U \cap C)$ K-bianalytically to $U \backslash (U \cap C)$ because we see again by $(**)$ that on the open subset of U defined by $x_i \neq 0$ the inverse of f_U is given by

$$x \mapsto \big(x_i, x_{p+1}, \dots, x_n, \frac{x_1}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_p}{x_i}\big)$$

for $1 \leq i \leq p$.

We shall construct $X^{\#}$ and $f : X^{\#} \to X$ out of the set $\{(U^{\#}, f_U)\}$ for all U in the atlas $\{(U, f_U)\}$ on X. We take U, U' with $U'' = U \cap U' \neq \emptyset$. If $U'' \cap C = \emptyset$, then f_U, $f_{U'}$ respectively map $f_U^{-1}(U'')$, $f_{U'}^{-1}(U'')$ K-bianalytically to U''. We shall identify the above open subsets of $U^{\#}$, $(U')^{\#}$ by this bijection. If $U'' \cap C \neq \emptyset$, then we shall identify (x, t) in $f_U^{-1}(U'')$ with the (x, t) in $f_{U'}^{-1}(U'')$. This identification is based on the following fact: If $\phi_U(x) = (x_1, \dots, x_n)$, $f_{U'}(x) = (x'_1, \dots, x'_n)$ and $(u_1, \dots, u_{p-1})$ are the local coordinates of t in V_i, then

$$\phi_{U'}^{\#} \circ (\phi_U^{\#})^{-1} : \phi_U^{\#}(U^{\#} \cap (U'' \times V_i)) \to \phi_{U'}^{\#}((U')^{\#} \cap (U'' \times V_i))$$

is given by

$$(x_i, x_{p+1}, \dots, x_n, u_1, \dots, u_{p-1}) \mapsto (x'_i, x'_{p+1}, \dots, x'_n, u_1, \dots, u_{p-1}).$$

Since $x'_1, \dots, x'_n$ are K-analytic functions of $(x_1, \dots, x_n)$, we see by $(**)$ that the above map is K-analytic. Therefore if we define $X^{\#}$ as the union of all $U^{\#}$ and topologize $X^{\#}$ as in the case of $P_n(K)$, then $X^{\#}$ becomes a Hausdorff space and the set of charts defined above gives an atlas on $X^{\#}$. In this way $X^{\#}$ becomes an n-dimensional K-analytic manifold. If finally we define $f : X^{\#} \to X$ as $f\big|U^{\#} = f_U$ for every U, then f becomes a K-analyic map with the properties stated in the beginning.

We add the following remark for our later use. If K is any field with an absolute value $|\cdot|_K$, then for any $\varepsilon > 0$ we define I_ε as the set of all a in K satisfying $|a|_K \leq \varepsilon$. By making ε smaller if necessary, we shall assume that $\varepsilon = |a_0|_K$ for some $a_0$in $K^{\times}$. We observe that K is locally compact if and only if I_1 is compact. This follows from the fact that $a \mapsto a_0^{-1} a$ maps I_ε bicontinuously to I_1. If K is locally compact,

then K is complete. Furthermore all K-analytic manifolds are locally compact. We recall that $P_n(K)$ is a continuous image of the subset of $K^{n+1}\backslash\{0\}$ defined by $\max(|t_1|_K, \ldots, |t_{n+1}|_K) = 1$. Since this subset is compact, $P_n(K)$ is also compact. Therefore if $f : X^{\#} \to X$ is a monoidal transformation, then f is a proper map, i.e., the preimage under f of any compact subset of X is a compact subset of $X^{\#}$.

3.2 Hironaka's desingularization theorem (analytic form)

We shall explain Hironaka's desingularization theorem in his fundamental paper [20]. Actually, we shall do so only in the special case we need and without proof. We start with some preliminary observations and definitions.

Let X denote an n-dimensional K-analytic manifold and E a closed submanifold of X of codimension 1. Then at every point a of E there exist local coordinates $(x_1, \ldots, x_n)$ of X around a such that E is defined locally around a by $x_1 = 0$, i.e., $E \cap U$ for some neighborhood U of a is defined by $x_1 = 0$. We call $x_1 = 0$ or rather x_1 itself a *local equation* of E around a. We may assume that $x_i(a) = 0$ for all i. A characterization of a local equation f of E around a is that f is an element of the local ring $\mathcal{O}_a$ of X at a satisfying $f|E = 0$ and $(df)_a \neq 0$. We shall show that two local equations f and g of E around a differ by a unit of $\mathcal{O}_a$. We have only to show that g divides f in $\mathcal{O}_a$. We may assume that $g = x_1$. We know that $\mathcal{O}_a$ is isomorphic to $K\langle\langle x\rangle\rangle = K\langle\langle x_1, \ldots, x_n\rangle\rangle$ and by Lemma 2.1.2 the image $f(x)$ of f in $K\langle\langle x\rangle\rangle$ can be written uniquely as $f(x) = x_1 f_1(x) + f_2(x')$ with $f_1(x)$ in $K\langle\langle x\rangle\rangle$ and $f_2(x')$ in $K\langle\langle x_2, \ldots, x_n\rangle\rangle$. Since f and x_1 are local equations of E around a, we see that the function f_2 defined by $f_2(x')$ on some neighborhood of 0 in K^{n-1} is 0. Then by Lemma 2.1.3, we get $f_2(x') = 0$, i.e., f is divisible by g in $\mathcal{O}_a$.

Suppose now that we have a set of closed submanifolds E_i of X of codimension 1 for i in an index set I satisfying the following condition: At every point a of X, if $E_{i_1}, \ldots, E_{i_p}$ are all the E_i containing a with respective local equations $f_1, \ldots, f_p$ around a, then $(df_1)_a, \ldots, (df_p)_a$ are linearly independent over K or, equivalently, there exist local coordinates of X around a of the form $(f_1, \ldots, f_p, f_{p+1}, \ldots, f_n)$. In other words all the E_i passing through a "meet transversally" at a. Then we say that the set $\{E_i;\ i \in I\}$ has *normal crossings*. This clearly implies $p \leq n$. Therefore if we denote by $\mathcal{N}$ the *nerve complex* of $\{E_i;\ i \in I\}$ as defined by P. Alexandroff, then the dimension of the simplicial complex $\mathcal{N}$ is at most $n - 1$. We recall that a p-simplex of $\mathcal{N}$ means any set of $p + 1$ elements of $\{E_i;\ i \in I\}$ with nonempty intersection.

We take $f(x)$ from the polynomial ring $K[x_1, \ldots, x_n]$, which we regard as a subring of $K\langle\langle x_1, \ldots, x_n\rangle\rangle$. Then $f(x)$ defines a K-analytic function f on $X = K^n$. We shall assume that $f(x)$ is not in K, i.e., f is not a constant function on X. We shall further assume that $n > 1$. We shall denote by $f^{-1}(0)$ the preimage of $\{0\}$ under f, i.e., the set of zeros of f in X. Also we put

$$f^{-1}(0)_{sing} = f^{-1}(0) \cap C_f,$$

in which C_f is the critical set of f. Then we have the following three possibilities: Firstly $f^{-1}(0) = \emptyset$; secondly $f^{-1}(0) \neq \emptyset$ and $f^{-1}(0)_{sing} = \emptyset$; thirdly $f^{-1}(0)_{sing} \neq \emptyset$. All these cases occur, e.g., for $K = \mathbb{R}$. Simple respective examples are as follows:

$$f(x) = \sum_{1 \leq i \leq n} x_i^2 + 1, \qquad \sum_{1 \leq i \leq n} x_i^2 - 1, \qquad \sum_{1 \leq i \leq p} x_i^2 - \sum_{p < j \leq n} x_j^2 \quad (1 \leq p \leq n).$$

At any rate in the second case $f^{-1}(0)$ becomes a closed submanifold of X of codimension 1 with f as its local equation around every point of $f^{-1}(0)$. In an oversimplified manner we can say that Hironaka's desingularization theorem or rather its consequence gives a method to improve the third case. An exact statement, including the trivial case where $n = 1$, is as follows:

Theorem 3.2.1 *Let K denote a complete field with $char(K) = 0$ and $f(x)$ any element, not in K, of the polynomial ring $K[x_1, \ldots, x_n]$ for $n \geq 1$; put $X = K^n$. Then there exist an n-dimensional K-analytic manifold Y, a finite set $\mathcal{E} = \{E\}$ of closed submanifolds of Y of codimension 1 with a pair of positive integers (N_E, n_E) assigned to each E, and a K-analytic map $h : Y \to X$ satisfying the following conditions: Firstly, h is the composite map of a finite number of monoidal transformations each with a smooth center; secondly,*

$$(f \circ h)^{-1}(0) = \bigcup_{E \in \mathcal{E}} E$$

and h induces a K-bianalytic map

$$Y \backslash h^{-1}(f^{-1}(0)_{sing}) \to X \backslash f^{-1}(0)_{sing};$$

thirdly, at every point b of Y if $E_1, \ldots, E_p$ are all the E in $\mathcal{E}$ containing b with respective local equations $y_1, \ldots, y_p$ around b and $(N_i, n_i) = (N_E, n_E)$ for $E = E_i$, then there exist local coordinates of Y around b of the form $(y_1, \ldots, y_p, y_{p+1}, \ldots, y_n)$ such that

$$f \circ h = \varepsilon \cdot \prod_{1 \leq i \leq p} y_i^{N_i}, \qquad h^*\Big(\bigwedge_{1 \leq i \leq n} dx_i\Big) = \eta \cdot \prod_{1 \leq i \leq p} y_i^{n_i - 1} \cdot \bigwedge_{1 \leq i \leq n} dy_i$$

on some neighborhood of b, in which ε, η are units of the local ring $\mathcal{O}_b$ of Y at b. In particular $\mathcal{E}$ has normal crossings.

We observe that if

$$f^{-1}(0)_{smooth} = f^{-1}(0) \backslash C_f$$

is not empty and if we denote by E' the union of those E not contained in $h^{-1}(f^{-1}(0)_{sing})$, then h gives rise to a K-bianalytic map of $E' \backslash h^{-1}(f^{-1}(0)_{sing})$ to $f^{-1}(0)_{smooth}$. We call E' the *strict transform* of $f^{-1}(0)$ under h. The nerve complex $\mathcal{N}(\mathcal{E})$ of $\mathcal{E}$ with the function $E \mapsto (N_E, n_E)$, called the *numerical data*, on the set of its vertices is an important combinatorial object associated with $f(x)$ or rather $f^{-1}(0)_{sing}$.

3.3 Desingularization of plane curves

We shall outline the classical desingularization of plane curves, i.e., the case $n = 2$ in Theorem 3.2.1, and then explain the details by examples. We take any field F with $\mathrm{char}(F) = 0$ and a polynomial $f(x, y) \neq 0$ in two variables x, y with coefficients in F such that

$$f(0) = \frac{\partial f}{\partial x}(0) = \frac{\partial f}{\partial y}(0) = 0;$$

we have denoted $(0, 0)$ by 0. If $f_m(x, y)$ is the leading form of $f(x, y)$ as an element of $F[[x, y]]$ necessarily for $m \geq 2$, then, as we have seen in Chapter 2.3, we may assume that $f(0, y) = cy^m + \dots$ with c in $F^\times$. We have shown there that $f(x, y)$ differs from a Weierstrass polynomial

$$P_x(y) = y^m + a_1(x)y^{m-1} + \dots + a_m(x)$$

in $F[[x]][y]$ by a unit of $F[[x, y]]$. We shall assume, for the sake of simplicity, that $f(x, y)$ is irreducible in $\Omega[[x, y]]$ for an algebraically closed extension Ω of F. Then $P_x(y)$ is irreducible in $\Omega((x))[y]$. Therefore if η is a zero of $P_x(y)$, then $L = \Omega((x))(\eta)$ is an extension of $\Omega((x))$ of degree m. The fact is that if $x^{1/m}$ is any m-th root of x, then $L = \Omega((x^{1/m}))$. One way to see this is as follows:

We observe that $K = \Omega((x))$ is a complete non-archimedean field with $\mathcal{O}_K = \Omega[[x]]$ and $x\mathcal{O}_K$ as its maximal ideal. Therefore L is also a complete nonarchimedean field and, since $\mathcal{O}_K/x\mathcal{O}_K = \Omega$ is algebraically closed, we will have $\mathcal{O}_L = \Omega[[\pi_L]]$ and $x\mathcal{O}_L = \pi_L^m\mathcal{O}_L$. This follows, e.g., from Proposition 11.6.1. Furthermore, as we have remarked at the end of Chapter 2.1, the m-th power map from $\mathcal{O}_L^\times$ to itself is surjective. Therefore $x^{1/m}$ is in $\mathcal{O}_L$ and $x^{1/m}\mathcal{O}_L = \pi_L\mathcal{O}_L$, hence $\mathcal{O}_L = \Omega[[x^{1/m}]]$ and $L = \Omega((x^{1/m}))$.

Since η is an element of $\mathcal{O}_L$, it becomes a power series in $x^{1/m}$. We write this "Puiseux series" as

$$\eta = \sum_{0<i\leq j_0} a_{0i}x^i + \sum_{0\leq i\leq j_1} a_{1i}x^{(\mu_1+i)/\nu_1} + \sum_{0\leq i\leq j_2} a_{2i}x^{(\mu_2+i)/\nu_1\nu_2} + \dots + \sum_{i\geq 0} a_{gi}x^{(\mu_g+i)/\nu_1\cdots\nu_g},$$

in which the exponents are strictly increasing, $a_{10}a_{20}\cdots a_{g0} \neq 0$, μ_i, ν_i are relatively prime positive integers with $\nu_i > 1$ for $1 \leq i \leq g$, and $\nu_1\nu_2\cdots\nu_g = m$. Furthermore $\mu_1 > \nu_1$. A basic fact is that the g pairs

$$(\mu_1, \nu_1), (\mu_2, \nu_2), \dots, (\mu_g, \nu_g)$$

depend only on the factor ring $\Omega[[x, y]]/\Omega[[x, y]]f(x, y)$ and, to some extent, they determine the ring. At any rate they are called the *characteristic pairs* of the factor ring.

We shall now replace F by a complete field K and put $X = K^2$. We shall assume, for the sake of simplicity, that $f^{-1}(0)_{sing} = \{0\}$. Then there exists a unique shortest sequence of quadratic transformations such that their composition

$h : Y \to X$ has the properties stated in Theorem 3.2.1. We might mention that in the present case $f^{-1}(0)$ is not just $\{0\}$. At any rate we recall that the quadratic transform $X^{\#}$ of X with any point (a, b) of X as its center is covered, up to K-bianalytic maps, by two copies of K^2. More precisely, if (x, y) are the coordinates on X, then $X^{\#}$ is covered by $X_1 = K^2$ with coordinates (x_1, y_1) and $X_1' = K^2$ with coordinates (x_1', y_1') such that the restrictions of the quadratic transformation $X^{\#} \to X$ to X_1, X_1' are given by

$$(x - a, y - b) = (x_1, x_1y_1) = (x_1'y_1', y_1').$$

Therefore the open subsets $K \times K^\times, K^\times \times K$ respectively of X_1, X_1' are identified as $(x_1', y_1') = (1/y_1, x_1y_1)$, $(x_1, y_1) = (x_1'y_1', 1/x_1')$. The exceptional curve of $X^{\#} \to X$ has x_1, y_1' as its local equations in X_1, X_1'. If now we denote by $\mathcal{E}$ the set of all exceptional curves on Y, numbered as $E_1, \ldots, E_T$ by the order of their "creation", and the strict transform E_{T+1} of $f^{-1}(0)$ under h, then T and $(N_I, n_I) = (N_E, n_E)$ where $E = E_I$ for all I can be described by the characteristic pairs. Actually $(N_I, n_I) = (1, 1)$ for $I = T + 1$ is clear.

We shall elaborate on the above statement. If a_0, a_1 are relatively prime positive integers, the Euclid algorithm to find their GCD, which is 1, gives rise to a sequence $k_0, k_1, \ldots, k_t$ in $\mathbb{N}$ as

$$a_0 = k_0a_1 + a_2, \quad a_1 = k_1a_2 + a_3, \quad \ldots, \quad a_{t-1} = k_{t-1}a_t + 1,$$

in which $a_1 > a_2 > \ldots > a_t = k_t > 1$ for some $t > 0$ and $k_1, \ldots, k_{t-1} > 0$. We shall write $a_0/a_1 = [k_0, k_1, \ldots, k_t]$. In this notation we introduce k_{ij} as

$$\mu_i/\nu_i - \mu_{i-1} = [k_{i0}, k_{i1}, \ldots, k_{it_i}],$$

where $\mu_0 = 0$, and put

$$I_i = k_{10} + k_{11} + \ldots + k_{it_i}, \quad m_i = \nu_{i+1} \cdots \nu_g$$

for $1 \le i \le g$. Then $T = I_g = \sum k_{ij}$ and

$$\begin{aligned} \frac{N_{I_i}}{m_i} &= \Big(\frac{N_{I_{i-1}}}{m_{i-1}} + \frac{\mu_i}{\nu_i} - \mu_{i-1}\Big)\nu_i^2, \\ n_{I_i} &= (n_{I_{i-1}} + \frac{\mu_i}{\nu_i} - \mu_{i-1})\nu_i \end{aligned}$$

for $1 \le i \le g$ with the understanding that $(N_{I_0}, n_{I_0}) = (0, 1)$, hence

$$\frac{n_{I_1}}{N_{I_1}} = \frac{\mu_1 + \nu_1}{\mu_1\nu_1 \cdots \nu_g}.$$

Furthermore $n_I/N_I > n_{I_1}/N_{I_1}$ if $I < I_1$ and $n_I/N_I > n_{I_i}/N_{I_i}$ if $I > I_i$ for $1 \le i \le g$, hence n_{I_1}/N_{I_1} is smaller than any other n_I/N_I.

The above-outlined desingularization of $f^{-1}(0)$ is due to F. Enriques and O. Chisini, and it is entirely classical. The exact values of (N_I, n_I) for all I and the fact that n_{I_1}/N_{I_1} is smaller than any other n_I/N_I can be found in [24]. The structure of

$\mathcal{N}(\mathcal{E})$ as a one-dimensional simplicial complex and a beautiful monotonic property of the function $I \mapsto n_I/N_I$ on the set of its vertices as well as relations of (N_I, n_I) for neighboring vertices have later been discovered by L. Strauss [54]. In particular, $\mathcal{N}(\mathcal{E})$ looks exactly like a tree with g branching vertices at E_{I_i} for $1 \le i \le g$. In the following we shall illustrate the situation in two examples.

Example 1. If we take $y^2 - x^3$ as $f(x,y)$, then $f(x,y), \partial f/\partial x, \partial f/\partial y$ all vanish only at 0. Furthermore $f(x,y)$ is irreducible in $\Omega[[x,y]]$, $f(x,y)$ itself is a Weierstrass polynomial, and $\eta = x^{3/2}$ is the Puiseaux series of η. Therefore $(3,2)$ is the only characteristic pair and $3/2 = [1,2]$, hence $T = I_1 = 3$ and $(N_3, n_3) = (6,5)$. We shall verify these and other properties directly without any assumption on $\mathrm{char}(K)$.

We apply a quadratic transformation, abbreviated as QT, to X with 0 as its center. Then in X_1, X_1' we have

$$\begin{aligned} f(x,y) &= x_1^2(y_1^2 - x_1) \ = (y_1')^2(1 - (x_1')^3 y_1'), \\ dx \wedge dy &= x_1 \ dx_1 \wedge dy_1 = y_1' \ dx_1' \wedge dy_1'. \end{aligned}$$

Since the two curves in X_1' with local equations y_1', $1-(x_1')^3 y_1'$ have normal crossings, we apply a QT to X_1 with 0 as its center. Then, by increasing the subscripts by 1, in X_2, X_2' we have

$$\begin{aligned} f(x,y) &= x_2^3(x_2 y_2^2 - 1) = (x_2')^2 (y_2')^3 (y_2' - x_2'), \\ dx \wedge dy &= x_2^2 \ dx_2 \wedge dy_2 = x_2' (y_2')^2 \ dx_2' \wedge dy_2'. \end{aligned}$$

Since the two curves in X_2 with local equations x_2, $x_2 y_2^2 - 1$ have normal crossings, we apply a QT to X_2' with 0 as its center. Then in X_3, X_3' we have

$$\begin{aligned} f(x,y) &= x_3^6 y_3^3 (y_3 - 1) \quad = (x_3')^2 (y_3')^6 (1 - x_3'), \\ dx \wedge dy &= x_3^4 y_3^2 \ dx_3 \wedge dy_3 = x_3' (y_3')^4 \ dx_3' \wedge dy_3'. \end{aligned}$$

We observe that the three curves in X_3 with local equations x_3, $y_3, y_3 - 1$ have normal crossings and the three curves in X_3' with local equations x_3', y_3', $1 - x_3'$ also have normal crossings. Therefore if we denote by Y the union of X_1', X_2, X_3, X_3' and define h on each one of them as the composition of $X_1' \to X$, $X_2 \to X_1 \to X$, $X_3 \to X_2' \to X_1 \to X$, $X_3' \to X_2' \to X_1 \to X$, then $h : Y \to X$ gives a desingularization of $f^{-1}(0)$. We observe that a list of local equations for E_1, E_2, E_3, E_4 is as follows:

$$\begin{aligned} E_1 \ &: \ y_1', x_3'; \qquad E_2 : x_2, y_3; \qquad E_3 : x_3, y_3'; \\ E_4 \ &: \ 1 - (x_1')^3 y_1', \quad x_2 y_2^2 - 1, \quad y_3 - 1, \quad 1 - x_3'. \end{aligned}$$

Therefore $(N_i, n_i) = (2,2), (3,3), (6,5), (1,1)$ for $i = 1,2,3,4$ and $\mathcal{N}(\mathcal{E})$ has three segments, i.e., 1-simplices, joining E_3 to E_1, E_2, E_4.

Example 2. If we put

$$f(x,y) = y^4 - 2x^3 y^2 - 4x^6 y + x^6 - x^9, \qquad \eta = x^{3/2} + x^{9/4},$$

then $f(x,y)$ is a Weierstrass polynomial $P_x(y)$ and $\eta^2 + x^3 = x^{3/2}(2\eta + x^3)$, hence $P_x(\eta) = 0$. Furthermore $\Omega((x))(\eta)$ contains $x^{1/4}$, hence $\Omega((x))(\eta) = \Omega((x^{1/4}))$, and

hence $f(x,y)$ is irreducible in $\Omega[[x,y]]$. By rewriting $f(x,y)$ as $f(x,y) = (x^3 + y^2)^2 - x^3(x^3+2y)^2$ we can easily see that $f^{-1}(0)_{sing}$ consists of all (a,b) satisfying $a^3+b^2 = a^3+2b = 0$, i.e., $(0,0)$ and $(a,2)$ where $a^3 = -4$. If 2 is not a cube in K, e.g., if $K = \mathbb{Q}_2$, therefore, the condition $f^{-1}(0)_{sing} = \{0\}$ is satisfied. We can avoid such an artificial condition if we agree to replace X by a small neighborhood of 0. At any rate $(3,2)$, $(9,2)$ are the characteristic pairs and $3/2 = 9/2-3 = [1,2]$, hence $T = I_2 = 6$ and $(N_3, n_3) = (12,5)$, $(N_6, n_6) = (30,13)$. We shall verify these and other properties directly.

We apply a QT to X with 0 as its center. Then in X_1, X_1' we have

$$\begin{aligned}
f(x,y) &= x_1^4\, f_1(x_1,y_1) = (y_1')^4\ f_1'(x_1',y_1'),\\
dx\wedge dy &= x_1\, dx_1\wedge dy_1 = y_1'\ dx_1'\wedge dy_1',\\
f_1(x,y) &= (y^2-x)^2 - 4x^3y - x^5,\\
f_1'(x,y) &= (x^3y-1)^2 - x^9y^5 - 4x^6y^3.
\end{aligned}$$

We apply a QT to X_1 with 0 as its center. Then in X_2, X_2' we have

$$\begin{aligned}
f(x,y) &= x_2^6\ f_2(x_2,y_2) = (x_2')^4(y_2')^6\ f_2'(x_2',y_2'),\\
dx\wedge dy &= x_2^2\ dx_2\wedge dy_2 = x_2'(y_2')^2\ dx_2'\wedge dy_2',\\
f_2(x,y) &= (1-xy^2)^2 - 4x^2y - x^3,\\
f_2'(x,y) &= (x-y)^2 - x^5y^3 - 4x^3y^2.
\end{aligned}$$

We apply a QT to X_2' with 0 as its center. Then in X_3, X_3' we have

$$\begin{aligned}
f(x,y) &= x_3^{12}y_3^6\, f_3(x_3,y_3) = (x_3')^4(y_3')^{12}\, f_3'(x_3',y_3'),\\
dx\wedge dy &= x_3^4y_3^2\, dx_3\wedge dy_3 \ = x_3'(y_3')^4\, dx_3'\wedge dy_3',\\
f_3(x,y) &= (1-y)^2 - x^6y^3 - 4x^3y^2,\\
f_3'(x,y) &= (x-1)^2 - x^5y^6 - 4x^3y^3.
\end{aligned}$$

We apply a QT to X_3' with $(1,0)$ as its center. Since $(1,0)$ in X_3' and $(0,1)$ in X_3 represent the same point, we could have applied a QT to X_3 with $(0,1)$ as its center. At any rate in X_4, X_4' we have

$$\begin{aligned}
f(x,y) &= (1+x_4)^4x_4^{14}y_4^{12}\, f_4(x_4,y_4)\\
&= (1+x_4'y_4')^4(y_4')^{14}\, f_4'(x_4',y_4'),\\
dx\wedge dy &= (1+x_4)x_4^5y_4^4\, dx_4\wedge dy_4\\
&= (1+x_4'y_4')(y_4')^5\, dx_4'\wedge dy_4',\\
f_4(x,y) &= 1 - 4(1+x)^3xy^3 - (1+x)^5x^4y^6,\\
f_4'(x,y) &= x^2 - 4(1+xy)^3y - (1+xy)^5y^4.
\end{aligned}$$

We apply a QT to X_4' with 0 as its center. Then in X_5, X_5' we have

$$\begin{aligned}
f(x,y) &= (1+x_5^2y_5)^4x_5^{15}y_5^{14}\,f_5(x_5,y_5)\\
&= (1+x_5'(y_5')^2)^4(y_5')^{15}\,f_5'(x_5',y_5'),\\
dx\wedge dy &= (1+x_5^2y_5)x_5^6y_5^5\,dx_5\wedge dy_5\\
&= (1+x_5'(y_5')^2)(y_5')^6\,dx_5'\wedge dy_5',\\
f_5(x,y) &= x-4(1+x^2y)^3y-(1+x^2y)^5x^3y^4,\\
f_5'(x,y) &= x^2y-4(1+xy^2)^3-(1+xy^2)^5y^3.
\end{aligned}$$

We apply a QT to X_5 with 0 as its center. Then in X_6, X_6' we have

$$\begin{aligned}
f(x,y) &= (1+x_6^3y_6)^4x_6^{30}y_6^{14}\,f_6(x_6,y_6)\\
&= (1+(x_6')^2(y_6')^3)^4(x_6')^{15}(y_6')^{30}\,f_6'(x_6',y_6'),\\
dx\wedge dy &= (1+x_6^3y_6)x_6^{12}y_6^5\,dx_6\wedge dy_6\\
&= (1+(x_6')^2(y_6')^3)(x_6')^6(y_6')^{12}\,dx_6'\wedge dy_6',\\
f_6(x,y) &= 1-4(1+x^3y)^3y-(1+x^3y)^5x^6y^4,\\
f_6'(x,y) &= x-4(1+x^2y^3)^3-(1+x^2y^3)^5x^3y^6.
\end{aligned}$$

If we denote by Y the union of X_1', X_2, $X_3\setminus\{(0,1)\}$, X_4, X_5', X_6, X_6' and define h on each one of them as the composition of $X_1'\to X, X_2\to X_1\to X$, …, $X_6'\to X_5\to X_4'\to X_3'\to X_2'\to X_1\to X$, then $h:Y\to X$ gives a desingularization of $f^{-1}(0)$. In fact, a list of local equations for E_1, E_2, …, E_7 is as follows:

$$\begin{array}{lcl}
E_1 & : & y_1',\quad 1+x_4,\quad 1+x_5'(y_5')^2,\quad 1+x_6^3y_6,\quad 1+(x_6')^2(y_6')^3;\\
E_2 & : & x_2,\quad y_3;\qquad E_3: x_3,\quad y_4;\qquad E_4: x_4,\quad y_6;\qquad E_5: y_5',\quad x_6';\\
E_6 & : & x_6,\quad y_6';\qquad E_7: f_1',\quad f_2,\quad f_3,\quad f_4,\quad f_5',\quad f_6,\quad f_6',
\end{array}$$

in which f_i, f_i' are $f_i(x_i,y_i)$, $f_i'(x_i',y_i')$ for all i. We can easily verify that $\mathcal{E}=\{E_1,E_2,\dots,E_7\}$ has normal crossings. Therefore

$$(N_i,n_i)=(4,2),(6,3),(12,5),(14,6),(15,7),(30,13),(1,1)$$

for $i=1,2,\dots,7$ and $\mathcal{N}(\mathcal{E})$ has six segments joining E_3 to E_1, E_2, E_4 and E_6 to E_4, E_5, E_7.

https://doi.org/10.1090/amsip/014/04

Chapter 4

Bernstein's theory

4.1 Bernstein's polynomial $b_f(s)$

We take a field K with $\mathrm{char}(K) = 0$ and the polynomial ring $K[x] = K[x_1, \ldots, x_n]$ for some $n > 0$. The formal differentiation $\partial/\partial x_i$ in $K[x]$ uniquely extends to an element, also denoted by $\partial/\partial x_i$, of $\mathrm{Der}_K(K(x), K(x))$ for $1 \leq i \leq n$. We shall denote by D_n or simply by D the K-subalgebra of $\mathrm{End}_K(K(x))$, the K-algebra of all K-linear transformations in $K(x)$, generated by the multiplication by x_i and $\partial/\partial x_i$ for all i. Furthermore, by an abuse of notation, we shall write $D = K[x, \partial/\partial x]$. The $2n$ generators of D satisfy the following *Heisenberg commutation relation*:

$$x_i x_j - x_j x_i = 0, \quad (\partial/\partial x_i)(\partial/\partial x_j) - (\partial/\partial x_j)(\partial/\partial x_i) = 0,$$
$$x_i(\partial/\partial x_j) - (\partial/\partial x_j)x_i + \delta_{ij} = 0$$

for $1 \leq i, j \leq n$. Such a commutation relation indeed appeared in quantum mechanics, cf., e.g., H. Weyl [59], p. 83 and its footnote 20, and D is sometimes called the *Weyl algebra*. We shall show that D is an associative K-algebra with the unit element generated by x_i, $\partial/\partial x_i$ for $1 \leq i \leq n$ with the Heisenberg commutation relation as its defining relation.

Lemma 4.1.1 *Let E denote a $2n$-dimensional vector space over K with a basis $\xi_1, \ldots, \xi_n, \eta_1, \ldots, \eta_n$ and $T(E)$ the tensor algebra of E; let $I(E)$ denote the two-sided ideal of $T(E)$ generated by*

$$\xi_i \otimes \xi_j - \xi_j \otimes \xi_i, \quad \eta_i \otimes \eta_j - \eta_j \otimes \eta_i, \quad \xi_i \otimes \eta_j - \eta_j \otimes \xi_i + \delta_{ij}$$

for all i, j. Then the K-algebra homomorphism $\theta : T(E) \to D_n$ defined by $\xi_i \mapsto x_i$, $\eta_i \mapsto \partial/\partial x_i$ for $1 \leq i \leq n$ gives rise to a K-algebra isomorphism from $T(E)/I(E)$ to D_n.

Proof. If ξ is any element of E, we denote its p-th power in $T^p(E) = E \otimes \ldots \otimes E$ by $\xi^{\otimes p}$. Every element w of $T(E)$ determines $d = d_w$ as the smallest $d \geq 0$ such that w is contained in the direct sum of $T^p(E)$ for $p \leq d$. Now by an induction on d_w we see that w can be expressed in the form

$$w = \sum c_{ij} \xi_1^{\otimes i_1} \otimes \ldots \otimes \xi_n^{\otimes i_n} \otimes \eta_1^{\otimes j_1} \otimes \ldots \otimes \eta_n^{\otimes j_n} + z$$

with c_{ij} in K, z in $I(E)$, and i, j in $\mathbb{N}^n$, and we get

$$\theta(w) = \sum c_{ij} x^i \, (\partial/\partial x)^j \,, \quad x^i = x_1^{i_1} \dots x_n^{i_n}, \quad \text{etc.}$$

Since for a similar reason every element of D can be written in the above form, the homomorphism θ is surjective. Therefore we have only to show that $\theta(w) = 0$ implies $c_{ij} = 0$ for all i, j. Suppose otherwise and choose $c_{ij} \neq 0$ with the smallest $|j| = j_1 + \ldots + j_n$. Then

$$\theta(w)x^j = \sum_i j! \; c_{ij} \; x^i,$$

in which $j! = j_1! \dots j_n! \neq 0$ by the assumption that $\mathrm{char}(K) = 0$. Therefore LHS $= 0$ while RHS $\neq 0$. We thus have a contradiction.

We shall consider D-modules. In general if A is any associative K-algebra with the unit element, then a vector space M over K is an A-module, more precisely a left A-module, if and only if there exists a K-algebra homomorphism $\theta : A \to \mathrm{End}_K(M)$. In that case $a \cdot \varphi$, or simply $a\varphi$, is defined as $\theta(a)\varphi$ for every (a, φ) in $A \times M$. We observe that $K(x)$ is a D-module and so is $K[x]$ because it is stable, i.e., mapped to itself, under the operations of D. We change our notation to introduce the kind of D-modules which we shall closely examine. We replace the above K by K_0, denote by s another variable in addition to $x_1, \dots, x_n$, and put $K = K_0(s)$. The Weyl algebra D will be relative to this K. We take an element $f(x)$ of $K_0[x]\backslash\{0\}$, denote by S the multiplicative subset of $K_0[x]$ generated by $f(x)$, and put

$$K[x]_f = S^{-1}K[x] = K_0(s)[x_1, \dots, x_n, 1/f(x)].$$

This can be converted into a D-module as follows.

In the notation of Lemma 4.1.1 we first convert $K[x]_f$ into a $T(E)$-module as

$$\xi_i \cdot \varphi(x) = x_i\varphi(x), \quad \eta_i \cdot \varphi(x) = \partial\varphi/\partial x_i + s\varphi(x)(\partial f/\partial x_i)/f(x)$$

for $1 \leq i \leq n$. We observe that $K[x]_f$ is stable under the operations of $T(E)$. Therefore we have only to show that the $3n^2$ generators of the ideal $I(E)$ annihilate every $\varphi(x)$ in $K[x]_f$. This can be done by formal computations. We shall do it by using the following obvious lemma:

Lemma 4.1.2 *Let $a_0, a_1, a_2, \dots$ denote a finite number of elements of any field F with $\mathrm{char}(F) = 0$ satisfying $a_0 + a_1 s + a_2 s^2 + \ldots = 0$ for infinitely many s in $\mathbb{Z}$. Then $a_i = 0$ for all i.*

Now the verification goes as follows: Let w denote any one of the above $3n^2$ elements, $\varphi(x)$ any element of $K[x]_f$ and express it as $\varphi_0(x)/d(s)$ with $\varphi_0(x)$ in $K_0[s, x_1, \dots, x_n, 1/f(x)]$ and $d(s)$ in $K_0[s]\backslash\{0\}$. Then we will have

$$w \cdot \varphi(x) = \frac{a_0 + a_1 s + a_2 s^2 + \dots}{d(s)}$$

with $a_0, a_1, a_2, \dots$ in $K_0(x)$. On the other hand, if we replace s by any element of $\mathbb{Z}$ other than the zeros of $d(s)$ so that $f(x)^s$ becomes the actual s-th power of $f(x)$, then we will have

$$(\xi_i \cdot \varphi(x))f(x)^s = x_i\varphi(x)f(x)^s, \quad (\eta_i \cdot \varphi(x))f(x)^s = \partial(\varphi(x)f(x)^s)/\partial x_i$$

for $1 \leq i \leq n$. Therefore $a_0 + a_1 s + a_2 s^2 + \ldots = 0$ for all such s, hence $a_i = 0$ for all i, and hence $w \cdot \varphi(x) = 0$. We have thus shown that $K[x]_f$ is a D-module. In the above notation Bernstein's theorem can be stated as follows:

Theorem 4.1.1 *There exists an element P_0 of D_n satisfying $P_0 \cdot f(x) = 1$.*

This is a fundamental theorem in the theory of local zeta functions, and it was proved by I. N. Bernstein [3]. Later in this chapter we shall explain his original proof. In the following we shall make a few preliminary remarks. If we multiply an element $b(s)$ of $K_0[s]\backslash\{0\}$ to both sides of $P_0 \cdot f(x) = 1$, then we will have

$$(*) \qquad P \cdot f(x) = b(s),$$

in which P is a "polynomial" $P(s, x, \partial/\partial x)$ in $s, x_1, \ldots, x_n, \partial/\partial x_1, \ldots, \partial/\partial x_n$ with coefficients in K_0. If we replace s by any element of $\mathbb{Z}$, then $(*)$ becomes

$$P(s, x, \partial/\partial x) f(x)^{s+1} = b(s) f(x)^s.$$

At any rate, the set of all such polynomials $b(s)$ and 0 forms an ideal in $K_0[s]$, which is a principal ideal ring. A monic polynomial $b(s)$ of the smallest degree is a generator of this ideal, and it is uniquely determined by $f(x)$ and K_0. We shall denote it by $b_f(s)$ and call $b_f(s)$ the *Bernstein polynomial* of $f(x)$. In the special case where

$$f(x) = x_1^2 + \ldots + x_n^2,$$

if Δ denotes the Laplacian $\sum(\partial/\partial x_i)^2$, then we will have

$$\Delta \cdot f(x) = 4(s+1)(s+n/2),$$

hence $b_f(s)$ is a factor of $(s+1)(s+n/2)$. We shall see later that they are actually equal. This case is classical. In the middle 60's M. Sato proved a similar statement for a large class of $f(x)$ in his theory of prehomogeneous vector spaces. We shall explain a part of this theory in Chapter 6.

4.2 Some properties of $b_f(s)$

Before we start with the proof of Theorem 4.1.1, we shall prove five elementary properties of $b_f(s)$. All proofs are straightforward, and they could have been left as exercises.

(i) If the Bernstein polynomial of $f(x)$ exists for an extension K_0' of K_0, then it also exists for K_0, and they are equal.

In fact let $b_f'(s)$ denote the Bernstein polynomial of $f(x)$ relative to K_0' and $P' \cdot f(x) = b_f'(s)$ for P' in $K_0'[s, x, \partial/\partial x]$; choose a K_0-basis $\{w_\alpha\}$ for K_0' and write

$$P' = \sum P_\alpha w_\alpha, \quad b_f'(s) = \sum b_\alpha(s) w_\alpha,$$

in which P_α is in $K_0[s, x, \partial/\partial x]$ and $b_\alpha(s)$ is in $K_0[s]$ for all α. Then we get $P_\alpha \cdot f(x) = b_\alpha(s)$ for all α with $b_\alpha(s) \neq 0$ for at least one α. Hence the Bernstein

polynomial $b_f(s)$ relative to K_0 exists and clearly $b_f(s) = b'_f(s)c'(s)$ for some $c'(s)$ in $K'_0[s]$. On the other hand, $b_\alpha(s) = b_f(s)c_\alpha(s)$ for some $c_\alpha(s)$ in $K_0[s]$ for all α. By putting these together we get

$$\Big(\sum c_\alpha(s)w_\alpha\Big)\, c'(s) = 1.$$

Since $c'(s) = b_f(s)/b'_f(s)$ is a monic polynomial, this implies $c'(s) = 1$, hence $b_f(s) = b'_f(s)$.

(ii) If the Bernstein polynomial of $f(x)$ exists and if $f'(x')$ is obtained from $f(x)$ by an invertible K_0-linear transformation $x \mapsto x'$, then the Bernstein polynomial of $f'(x')$ also exists, and they are equal.

The proof is as follows: We denote by x, $\partial/\partial x$, etc. the column vectors with x_i, $\partial/\partial x_i$, etc. as their i-th entries and put $x' = g^{-1}x$ for any g in $\mathrm{GL}_n(K_0)$. Then $\partial/\partial x = ({}^t g^{-1})\partial/\partial x'$. Therefore if we put $f'(x') = f(x) = f(gx')$ and assume that $P(s, x, \partial/\partial x) \cdot f(x) = b_f(s)$, then we get

$$P(s, gx', ({}^t g^{-1})\partial/\partial x') \cdot f'(x') = b_f(s).$$

Therefore $b_{f'}(s)$ exists, and it divides $b_f(s)$. The situation is now symmetric and $b_f(s)$ divides $b_{f'}(s)$, hence they are equal.

(iii) If c is in $K_0^\times$ and if $b_f(s)$ exists, then $b_{cf}(s)$ also exists, and they are equal.

This follows immediately from the fact that each one of $x_i \cdot \varphi$, $\partial/\partial x_i \cdot \varphi$ for every φ in $K[x]_f = K[x]_{cf}$ relative to $f(x)$ and $cf(x)$ are equal.

(iv) If $f(x)$ is in $K_0^\times$, then $b_f(s) = 1$ while if $f(x)$ is in $K_0[x]\backslash K_0$ and $b_f(s)$ exists, then it is divisible by $s + 1$.

Since the first part is clear, we shall prove the second part. Suppose that $b_f(s)$ exists for some $f(x)$ in $K_0[x]\backslash K_0$ and that $P(s, x, \partial/\partial x) \cdot f(x) = b_f(s)$. Then we will have

$$P(s, x, \partial/\partial x) f(x)^{s+1} = b_f(s) f(x)^s$$

for every s in $\mathbb{Z}$, in particular for $s = -1$. We observe that for $s = -1$ the LHS is in $K_0[x]$ while the RHS is $b_f(-1)/f(x)$, and $1/f(x)$ is not in $K_0[x]$. This implies $b_f(-1) = 0$, hence $b_f(s)$ is divisible by $s + 1$.

(v) Suppose that $f(x)$ is in $K_0[x]\backslash K_0$ and there is no point a in Ω^n, where Ω is any algebraically closed extension of K_0, satisfying

$$f(a) = \frac{\partial f}{\partial x_1}(a) = \ldots = \frac{\partial f}{\partial x_n}(a) = 0.$$

Then $b_f(s) = s + 1$.

This can be proved as follows: By Hilbert's Nullstellensatz there exist $a_0(x)$, $a_1(x), \ldots, a_n(x)$ in $K_0[x]$ satisfying

$$a_0(x)f(x) + \sum_{1 \le i \le n} a_i(x)\frac{\partial f}{\partial x_i} = 1.$$

Define P as

$$P = (s+1)a_0(x) + \sum_{1 \le i \le n} a_i(x)\ \partial/\partial x_i.$$

Then we have $P \cdot f(x) = s+1$. Since we have seen in (iv) that $b_f(s)$, if it exists, is divisible by $s+1$, we get $b_f(s) = s+1$.

If we take, e.g., $\mathbb{C}$ as K_0 and $f(x)$ from $\mathbb{C}[x]\backslash\mathbb{C}$, then we see by (iv), (v) that $b_f(s)/(s+1) \neq 1$ implies $f^{-1}(0)_{sing} \neq \emptyset$. In a certain sense the size of $b_f(s)/(s+1)$ corresponds to the complexity of $f^{-1}(0)_{sing}$. We might recall that to simplify $f^{-1}(0)_{sing}$ or, more precisely, to replace $f^{-1}(0)$ by the union of closed submanifolds of codimension 1 with normal crossings is one of the main objectives of desingularization. We shall determine $b_f(s)$ for an $f(x)$ such that $f^{-1}(0)$ itself has such a simple structure. Namely, we shall prove the following statement:

If $f(x) = x_1^{m_1} \dots x_n^{m_n}$, where m_i is in $\mathbb{N}$ for every i, then

$$b_f(s) = \prod_{1 \leq i \leq n} \prod_{1 \leq j \leq m_i} (s + j/m_i)$$

with the understanding that the i-th factor represents 1 for $m_i = 0$.

Since the general case can be reduced to the case where $n = 1$ by using multi-indices, we shall assume that $n = 1$ and we drop the subscripts, hence $f(x) = x^m$, etc.; we shall write d/dx instead of $\partial/\partial x$ and exclude the trivial case where $m = 0$. We see by an induction on $p \geq 0$ that

$$(d/mdx)^p \cdot x^q = (\prod_{0 \leq j < p} (s + (q-j)/m)) x^{q-p}$$

for every q in $\mathbb{Z}$. Therefore if we put

$$b(s) = \prod_{0 \leq j < m} (s + (m-j)/m) = \prod_{1 \leq j \leq m} (s + j/m),$$

then we get

$$(d/mdx)^m \cdot f(x) = b(s),$$

hence $b_f(s)$ divides $b(s)$. On the other hand, if P is in $K_0[s, x, d/dx]$ and $P \cdot f(x) = b_f(s)$, then by expressing P as

$$P = \sum_{i,j \geq 0} c_{ij}(s) x^i (d/mdx)^j$$

with $c_{ij}(s)$ in $K_0[s]$ we also get

$$\sum_{i \geq 0} c_{i,m+i}(s) \prod_{0 \leq j < m+i} (s + (m-j)/m) = b_f(s).$$

This shows that $b(s)$ divides $b_f(s)$, hence $b_f(s) = b(s)$.

4.3 Reduction of the proof

We shall translate Theorem 4.1.1 into an equivalent statement and proceed to its proof. In the following lemma $\Phi(s)|_{s \mapsto s-r}$ for any function $\Phi(s)$ means $\Phi(s-r)$.

Lemma 4.3.1 *If $\varphi(s,x)$ is in $K[x]_f = K_0(s)[x, 1/f(x)]$ and $P(s,x,\partial/\partial x)$ is in D_n, then for every r in $\mathbb{Z}$ we have*

$$P(s,x,\partial/\partial x)\cdot f(x)^{-r}\varphi(s,x) = f(x)^{-r}(P(s+r,x,\partial/\partial x)\cdot\varphi(s+r,x))|_{s\mapsto s-r}.$$

Proof. We first observe that the formula is valid in the special cases where $P(s,x,\partial/\partial x) = x_i$, $\partial/\partial x_i$ for $1 \le i \le n$. Furthermore if the formula is valid for P_1, P_2 in $D = D_n$, then it is valid for $c_1P_1 + c_2P_2$ for any c_1, c_2 in $K = K_0(s)$. Therefore we have only to show that the formula is valid also for $P_3 = P_1P_2$, and the proof is as follows: If we put

$$\varphi'(s,x) = P_2(s+r,x,\partial/\partial x)\cdot\varphi(s+r,x),$$

then

$$\begin{aligned} P_3(s,x,\partial/\partial x)\cdot f(x)^{-r}\varphi(s,x) &= P_1(s,x,\partial/\partial x)\cdot f(x)^{-r}\varphi'(s-r,x) \\ &= f(x)^{-r}\left\{(P_1(s+r,x,\partial/\partial x)\cdot\varphi'(s,x))|_{s\mapsto s-r}\right\} \\ &= f(x)^{-r}\left\{(P_3(s+r,x,\partial/\partial x)\cdot\varphi(s+r,x))|_{s\mapsto s-r}\right\}. \end{aligned}$$

Proposition 4.3.1 *Theorem 4.1.1 holds if and only if the D-module $K[x]_f$ is finitely generated.*

Proof. We shall, for the sake of simplicity, write $f, \varphi(s), P(s)$ instead of $f(x)$, $\varphi(s,x)$, $P(s,x,\partial/\partial x)$. We then have

$$\begin{aligned} D\cdot f^{-r+1} &= D\cdot(f\cdot f^{-r}) = Df\cdot f^{-r} \subset D\cdot f^{-r}, \\ D\cdot f^{-r} &\supset K[x]\cdot f^{-r} = K[x]f^{-r} \end{aligned}$$

for $r = 0, 1, 2, \ldots$, hence

$$D\cdot 1 \subset D\cdot f^{-1} \subset D\cdot f^{-2}\ldots, \quad \bigcup_{r\ge 0} D\cdot f^{-r} = K[x]_f.$$

Suppose now that $K[x]_f$ is generated as a D-module by a finite subset S of $K[x]_f$ and choose r large enough so that $D\cdot f^{-r+1}$ contains S. Then $K[x]_f = D\cdot f^{-r+1}$, hence $f^{-r} = P(s)\cdot f^{-r+1}$ for some $P(s)$ in D. Lemma 4.3.1 then shows that $P(s+r)\cdot f = 1$. Conversely suppose that $P_0\cdot f = 1$ for some $P_0 = P(s)$ in D. Then by Lemma 4.3.1 we get

$$P(s-1)\cdot 1 = f^{-1}, \quad P(s-2)\cdot f^{-1} = f^{-2}, \ldots,$$

hence $K[x]_f = D\cdot 1$.

In general if K is an arbitrary field, A is a K-algebra, which is associative and with the unit element, and M is an A-module, then the finite generation problem of M as an A-module can sometimes be investigated by converting A and M into a filtered K-algebra and a filtered A-module, and then passing to the corresponding graded $G(A)$-module $G(M)$. In the present case, as we shall see, this method works perfectly.

We have already used graded algebras and modules to prove the existence of Hilbert's functions in Chapter 1.3. If a K-algebra A contains an increasing sequence of subspaces $F_0(A), F_1(A), F_2(A), \ldots$ with A as their union satisfying

$$F_i(A)F_j(A) \subset F_{i+j}(A)$$

for all i, j, then A is called a *filtered K-algebra*. If an A-module M contains an increasing sequence of subspaces $F_0(M), F_1(M), F_2(M), \ldots$ with M as their union satisfying

$$F_i(A)F_j(M) \subset F_{i+j}(M)$$

for all i, j, then M is called a *filtered A-module*. In particular A itself is a filtered A-module. We put $F_r(M) = \{0\}$ for $r < 0$ and call $\{F_r(M)\}$ a *filtration* of M. If M is a graded A-module, where A is a graded K-algebra, and if we put $F_r(M) = M_0 + \ldots + M_r$, etc., as we have done in Chapter 1.3, then A becomes a filtered K-algebra and M a filtered A-module. Conversely, if M is a filtered A-module, where A is a filtered K-algebra, and if we put $G_r(M) = F_r(M)/F_{r-1}(M)$, etc., then the direct sum $G(M)$ of $G_r(M)$ for all r becomes a graded module over the graded K-algebra $G(A)$.

Proposition 4.3.2 *If M is a filtered A-module such that the $G(A)$-module $G(M)$ is finitely generated, then the A-module M is finitely generated.*

Proof. By assumption there exists a finite subset $\{\psi_1, \ldots, \psi_k\}$ of $G(M)$ such that $G(M) = G(A)\psi_1 + \ldots + G(A)\psi_k$. After expressing each ψ_i as a finite sum of homogeneous elements, we may assume that ψ_i itself is homogeneous, i.e., in $G_{r_i}(M)$ for some r_i in $\mathbb{N}$. We shall show that if we choose φ_i from $F_{r_i}(M)$ with ψ_i as its image in $G_{r_i}(M)$, then we will have

$$F_r(M) = F_{r-r_1}(A)\varphi_1 + \ldots + F_{r-r_k}(A)\varphi_k$$

for all r in $\mathbb{N}$. That will imply $M = \sum A\varphi_i$. If we denote the RHS by $F'_i(M)$, then clearly $F_r(M) \supset F'_r(M)$ for all r. Therefore we have only to show that $F_r(M) \subset F'_r(M)$ also for all r. Since $F_{-1}(0) = 0$, this is clear for $r = -1$. Therefore we shall apply an induction on r assuming that $F_{r-1}(M) \subset F'_{r-1}(M)$, hence $F_{r-1}(M) = F'_{r-1}(M)$, for some $r \geq 0$. We take φ arbitrarily from $F_r(M)$ and denote its image in $G_r(M)$ by ψ. Then we have $\psi = b_1\psi_1 + \ldots + b_k\psi_k$ for some b_i in $G_{r-r_i}(A)$ for all i. If we choose a_i from $F_{r-r_i}(A)$ with b_i as its image in $G_{r-r_i}(A)$, then $\varphi - \sum a_i\varphi_i$ is in $F_{r-1}(M)$. Therefore φ is in

$$F_{r-1}(M) + F'_r(M) = F'_{r-1}(M) + F'_r(M) = F'_r(M).$$

The induction is complete and the proposition is proved.

In view of the above proposition, we shall convert D into a filtered K-algebra and $M = K[x]_f$ into a filtered D-module. We have seen in the proof of Lemma 4.1.1 that every element of D can be uniquely expressed as

$$\sum c_{ij}x^i(\partial/\partial x)^j, \quad x^i = x_1^{i_1} \cdots x_n^{i_n}, \text{ etc.}$$

with c_{ij} in K for all i, j in $\mathbb{N}^n$. We define $F_r(D)$ by the condition that $|i| + |j| \leq r$ for all r. The Heisenberg commutation relation implies that

$$x^i(\partial/\partial x)^j x^{i'}(\partial/\partial x)^{j'} = x^{i+i'}(\partial/\partial x)^{j+j'} + \sum c_{i''j''} x^{i''}(\partial/\partial x)^{j''}$$

for every i, i', j, j' in $\mathbb{N}^n$, in which $i + i' = (i_1 + i'_1, \ldots, i_n + i'_n)$, etc. and $|i''| + |j''| < |i + i'| + |j + j'|$. This not only shows that F defines a filtration of D but also the crucial fact that $G(D)$ is K-isomorphic to the polynomial ring $K[x, y] = K[x_1, \ldots, x_n, y_1, \ldots, y_n]$ in $2n$ variables under the correspondence $x_i \mapsto x_i$, $\partial/\partial x_i \mapsto y_i$ for $1 \leq i \leq n$.

We shall next define $F_r(M)$ for $M = K[x]_f$ so that M becomes a filtered D-module. We choose α independently of r and define $F_r(M)$ as the subspace of $f^{-r}K[x]$ consisting of all $\varphi = f^{-r}p$, where $p = p(x)$ is in $K[x]$, such that

$$\deg(\varphi) \leq \alpha r, \quad \text{i.e., } \deg(p) \leq (\deg(f) + \alpha)r.$$

Then the condition that $\{F_r(M)\}$ forms an increasing sequence with M as its union becomes $\alpha > 0$. We observe that the condition $F_i(D)F_j(M) \subset F_{i+j}(M)$ for all i, j is equivalent to $x_i \cdot F_r(M)$, $\partial/\partial x_i \cdot F_r(M) \subset F_{r+1}(M)$ for $1 \leq i \leq n$ and for all r. Since $x_i \cdot \varphi = x_i\varphi$, hence $\deg(x_i \cdot \varphi) = \deg(\varphi) + 1$, the first condition becomes $\alpha \geq 1$. Since $\deg(\partial/\partial x_i \cdot \varphi) \leq \deg(\varphi) - 1$ and $\partial/\partial x_i \cdot \varphi$ is in $f^{-r-1}K[x]$ for every φ in $f^{-r}K[x]$, there is no new condition from $\partial/\partial x_i \cdot F_r(M) \subset F_{r+1}(M)$. We shall therefore take $\alpha = 1$. We have thus shown that if we define $F_r(M)$ as the subspace of $f^{-r}K[x]$ consisting of all φ such that $\deg(\varphi) \leq r$, then M becomes a filtered D-module.

We might remark that except when we regard $K[x]_f$ as a D-module, the field K need not be $K_0(s)$. It can be any field with $\mathrm{char}(K) = 0$. Furthermore if D is replaced by a general filtered K-algebra A, then $\mathrm{char}(K)$ need not be 0.

4.4 A general theorem on D-modules

We shall start with some general definitions and observations. We fix a K-algebra A and take A-modules M, N. We say that a K-linear map $\alpha : M \to N$ is an A-homomorphism if α is A-linear, i.e., $\alpha(a\varphi) = a\alpha(\varphi)$ for every (a, φ) in $A \times M$. We take A-modules M', M, M'' and A-homomorphisms $\alpha : M' \to M$, $\beta : M \to M''$. We say that the sequence

$$(*) \qquad 0 \to M' \to M \to M'' \to 0$$

is exact in the category of A-modules or simply exact as A-modules if α is injective, β is surjective, and $\mathrm{Im}(\alpha) = \mathrm{Ker}(\beta)$. If we identify M' with its image under α, this means that the factor module M/M' becomes A-isomorphic to M'' under β. In the case where A is a filtered K-algebra and M', M, M'' are filtered A-modules, $(*)$ is called exact as filtered A-modules if it gives rise to a sequence

$$0 \to F_r(M') \to F_r(M) \to F_r(M'') \to 0$$

for every r, which is exact as K-modules, i.e., vector spaces over K. In that case we clearly have

$$\dim_K(F_r(M)) = \dim_K(F_r(M')) + \dim_K(F_r(M''))$$

for all r. In the case where A is a graded K-algebra and M', M, M'' are graded A-modules, $(*)$ is called exact as graded A-modules if it gives rise to a sequence

$$0 \to M'_r \to M_r \to M''_r \to 0$$

for every r, which is exact as K-modules. The fact is that G is an "exact functor" in the following sense: If $(*)$ is exact as filtered A-modules, then the associated sequence

$$0 \to G(M') \to G(M) \to G(M'') \to 0$$

is exact as graded $G(A)$-modules. In fact, if we identify $F_r(M')$ with its image in $F_r(M)$, then the kernel of the K-homomorphism from $G_r(M) = F_r(M)/F_{r-1}(M)$ to $G_r(M'') = F_r(M'')/F_{r-1}(M'')$, which is clearly surjective, is

$$\begin{aligned}(F_r(M') + F_{r-1}(M))/F_{r-1}(M) &= F_r(M')/(F_r(M') \cap F_{r-1}(M)) \\ &= F_r(M')/F_{r-1}(M') = G_r(M')\end{aligned}$$

for all r. We observe that if A is a filtered K-algebra and M in the exact sequence $(*)$ of A-modules is a filtered A-module, and if we put

$$F_r(M') = F_r(M) \cap M', \quad F_r(M'') = (F_r(M) + M')/M'$$

for all r, then M', M'' become filtered A-modules and $(*)$ is exact as filtered A-modules.

Suppose now that M is a filtered A-module for a filtered K-algebra A and

$$\dim_K(F_r(M)) = (e/d!)r^d + o(r^d), \quad \text{i.e., } \dim_K(F_r(M))/r^d \to e/d!,$$

as r tends to ∞ for some $d \geq 0$, $e > 0$ in $\mathbb{Z}$. Then we say that the *filtration F is of type (d, e)* or *F is a (d, e)-filtration*. We observe that if M has such a filtration, then necessarily $M \neq 0$. There are two immediate examples of such filtrations. We take the polynomial ring $K[x_1, \ldots, x_m]$ as A and M, and regard M as a filtered A-module with $F_r(M)$ consisting of all polynomials of degree at most r. Then

$$\dim_K(F_r(M)) = \mathrm{card}\{i \in \mathbb{N}^m; |i| \leq r\} = (r+m)\ldots(r+1)/m!$$

for all r in $\mathbb{N}$, hence F gives an $(m, 1)$-filtration. Also the filtration of the D-module $K[x]_f$ defined in section 4.3 is an $(n, (\deg(f)+1)^n)$-filtration. At any rate the following lemma is clear by definition:

Lemma 4.4.1 *Let $0 \to M' \to M \to M'' \to 0$ denote an exact sequence of filtered A-modules such that the filtrations of M', M'' are of types (d', e'), (d'', e'') respectively. Then the filtration of M is of type (d, e) where $d = max(d', d'')$ and $e = e'$, $e' + e''$, e'' according as $d' > d''$, $d' = d''$, $d' < d''$.*

We also need the fact that the converse of Proposition 4.3.2 holds with additional information. Suppose that A is a filtered K-algebra and M is an A-module considered as filtered A-modules under two filtrations F, F'. We say that F, F' are *equivalent* if there exist r_0, s_0 in $\mathbb{N}$ satisfying

$$F_r(M) \subset F'_{r+s_0}(M), \quad F'_r(M) \subset F_{r+r_0}(M)$$

for all r. This is clearly an equivalence relation. It follows from the definition that if F is of type (d, e) and F' is equivalent to F, then F' is also of type (d, e). We say that a filtration F of M is *standard* if $G(M)$ becomes a finitely generated $G(A)$-module.

Proposition 4.4.1 *If A is a filtered K-algebra and M is a finitely generated A-module, then M always has a standard filtration which is unique up to equivalence.*

Proof. Suppose that M is generated as an A-module by its finite subset $\{\varphi_1, \ldots, \varphi_k\}$. If we regard A^k as an A-module by the prescription

$$a \cdot (a_1, \ldots, a_k) = (aa_1, \ldots, aa_k),$$

then the correspondence $(a_1, \ldots, a_k) \mapsto a_1\varphi_1 + \ldots + a_k\varphi_k$ gives rise to a surjective A-homomorphism $A^k \to M$ with kernel, say N. If we put

$$F_r(A^k) = F_r(A)^k, \quad F_r(M) = \sum_{1 \le i \le k} F_r(A)\varphi_i, \quad F_r(N) = F_r(A^k) \cap N,$$

then the sequence $0 \to N \to A^k \to M \to 0$ becomes exact as filtered A-modules. Since G is an exact functor, the $G(A)$-homomorphism $G(A^k) = G(A)^k \to G(M)$ is surjective. Therefore the $G(A)$-module $G(M)$ is generated by k elements, hence the above filtration F of M is standard.

We take an arbitrary standard filtration F' of M and show that it is equivalent to F. As we have seen in the proof of Proposition 4.3.2, we can find a finite subset $\{\phi_1, \ldots, \phi_l\}$, where each ϕ_j is contained in $F'_{r_j}(M)$ for some r_j in $\mathbb{N}$, such that

$$F'_r(M) = F_{r-r_1}(A)\phi_1 + \ldots + F_{r-r_l}(A)\phi_l$$

for all r, hence $M = \sum A\phi_j$. In particular we can write

$$\varphi_i = \sum_{1 \le j \le l} a_{ij}\phi_j, \quad \phi_j = \sum_{1 \le i \le k} b_{ji}\varphi_i$$

with a_{ij}, b_{ji} in A for $1 \le i \le k$, $1 \le j \le l$. We may assume that a_{ij}, b_{ji} are all contained in $F_{r_0}(A)$ for some r_0 in $\mathbb{N}$. If we put

$$s_0 = \max(r_0 + r_1, \ldots, r_0 + r_l),$$

then we will have

$$\begin{aligned} F_r(M) &= \sum_{1 \le i \le k} F_r(A)\varphi_i \quad \subset \sum_{1 \le j \le l} F_{r+r_0}(A)\phi_j \subset F'_{r+s_0}(M), \\ F'_r(M) &= \sum_{1 \le j \le l} F_{r-r_j}(A)\phi_j \subset \sum_{1 \le i \le k} F_{r+r_0}(A)\varphi_i = F_{r+r_0}(M) \end{aligned}$$

for all r. Therefore F and F' are equivalent.

If now A is a filtered K-algebra such that $G(A)$ is K-isomorphic to a polynomial ring $K[x_1, \ldots, x_m]$ for some $m > 0$, M is a finitely generated A-module different from 0, and F is a standard filtration of M, then F is a (d, e)-filtration with $d \leq m$. This basic fact follows from Theorem 1.3.3 in view of the fact that

$$\dim_K(F_r(M)) = \sum_{0 \leq i \leq r} \dim_K(G_i(M)) = \chi(G(M), r)$$

with $\deg(\chi(G(M), t)) \leq m$ for all large r. Furthermore d, e are independent of the choice of F by Proposition 4.4.1. Therefore we shall denote them by $d(M)$, $e(M)$. The following statement is the *main theorem* in Bernstein's theory:

Theorem 4.4.1 *If M is any D-module with a (d, e)-filtration where $D = D_n$, then necessarily $d \geq n$. Furthermore if $d = n$, then the length of any strictly increasing sequence of D-submodules of M is at most equal to e. In particular, the D-module M is finitely generated.*

Since the D-module $K[x]_f$ has an $(n, (\deg(f) + 1)^n)$-filtration, Theorem 4.4.1 implies that it is a finitely generated D-module, and that implies Theorem 4.1.1 by Proposition 4.3.1. As for the proof of Theorem 4.4.1 we shall show at this point only the fact that the first part implies the second part. We, therefore, assume that $d = n$ for M and take any finite strictly increasing sequence of D-submodules of M:

$$0 = L_0 \subset L_1 \subset \ldots \subset L_k.$$

If we choose φ_i from $L_i \backslash L_{i-1}$ and put $M_i = D\varphi_1 + \ldots + D\varphi_i$ for $0 \leq i \leq k$, then we get a similar sequence:

$$0 = M_0 \subset M_1 \subset \ldots \subset M_k.$$

We observe that M_i and M_i/M_{i-1} are finitely generated D-modules different from 0 for $1 \leq i \leq k$. Therefore, by the first part and Lemma 4.4.1 we get $n \leq d(M_i/M_{i-1}) \leq d(M_i)$ for $1 \leq i \leq k$. Since M_i is an A-submodule of M which has an (n, e)-filtration, we get $d(M_i) \leq n$, hence $d(M_i) = d(M_i/M_{i-1}) = n$ for $1 \leq i \leq n$. Again by Lemma 4.4.1 we then get

$$e(M_i) = e(M_{i-1}) + e(M_i/M_{i-1}) > e(M_{i-1})$$

for $1 < i \leq k$ and $e(M_1) > 0$ by definition, hence $e(M_i) \geq i$ for $1 \leq i \leq k$. Since M_k is an A-submodule of M and $d(M_k) = n$, we have $e(M_k) \leq e$, hence $k \leq e$. Therefore the first part of Theorem 4.4.1 indeed implies its second part.

4.5 Completion of the proof

We shall prove the first part of Theorem 4.4.1. We start with preliminary remarks and two lemmas. Firstly if A is a filtered K-algebra with a polynomial ring as $G(A)$, M is a finitely generated A-module, and N is any A-submodule of M, then

N is also a finitely generated A-module. The proof goes as follows: We take a standard filtration F of M and restrict F to N, i.e., we put $F_r(N) = F_r(M) \cap N$ for all r. Then $G(N)$ becomes a $G(A)$-submodule of $G(M)$. Therefore $G(N)$ is a finitely generated $G(A)$-module by Theorem 1.3.1, hence N is a finitely generated A-module by Proposition 4.3.2. Secondly, let A denote a K-algebra and M an A-module defined by a K-algebra homomorphism $\theta : A \to \mathrm{End}_K(M)$; let σ denote any element of the group $\mathrm{Aut}(A)$ of K-algebra automorphisms of A. Then we can convert M into another A-module by using $\theta \circ \sigma$ instead of θ. We shall denote the new A-module by M^σ; we keep in mind that M and M^σ differ only in the actions of A. If A is a filtered K-algebra, we shall denote by $\mathrm{Aut}_F(A)$ the subgroup of $\mathrm{Aut}(A)$ defined by the condition that σ keeps $F_r(A)$ for every r. In the special case where M is a finitely generated A-module such that $G(A)$ is a polynomial ring, we clearly have $d(M^\sigma) = d(M)$, etc. for every σ in $\mathrm{Aut}_F(A)$.

Lemma 4.5.1 *Suppose that $char(K) = 0$, F is the filtration of $D = D_n$ defined in section 4.3, and σ is any element of $Aut_F(D)$; regard x, $\partial/\partial x$ as column vectors. Then*

$$\sigma x = ax + b(\partial/\partial x) + \gamma', \quad \sigma(\partial/\partial x) = cx + d(\partial/\partial x) + \gamma'',$$

in which the $2n \times 2n$ matrix with a, b, c, d as its entry matrices is in the symplectic group $Sp_{2n}(K)$ and $\gamma = {}^t({}^t\gamma' \, {}^t\gamma'')$ is in K^{2n}. Conversely, for every such element of $Sp_{2n}(K) \times K^{2n}$ the above prescription defines an element σ of $Aut_F(D)$.

Proof. Since σ keeps $F_1(D)$, we have the above situation with a, b, c, d in $\mathrm{M}_n(K)$ and γ in K^{2n}. Since σ is in $\mathrm{Aut}(D)$, it keeps the defining relation of D. Therefore if we denote the new x, $\partial/\partial x$ by x^*, $(\partial/\partial x)^*$, then we have

$$x_i^* x_j^* - x_j^* x_i^* = 0, \quad (\partial/\partial x_i)^*(\partial/\partial x_j)^* - (\partial/\partial x_j)^*(\partial/\partial x_i)^* = 0,$$

$$x_i^*(\partial/\partial x_j)^* - (\partial/\partial x_j)^* x_i^* + \delta_{ij} = 0$$

for $1 \le i, j \le n$. By a straightforward calculation, we see that they are respectively equivalent to $a\,{}^t b = b\,{}^t a$, $c\,{}^t d = d\,{}^t c$, $a\,{}^t d - b\,{}^t c = 1_n$, the unit element of $\mathrm{M}_n(K)$. Therefore the coefficient-matrix is in $\mathrm{Sp}_{2n}(K)$ while there is no condition on γ. By reversing the above argument we see that every element of $\mathrm{Sp}_{2n}(K) \times K^{2n}$ gives rise to an element of $\mathrm{Aut}_F(D)$.

We shall later use two kinds of σ both keeping x_i, $\partial/\partial x_i$ for $1 \le i < n$ and mapping x_n, $\partial/\partial x_n$ respectively to $x_n + \gamma_n$, $\partial/\partial x_n + \gamma_{2n}$ and $-\partial/\partial x_n + \gamma_n$, $x_n + \gamma_{2n}$, in which γ_n, γ_{2n} are in K.

Lemma 4.5.2 *Suppose that K is an algebraically closed noncountable field such as $\mathbb{C}$, t is a variable, and M is a $K[t]$-module different from 0 with at most countable $dim_K(M)$; denote by $\theta : K[t] \to End_K(M)$ the K-algebra homomorphism defining M as a $K[t]$-module. Then there exists an element α of K such that $\theta(t - \alpha)$ is not a unit of $End_K(M)$.*

Proof. We shall assume that $\theta(t - \alpha)$ is a unit of $\mathrm{End}_K(M)$ for every α in K and derive a contradiction. Take any $p = p(t) \ne 0$ from $K[t]$ and factorize it as $p(t) = \beta \cdot \prod(t - \alpha)$ with β in $K^\times$ and α in K. This is possible because K is

algebraically closed. Then $\theta(p) = \beta \cdot \prod \theta(t-\alpha)$ is a unit of $\mathrm{End}_K(M)$. Therefore θ uniquely extends to a K-algebra homomorphism from $K(t)$ to $\mathrm{End}_K(M)$, which we shall denote also by θ. We choose any $\varphi \neq 0$ from M, which is possible because $M \neq 0$, and consider the K-linear map from $K(t)$ to M defined by $q \mapsto \theta(q)\varphi$. We observe that the set $\{1/(t-\alpha); \alpha \in K\}$ is linearly independent over K. Since K is noncountable and $\dim_K(M)$ is at most countable, therefore, the above K-linear map $K(t) \to M$ is not injective. Therefore $\theta(q)\varphi = 0$ for some $q \neq 0$; but $\theta(q)$ is a unit of $\mathrm{End}_K(M)$, hence $\varphi = 0$, a contradiction.

We are ready to prove the first part of Theorem 4.4.1 stating that if M is a D-module with a (d,e)-filtration, then $d \geq n$. Since $M \neq 0$, it contains a finitely generated D-module $M' \neq 0$ and then $d(M') \leq d$. Therefore we have only to show that if $M \neq 0$ is a fintely generated D-module, then $d(M) \geq n$. We keep in mind that, since $\dim_K(D)$ is countable and the D-module M is finitely generated, $\dim_K(M)$ is at most countable. Since $d(M) \geq 0$, the above statement becomes trivial for $n = 0$. Therefore we shall apply an induction on n assuming that $n > 0$. After tensorizing D and M over K by an extension of K, we may assume that K is algebraically closed and noncountable. We shall denote the K-algebra homomorphism $D \to \mathrm{End}_K(M)$ defining M as a D-module by θ. We shall assume that $d(M) < n$ and derive a contradiction.

Put $x_n = t$. Then by Lemma 4.5.2 there exists an element α of K such that $\theta(t-\alpha)$ is not a unit of $\mathrm{End}_K(M)$. We may replace $t-\alpha$ by t and denote the kernel and the cokernel of $\theta(t)$ respectively by M' and M''. If we put $D' = D_{n-1}$, then $\theta(t)$ is a D'-homomorphism, hence M' and M'' are D'-modules. Since $\theta(t)$ is not a unit of $\mathrm{End}_K(M)$, either $M' = 0$, $M'' \neq 0$ or $M' \neq 0$. We shall show that either case will bring a contradiction.

Suppose first that $M' = 0$, hence $M'' = M/tM \neq 0$. Since M is a finitely generated D-module, it has a standard filtration F by Proposition 4.4.1, and it gives rise to a standard filtration F of M'' as its image under $M \to M''$, i.e., as $F_r(M'') = (F_r(M) + tM)/tM$ for all r. We observe that $F_r(M)/tF_{r-1}(M)$ is mapped surjectively to $F_r(M'')$ under $M \to M''$ and $\theta(t)$ is injective. Therefore we get

$$\dim_K(F_r(M'')) \leq \dim_K(F_r(M)) - \dim_K(F_{r-1}(M)) = O(r^{d(M)-1}),$$

i.e., the LHS divided by $r^{d(M)-1}$ is bounded, as r tends to ∞. Since $M'' \neq 0$, it contains $\psi \neq 0$, which is in $F_{r_0}(M'')$ for some r_0 in $\mathbb{N}$. We introduce a D'-module L'' and its standard filtration as $L'' = D'\psi$ and $F'_r(L'') = F_r(D')\psi$ for all r. Then by induction we have $n-1 \leq d(L'')$. On the other hand, by definition we have $F'_r(L'') \subset F_r(D)\psi \subset F_{r+r_0}(M'')$, hence

$$\dim_K(F'_r(L'')) \leq \dim_K(F_{r+r_0}(M'')) = O(r^{d(M)-1})$$

as r tends to ∞, and hence $d(L'') \leq d(M) - 1$. Since $d(M) < n$ by assumption, we have the contradiction that $n-1 \leq d(L'') < n-1$.

Suppose next that $M' \neq 0$ and denote the union of $\mathrm{Ker}(\theta(t^m))$ for all $m > 0$ by N. Then N is a D'-submodule of M and it is stable under $\theta(t)$. We shall show that N is also stable under $\theta(\partial/\partial t)$. In doing so we shall use the following consequence

of the defining relation of D:

$$(**) \qquad (\partial/\partial t)t^m = t^m(\partial/\partial t) + mt^{m-1}$$

valid for all m in $\mathbb{N}$. If now φ is in N, then $t^m\varphi = 0$ for some $m > 0$. This implies by $(**)$

$$t^{m+1}((\partial/\partial t)\varphi) = (\partial/\partial t)(t^{m+1}\varphi) - (m+1)t^m\varphi = 0.$$

Therefore $(\partial/\partial t)\varphi$ is in N, hence N is stable under $\theta(\partial/\partial t)$. We have thus shown that N is a D-submodule of M. By our remark in the beginning N is then a finitely generated D-module, hence $d(N)$ is defined and $d(N) \leq d(M)$, and hence $d(N) < n$ by assumption. Furthermore $N \neq 0$ because N contains $\mathrm{Ker}(\theta(t)) = M' \neq 0$. Therefore we can replace M by N, and we will have the situation that every element φ of M satisfies $t^m\varphi = 0$ for some $m > 0$ depending on φ. The rest of the proof is as follows.

We shall show that $\mathrm{Ker}(\theta(\partial/\partial t - \alpha)) = 0$ for all α in K. Suppose otherwise and choose $\varphi \neq 0$ from the above kernel for some α in K; also choose the smallest $m > 0$ satisfying $t^m\varphi = 0$. Then $(\partial/\partial t)\varphi = \alpha\varphi$ implies by $(**)$

$$0 = (\partial/\partial t)(t^m\varphi) = \alpha t^m\varphi + mt^{m-1}\varphi = mt^{m-1}\varphi.$$

Since $\mathrm{char}(K) = 0$, this implies $t^{m-1}\varphi = 0$, a contradiction. We now take σ in Lemma 4.5.1 inducing the identity on D' and mapping $t, \partial/\partial t$ respectively to $-\partial/\partial t$, t. Then M^σ becomes a finitely generated D-module different from 0, $d(M^\sigma) = d(M) < n$, and $\mathrm{Ker}(\theta \circ \sigma(t - \alpha)) = 0$ for all α in K. We can replace M by M^σ, and we get $\mathrm{Ker}(\theta(t - \alpha)) = 0$ for all α in K. On the other hand, $\theta(t - \alpha)$ is not a unit of $\mathrm{End}_K(M)$ for some α in K by Lemma 4.5.2. If we finally replace $t - \alpha$ by t, then we get back to the previous case where $M' = 0$. We have seen in that case that the assumption $d(M) < n$ brings a contradiction.

https://doi.org/10.1090/amsip/014/05

Chapter 5

Archimedean local zeta functions

5.1 The group $\Omega(K^\times)$

We say that G is a topological group if G is a Hausdorff space and a group such that the group operations, i.e., the maps $G \times G \to G$ and $G \to G$ defined by $(g, g') \mapsto gg'$ and $g \mapsto g^{-1}$, are continuous. If G, H are topological groups, we shall denote by $\mathrm{Hom}(G, H)$ the set of all continuous homomorphisms from G to H. We observe that if G is compact and H has no compact subgroup other than 1, e.g., the additive group $\mathbb{R}$, then $\mathrm{Hom}(G, H)$ becomes 1, in which 1 denotes the group consisting of the unit element only. We further observe that if H is commutative, then $\mathrm{Hom}(G, H)$ becomes a commutative group as $(\theta\theta')(g) = \theta(g)\theta'(g)$ for every $\theta,\ \theta'$ in $\mathrm{Hom}(G, H)$ and g in G. We shall determine $\mathrm{Hom}(K^\times, \mathbb{C}^\times)$ for $K = \mathbb{R},\ \mathbb{C}$ after introducing some notation and proving a lemma.

In general, if K is any field with an absolute value $|\cdot|_K$, we shall denote by $K_1^\times$ the subgroup of $K^\times$ defined by $|a|_K = 1$. In the case where $K = \mathbb{R},\ \mathbb{C}$ we respectively put $|a|_K = |a|,\ |a|^2$ for every a in K. We might remark that we have created a minor discrepancy by introducing the above $|\cdot|_{\mathbb{C}}$ but with the advantage of making some formulas uniform for $K = \mathbb{R}$, $\mathbb{C}$ and also for a p-adic field. At any rate $K_1^\times = \{\pm 1\}$ if $K = \mathbb{R}$ and $K_1^\times$ is the unit circle with center 0 in the complex plane if $K = \mathbb{C}$. Furthermore, if $\mathbb{R}_+^\times$ denotes the subgroup of $\mathbb{R}^\times$ defined by $a > 0$, then $K^\times / K_1^\times$ becomes isomorphic to $\mathbb{R}_+^\times$ under $|\cdot|_K$, and the extension splits, i.e., $K^\times = \mathbb{R}_+^\times \times K_1^\times$.

Lemma 5.1.1 *Let $I = (-\delta, \delta)$ for any $\delta > 0$ denote an open interval in $\mathbb{R}$ and θ a continuous map from I to $\mathbb{R}$ with the property that $\theta(x + y) = \theta(x) + \theta(y)$ for all x, y in I satisfying $|x| + |y| < \delta$ and $\theta(-x) = -\theta(x)$ for all x in I. Then $\theta(x) = ax$ for some a in $\mathbb{R}$ and for all x in I. In particular, θ uniquely extends to an element of Hom$(\mathbb{R}, \mathbb{R})$.*

Proof. First of all we have $\theta(0) = 0$ and if $x_1, \ldots, x_n$ are in $\mathbb{R}$ satisfying $|x_1| + \ldots + |x_n| < \delta$, hence necessarily in I, then by an induction on n we see that $\theta(x_1 + \ldots + x_n) = \theta(x_1) + \ldots + \theta(x_n)$. Therefore if m, n are in $\mathbb{N}$ and $m, n > 1/\delta$, then by applying the above remark to $x_i = 1/mn$ for $1 \le i \le n$, we get $\theta(1/m) = n\theta(1/mn)$, hence $m\theta(1/m) = mn\theta(1/mn)$. Since the RHS is symmetric in m and

n, it is also equal to $n\theta(1/n)$. Therefore, $a = m\theta(1/m)$ is independent of m in $\mathbb{N}$ satisfying $m > 1/\delta$. Furthermore if $m, n > 0$ are in $\mathbb{N}$ and n/m is in I, then

$$\theta(n/m) = n\theta(1/m) = a(n/m), \quad \theta(-n/m) = -\theta(n/m) = a(-n/m).$$

We have thus shown that $\theta(x) = ax$ for all x in $\mathbb{Q} \cap I$, hence for all x in I by continuity.

We shall determine $\mathrm{Hom}(\mathbb{R}, \mathbb{C}_1^\times)$ and $\mathrm{Hom}(\mathbb{C}_1^\times, \mathbb{C}_1^\times)$ by using Lemma 5.1.1 starting with $\mathrm{Hom}(\mathbb{R}, \mathbb{C}_1^\times)$. If we restrict the homomorphism $\mathbf{e} : \mathbb{R} \to \mathbb{C}_1^\times$ defined by $x \mapsto \mathbf{e}(x) = \exp(2\pi i x)$ to $(-1/2, 1/2)$, then it has a unique inverse, say ψ, over $\mathbb{C}_1^\times \backslash \{-1\}$. If χ is an arbitrary element of $\mathrm{Hom}(\mathbb{R}, \mathbb{C}_1^\times)$, then $I = (-\delta, \delta)$ for a small $\delta > 0$ and $\theta = \psi \circ \chi$ will have the property in Lemma 5.1.1, hence θ extends to $\mathbb{R}$ and $\theta(x) = ax$ for a unique a in $\mathbb{R}$. This implies $\chi(x) = \mathbf{e}(ax)$ for all x in $\mathbb{R}$. The converse is obvious and $\mathrm{Hom}(\mathbb{R}, \mathbb{C}_1^\times)$ is isomorphic to $\mathbb{R}$ as $\chi \mapsto a$. Similarly, if χ is an element of $\mathrm{Hom}(\mathbb{C}_1^\times, \mathbb{C}_1^\times)$, then $\chi \circ \mathbf{e}$ becomes an element of $\mathrm{Hom}(\mathbb{R}, \mathbb{C}_1^\times)$, hence $\chi(\mathbf{e}(x)) = \mathbf{e}(ax)$ for a unique a in $\mathbb{R}$ and for all x in $\mathbb{R}$. Since $\chi \circ \mathbf{e}$ maps $\mathbb{Z}$ to 1, we see that a is in $\mathbb{Z}$, and $\chi(t) = t^a$ for all t in $\mathbb{C}_1^\times$. The converse is obvious and $\mathrm{Hom}(\mathbb{C}_1^\times, \mathbb{C}_1^\times)$ is isomorphic to $\mathbb{Z}$ as $\chi \mapsto a$. These are well-known examples in Pontrjagin's theory. We are ready to prove the following proposition.

Proposition 5.1.1 *If $K = \mathbb{R}$ or $\mathbb{C}$, then $\Omega(K^\times) = \mathrm{Hom}(K^\times, \mathbb{C}^\times)$ consists of all ω such that*

$$\omega(a) = |a|_K^s (a/|a|)^p,$$

in which s is in $\mathbb{C}$ and p is in $\mathbb{Z}$ considered modulo 2 for $K = \mathbb{R}$. Furthermore under the correspondence $\omega \mapsto (s, p)$ the group $\Omega(K^\times)$ is isomorphic to $\mathbb{C} \times (\mathbb{Z}/2\mathbb{Z})$ or $\mathbb{C} \times \mathbb{Z}$ according as $K = \mathbb{R}$ or $\mathbb{C}$.

Proof. If a is an arbitrary element of $K^\times$, then under its product expression $a = |a|(a/|a|)$ we have $K^\times = \mathbb{R}_+^\times \times K_1^\times$. Since $\mathrm{Hom}(K_1^\times, \mathbb{R}_+^\times) = 1$, therefore, we see that $\Omega(K^\times)$ is isomorphic to

$$\mathrm{Hom}(\mathbb{R}_+^\times, \mathbb{R}_+^\times) \times \mathrm{Hom}(\mathbb{R}_+^\times, \mathbb{C}_1^\times) \times \mathrm{Hom}(K_1^\times, \mathbb{C}_1^\times).$$

We shall determine each factor. Firstly, if ω is in $\mathrm{Hom}(\mathbb{R}_+^\times, \mathbb{R}_+^\times)$, then $\theta = \log \circ \omega \circ \exp$ gives an element of $\mathrm{Hom}(\mathbb{R}, \mathbb{R})$, hence $\omega(x) = x^\sigma$ for a unique σ in $\mathbb{R}$ and for all x in $R_+^\times$. Secondly, if ω is in $\mathrm{Hom}(\mathbb{R}_+^\times, \mathbb{C}_1^\times)$, then $\theta = \omega \circ \exp$ gives an element of $\mathrm{Hom}(\mathbb{R}, \mathbb{C}_1^\times)$, hence $\omega(x) = x^{i\tau}$ for a unique τ in $\mathbb{R}$ and for all x in $\mathbb{R}_+^\times$. Thirdly, if ω is in $\mathrm{Hom}(K_1^\times, \mathbb{C}_1^\times)$, then $\omega(t) = t^p$ with p in $\mathbb{Z}$ for all t in $K_1^\times$. In the case where $K = \mathbb{R}$, since $K_1^\times = \{\pm 1\}$, we take $p \mod 2$. Then in both cases p becomes unique. We have thus shown that if ω is any element of $\Omega(K^\times)$, then we can write

$$\omega(a) = \omega(|a|)\omega(a/|a|) = |a|^{\sigma + i\tau}(a/|a|)^p$$

for all a in $K^\times$ with unique σ, τ in $\mathbb{R}$, and p in $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}$ according as $K = \mathbb{R}$ or $\mathbb{C}$. If we put $s = [K : \mathbb{R}]^{-1}(\sigma + i\tau)$, then $\omega(a)$ takes the form in the proposition. The converse is clear.

A remarkable fact is that $\Omega(K^\times)$ is a union of two or countably many copies of $\mathbb{C}$ for $K = \mathbb{R}$ or $\mathbb{C}$. In particular, $\Omega(K^\times)$ is a one-dimensional $\mathbb{C}$-analytic manifold.

Therefore we can define $\mathbb{C}$-analytic functions or simply holomorphic functions on any nonempty open subset of $\Omega(K^\times)$ and talk about their meromorphic continuation, poles, etc. For such purposes we introduce some notation. If s is arbitrary in $\mathbb{C}$, then

$$\omega_s(a) = |a|_K^s$$

defines an element ω_s of $\Omega(K^\times)$, and for every ω in $\Omega(K^\times)$ we will have

$$|\omega(a)| = \omega_{\sigma(\omega)}(a)$$

with $\sigma(\omega)$ in $\mathbb{R}$. If we express ω as in Proposition 5.1.1, then $\sigma(\omega) = \mathrm{Re}(s)$, the real part of s. If σ is arbitrary in $\mathbb{R}$, then we denote by $\Omega_\sigma(K^\times)$ the open subset of $\Omega(K^\times)$ defined by $\sigma(\omega) > \sigma$. We shall sometimes denote by $\mathbb{C}_\sigma$ the open subset of $\mathbb{C}$ defined similarly by $\mathrm{Re}(s) > \sigma$. In this notation $\Omega_0(K^\times)$ becomes a union of the right-half plane $\mathbb{C}_0$.

5.2 Schwartz space $\mathcal{S}(K^n)$

We start with the definition of $\mathcal{S}(K^n)$ for $K = \mathbb{R}, \mathbb{C}$. Since $\mathcal{S}(\mathbb{C}^n)$ is defined as $\mathcal{S}(\mathbb{R}^{2n})$ after identifying $\mathbb{C}$ with $\mathbb{R}^2$, we assume that $K = \mathbb{R}$ and put $X = \mathbb{R}^n$. If φ is any $\mathbb{C}$-valued continuous function on a topological space, its uniform norm $\|\varphi\|_\infty$ is defined as the supremum of $|\varphi(x)|$ for all x in the space. A $\mathbb{C}^\infty$-function Φ on X, i.e., a $\mathbb{C}$-valued function Φ on X having derivatives of arbitrarily high order, is called a *Schwartz function* if $\|P\Phi\|_\infty$ for every P in $D_n = \mathbb{C}[x, \partial/\partial x]$ is finite. We observe that the set $\mathcal{S}(X)$ of all Schwartz functions on X forms a vector space over $\mathbb{C}$ and it is invariant under any invertible $\mathbb{R}$-linear transformation in X. In the verification we use the fact that $\|\Phi\| = \|P\Phi\|_\infty$ for every P in D_n gives a seminorm on $\mathcal{S}(X)$. We recall that if E is a vector space over $\mathbb{C}$, then a seminorm $\|\cdot\|$ on E is defined by the following conditions:

$$0 \le \|\varphi\| < \infty, \quad \|c\varphi\| = |c|\ \|\varphi\|, \quad \|\varphi + \varphi'\| \le \|\varphi\| + \|\varphi'\|$$

for all φ, φ' in E and c in $\mathbb{C}$. We observe that the finiteness of $\|P\Phi\|_\infty$ for all P in D_n is equivalent to the finiteness of

$$\|\Phi\|_{i,j} = \sup_{x \in X} |x^i (\partial/\partial x)^j \Phi(x)|$$

for all i, j in $\mathbb{N}^n$. The set of such seminorms is countable. We further observe that $\|\Phi\|_\infty = \|\Phi\|_{0,0}$ and $\|\Phi\|_\infty = 0$ implies $\Phi = 0$. The following lemma is known in general topology:

Lemma 5.2.1 *Let E denote a vector space over $\mathbb{C}$ and $\{\|\cdot\|_i;\ i \in \mathbb{N}\}$ a set of seminorms on E such that $\|\varphi\|_i = 0$ for all i implies $\varphi = 0$; define the distance $d(\varphi, \varphi')$ in E as*

$$d(\varphi, \varphi') = \sum_{i \ge 0} (1/2^i) \|\varphi - \varphi'\|_i / (1 + \|\varphi - \varphi'\|_i).$$

Then E becomes a metric space. Furthermore if $\{\varphi_i\}$ is any sequence in E, then $\|\varphi_j - \varphi_k\|_i$ tends to 0 as j,k tend to ∞ for every i if and only if $d(\varphi_j, \varphi_k)$ tends to 0 as j,k tend to ∞.

We shall outline the proof that E is a metric space, i.e., $d(\varphi,\varphi') = 0$ if and only if $\varphi = \varphi'$, $d(\varphi,\varphi') = d(\varphi',\varphi)$, and $d(\varphi,\varphi'') \le d(\varphi,\varphi') + d(\varphi',\varphi'')$. The first two properties are clear while the third property follows from the fact that the function $f(t) = t/(1+t)$ for $t \ge 0$ is monotone increasing, $0 \le f(t) < 1$, and

$$(f(t) + f(t')) - f(t+t') = tt'(2+t+t')/(1+t)(1+t')(1+t+t') \ge 0.$$

In particular, $\mathcal{S}(X)$ is a metric space and the topology in $\mathcal{S}(X)$ is invariant under any invertible $\mathbb{R}$-linear transformation in X. The vector space $\mathcal{S}(X)$ with the so-defined topology is called the *Schwartz space* of X. If $\{\Phi_k\}$ is a Cauchy sequence in $\mathcal{S}(X)$, then $\{(\partial/\partial x)^j \Phi_k\}$ forms a Cauchy sequence relative to the uniform norm for every j in $\mathbb{N}^n$. Therefore $(\partial/\partial x)^j \Phi_k$ is uniformly convergent to Ψ_j, say, as k tends to ∞ and if we put $\Psi_0 = \Psi$, then $(\partial/\partial x)^j \Psi = \Psi_j$ for every j. This is well known in calculus; it is proved by using the representation of a differentiable function as an integral of its derivative and applying an elementary form of Lebesgue's theorem reviewed in Chapter 1.1. Furthermore, $\{\|\Phi_k\|_{i,j}\}$ is a Cauchy sequence in $\mathbb{R}$ with $\|\Psi\|_{i,j}$ as its limit for every i,j. In particular, this shows that Ψ is an element of $\mathcal{S}(X)$, hence $\mathcal{S}(X)$ is a complete metric space. We denote the topological dual of $\mathcal{S}(X)$ by $\mathcal{S}(X)'$. In other words, $\mathcal{S}(X)'$ is the subspace of the dual space of $\mathcal{S}(X)$ consisting of its elements which are continuous functions on $\mathcal{S}(X)$, i.e., which convert every null sequence in $\mathcal{S}(X)$ into a null sequence in $\mathbb{C}$. An element of $\mathcal{S}(X)'$ is called a *tempered distribution* in X. We recall that a *distribution* in X was introduced by L. Schwartz in [51]-1 by using the space $\mathcal{D}(X)$ of all C^∞-functions on X with compact support instead of $\mathcal{S}(X)$ and a tempered distribution in [51]-II to discuss Fourier transformations.

We shall show, for our later use, the well-known fact that $\mathcal{D}(X)$ is dense in $\mathcal{S}(X)$. We might start with A. Cauchy's historical remark that the $\mathbb{R}$-analytic function $\exp(-1/x^2)$ on $\mathbb{R}^\times$ completed by the value 0 at $x = 0$ becomes a C^∞-function on $\mathbb{R}$ with 0 as its Maclaurin expansion. We replace the above x by $(1 - 4(t-a)^2)^{1/2}$ and put

$$\theta_a(t) = \exp(-1/(1 - 4(t-a)^2))$$

for $|t-a| < 1/2$ and $\theta_a(t) = 0$ for $|t-a| \ge 1/2$. Then θ_a becomes a C^∞-function on $\mathbb{R}$. Furthermore, if we put $I = \{0, \pm 1/2, \pm 1\}$ and $J = I \cup \{\pm 3/2\}$, then

$$\chi = \left(\sum_{a \in I} \theta_a\right) / \left(\sum_{b \in J} \theta_b\right)$$

is a C^∞-function on $\mathbb{R}$ such that $\chi(t) = 1$ for $|t| \le 1$, $\chi(t) = 0$ for $|t| \ge 2$ and $\chi(-t) = \chi(t)$, $0 \le \chi(t) \le 1$ for all t in $\mathbb{R}$. In particular, $\chi(t)$ becomes a C^∞-function of t^2. In the following lemma and also later $r(x)$ denotes the distance from 0 to x, i.e., $(\sum x_i^2)^{1/2}$:

Lemma 5.2.2 *Take any Φ from $\mathcal{S}(X)$ and put $\Phi_k(x) = \chi(k^{-1}r(x))\Phi(x)$ for $k = 1, 2, \ldots$. Then $\{\Phi_k\}$ gives a sequence in $\mathcal{D}(X)$ which tends to Φ as k tends to ∞, i.e., $\{\Phi_k - \Phi\}$ is a null sequence in $\mathcal{S}(X)$.*

Proof. By definition Φ_k is a C^∞-function on X satisfying $\Phi_k(x) = 0$ for $r(x) \geq 2k$, hence Φ_k is in $\mathcal{D}(X)$. We shall show that

$$\|\Phi_k - \Phi\|_{i,j} = \|x^i(\partial/\partial x)^j((\chi(k^{-1}r(x)) - 1)\Phi(x))\|_\infty$$

tends to 0 as k tends to ∞ for all i, j. We observe that the RHS is at most equal to

$$\sum (j!/j'!\, j''!)\ \|(\partial/\partial x)^{j'}(\chi(k^{-1}r(x)) - 1)\Psi_{j'}(x)\|_\infty,$$

in which $\Psi_{j'}(x) = x^i(\partial/\partial x)^{j''}\Phi(x)$ and the summation is with respect to j' in $\mathbb{N}^n$ such that $j'' = j - j'$ is also in $\mathbb{N}^n$. Since $\Psi_{j'}$ is in $\mathcal{S}(X)$, we have only to show that

$$(*) \qquad \lim_{k\to\infty} \|(\partial/\partial x)^\alpha(\chi(k^{-1}r(x)) - 1)\Phi(x)\|_\infty = 0$$

for every $\alpha = (\alpha_1, \ldots, \alpha_n)$ in $\mathbb{N}^n$ and Φ in $\mathcal{S}(X)$. We observe that if we put $t = k^{-1}r(x),\ u = r(x)^{-1}x$, then

$$(**) \qquad (\partial/\partial x)^\alpha(\chi(t) - 1) = \sum_{|j|\leq|\alpha|} \phi_{\alpha,j}(t)u^j r(x)^{-|\alpha|}\ ,$$

in which $\phi_{\alpha,j}$ is a C^∞-function on $\mathbb{R}$ satisfying $\phi_{\alpha,j}(t) = 0$ for $|t| \leq 1$. In fact, $(**)$ holds for $|\alpha| = 0$ with $\phi_{0,0}(t) = \chi(t) - 1$. Therefore we assume by induction that $(**)$ holds for some α. If we denote by β the new element of $\mathbb{N}^n$ obtained by increasing α_i for some i by 1, then we will have

$$\begin{aligned}(\partial/\partial x)^\beta(\chi(t) - 1) = \ & \textstyle\sum_{|j|\leq|\alpha|} \quad \{(d\phi_{\alpha,j}/dt)tu_i + \\ & \qquad \phi_{\alpha,j}(t)(j_i u_i^{-1} - (|\alpha| + |j|)u_i)\}u^j r(x)^{-|\beta|}.\end{aligned}$$

This implies that $(**)$ holds also for β, hence $(**)$ holds for all α. Now if $|\alpha| = 0$, then

$$\|(\partial/\partial x)^\alpha(\chi(k^{-1}r(x)) - 1)\Phi(x)\|_\infty \leq 2\|r\Phi\|_\infty \cdot k^{-1}$$

and if $|\alpha| > 0$, then

$$\text{LHS} \leq \left(\sum_{|j|\leq|\alpha|} \|\phi_{\alpha,j}\|_\infty\right) \|\Phi\|_\infty \cdot k^{-|\alpha|}.$$

Therefore we certainly have $(*)$.

As a consequence of Lemma 5.2.2, if T in $\mathcal{S}(X)'$ has the property that $T(\varphi) = 0$ for every φ in $\mathcal{D}(X)$, then $T = 0$. An example of the Schwartz function is

$$\Phi(x) = \exp(-\pi \cdot r(x)^2).$$

In fact, Φ is an $\mathbb{R}$-analytic function, hence a C^∞-function, on X. Furthermore, for every i, j in $\mathbb{N}^n$ we have

$$|x^i(\partial/\partial x)^j \Phi(x)| \leq \text{const} \cdot r^{|i|+|j|} \exp(-\pi r^2)|_{r=r(x)},$$

and the RHS tends to 0 as $r(x)$ tends to ∞. Incidentally, the factor π in $\pi \cdot r(x)^2$ makes the integral of Φ over X to become 1.

We go back to the topological dual $\mathcal{S}(X)'$ of $\mathcal{S}(X)$. In general, let E denote a vector space over $\mathbb{C}$ and E' a subspace of the dual space of E; let $\{T_k\}$ denote any sequence in E' with the property that for every φ in E a finite limit

$$T(\varphi) = \lim_{k\to\infty} T_k(\varphi)$$

exists. Then $\varphi \mapsto T(\varphi)$ clearly gives a $\mathbb{C}$-linear map from E to $\mathbb{C}$, i.e., T is an element of the dual space of E. If such a T is always contained in E', then we say that E' is *complete*. We shall explain, after Gel'fand and Shilov [16], Appendix A, a proof by M.S. Brodskii of the following basic theorem:

Theorem 5.2.1 *The vector space $\mathcal{S}(X)'$ of tempered distributions in $X = \mathbb{R}^n$ is complete.*

Proof. We take a sequence $\{T_k\}$ in $\mathcal{S}(X)'$ with the property that for every Φ in $\mathcal{S}(X)$ a finite limit $T(\Phi)$ of $\{T_k(\Phi)\}$ as $k \to \infty$ exists. To be proved is the fact that T is continuous. We shall assume that T is not continuous and derive a contradiction in three steps.

If T is not continuous, there exists a null sequence $\{\Phi_p\}$ in $\mathcal{S}(X)$ such that $\{T(\Phi_p)\}$ is not a null sequence in $\mathbb{C}$. By replacing $\{\Phi_p\}$ by a subsequence, we may assume that $|T(\Phi_p)| \geq c$ for all p and for some $c > 0$ independent of p. Since $\{\Phi_p\}$ is a null sequence in $\mathcal{S}(X)$, we have $\|\Phi_p\|_{i,j} \to 0$ as $p \to \infty$ for every i, j in $\mathbb{N}^n$. Therefore for any given k, if we choose $p' = p(k)$ sufficiently large, we will have

$$\|\Phi_{p'}\|_{i,j} \leq 2^{-2k}$$

for all i, j satisfying $|i| + |j| \leq k$. If we put $\varphi_k = 2^k \Phi_{p'}$, then we have

$$(*) \qquad \|\varphi_k\|_{i,j} \leq 2^{-k} \quad (|i| + |j| \leq k), \qquad |T(\varphi_k)| \geq 2^k c$$

for every k in $\mathbb{N}$.

We shall next show that if for every k in $\mathbb{N}$ we suitably choose k', $k'' \geq k$ depending on k and put $\psi_k = \varphi_{k'}$, $S_k = T_{k''}$, then we will have

$$(**) \qquad |S_p(\psi_k)| \leq 2^{p-k} \quad (0 \leq p < k), \qquad |S_k(\psi_k)| > \sum_{0\leq p<k} |S_k(\psi_p)| + k.$$

Since $T_q(\varphi_0) \to T(\varphi_0)$ as $q \to \infty$ and $|T(\varphi_0)| \geq c$ by $(*)$, if we put $\psi_0 = \varphi_0$ and $S_0 = T_q$ for a large q, we will have $|S_0(\psi_0)| > 0$. Then ψ_0, S_0 satisfy $(**)$ for $k = 0$. Assume by induction that for some $k \geq 0$ we have ψ_p, S_p for $0 \leq p \leq k$ satisfying

$(**)$. Since $S_p(\varphi_q) \to 0$, $T(\varphi_q) \to \infty$ as $q \to \infty$, if we put $\psi_{k+1} = \varphi_q$ for a large $q > k$, then we will have

$$|S_p(\psi_{k+1})| \le 2^{p-k-1} \quad (0 \le p \le k), \qquad |T(\psi_{k+1})| > \sum_{0 \le p \le k} |T(\psi_p)| + k + 1.$$

Since $T_q(\psi_p) \to T(\psi_p)$ as $q \to \infty$ for $0 \le p \le k+1$, if we put $S_{k+1} = T_q$ for a large $q > k$, then we will have

$$|S_{k+1}(\psi_{k+1})| > \sum_{0 \le p \le k} |S_{k+1}(\psi_p)| + k + 1.$$

This completes the induction.

We shall show that

$$\Psi = \lim_{k \to \infty} \left(\sum_{0 \le p \le k} \psi_p \right)$$

exists in $\mathcal{S}(X)$. If for any i, j in $\mathbb{N}^n$ we choose $k_1 \ge k_0 \ge |i| + |j|$, then, since $\psi_k = \varphi_{k'}$ for $k' \ge k$, by $(*)$ we have

$$\| \sum_{k_0 \le k \le k_1} \psi_k \|_{i,j} \le \sum_{k_0 \le k \le k_1} 2^{-k} \le 2^{1-k_0},$$

in which $2^{1-k_0} \to 0$ as $k_0 \to \infty$. Since $\mathcal{S}(X)$ is complete, this implies the existence of Ψ above in $\mathcal{S}(X)$. Then by the continuity of $S_k = T_{k''}$ we get

$$S_k(\Psi) = \lim_{k_0 \to \infty} \left(\sum_{0 \le p \le k_0} S_k(\psi_p) \right).$$

On the other hand, for all $k_0 \ge k$ by $(**)$ we have

$$\begin{aligned} \left| \sum_{0 \le p \le k_0} S_k(\psi_p) \right| &\ge |S_k(\psi_k)| - \sum_{0 \le p < k} |S_k(\psi_p)| - \sum_{p > k} |S_k(\psi_p)| \\ &> k - \sum_{p > k} 2^{k-p} = k - 1, \end{aligned}$$

hence $|S_k(\Psi)| \ge k - 1$. On the other hand

$$\lim_{k \to \infty} S_k(\Psi) = \lim_{k \to \infty} T_k(\Psi) = T(\Psi)$$

is finite. We thus have a contradiction.

We shall now explain Gel'fand and Shilov [16], Appendix 2, especially the important "method of analytic continuation." It is based on the completeness of $\mathcal{S}(X)'$. In fact we can replace $\mathcal{S}(X)$ and $\mathcal{S}(X)'$ respectively by a vector space E over $\mathbb{C}$ and any complete subspace E' of its dual space. Let U denote a subset (resp. open subset) of $\mathbb{C}$, which we assume to be nonempty, and $s \mapsto T_s$ an E'-valued function

on U. We say that T_s is continuous (resp. holomorphic) on U if $T_s(\varphi)$ for every φ in E is continuous (resp. holomorphic) on U. If C is a continuous curve of finite length in $\mathbb{C}$ and if T_s is continuous on C, then

$$S(\varphi) = \int_C T_s(\varphi) ds$$

is defined for every φ in E and $\varphi \mapsto S(\varphi)$ defines an element S of the dual space of E. We shall show that S is contained in E'. We parametrize C by a continuous function $s(t)$ for $0 \leq t \leq 1$ and for every k in $\mathbb{N}$ we put

$$S_0 = 0, \qquad S_k = \sum_{1 \leq i \leq k} T_{s_i}(s_i - s_{i-1}) \quad (k > 0),$$

in which $s_i = s(i/k)$ for $0 \leq i \leq k$. Then S_k is in E' and $S_k(\varphi) \to S(\varphi)$ as $k \to \infty$ for every φ in E. Therefore S is in E' by the completeness of E'. We shall write

$$S = \int_C T_s \, ds.$$

Suppose now that T_s is holomorphic on U, s_0 is in $\mathbb{C}$, and the punctured disc $\{s \in \mathbb{C};\ 0 < |s - s_0| \leq r\}$ is contained in U for some $r > 0$. Then $T_s(\varphi)$ for every φ in E can be expanded into its Laurent series

$$T_s(\varphi) = \sum_{k \in \mathbb{Z}} c_k(\varphi)(s - s_0)^k,$$

in which

$$c_k = \frac{1}{2\pi i} \int_{|s - s_0| = r} \frac{T_s}{(s - s_0)^{k+1}} \, ds$$

is in E' for every k in $\mathbb{Z}$. We call

$$T_s = \sum_{k \in \mathbb{Z}} c_k (s - s_0)^k$$

the *Laurent expansion* of T_s at s_0. We say that s_0 is a *pole* of T_s if $c_k \neq 0$ only for a finite number of $k < 0$.

Proposition 5.2.1 *Let E denote a vector space over $\mathbb{C}$ and E' any complete subspace of its dual space; let $U \subset U_1$ denote open subsets of $\mathbb{C}$, in which U is nonempty and every connected component of U_1 intersects U; finally let T_s denote an E'-valued holomorphic function on U such that for every φ in E the $\mathbb{C}$-valued holomorphic function $T_s(\varphi)$ on U has a holomorphic continuation to U_1. Then $\varphi \mapsto T_s(\varphi)$ defines an element T_s of E' for every s in U_1.*

Proof. We may restrict s to any connected component of U_1, hence we may assume that U_1 is connected. If we put

$$\Sigma = \{s \in U_1;\ T_s \in E'\},$$

then $U \subset \Sigma \subset U_1$. We shall derive a contradiction assuming that $\Sigma \neq U_1$. If we denote by V the largest open subset of $\mathbb{C}$ contained in Σ, then $U \subset V \subset \Sigma$. We observe that if we denote by $\bar{V}$ the closure of V in $\mathbb{C}$, then $(U_1 \backslash V) \cap \bar{V} \neq \emptyset$. Otherwise $U_1 \backslash V = U_1 \backslash \bar{V}$, hence $U_1 \backslash V$ is open in U_1 and nonempty because it contains $U_1 \backslash \Sigma$. This contradicts the assumption that U_1 is connected. We can therefore choose s_1 from $(U_1 \backslash V) \cap \bar{V}$. We denote by $\mathrm{dis}(s, \partial U_1)$ the distance from any point s of $\mathbb{C}$ to the boundary ∂U_1 of U_1. Since the subsequent argument becomes simpler if $\partial U_1 = \emptyset$, we shall assume otherwise, i.e., $\mathrm{dis}(s, \partial U_1)$ is finite for every s. We choose s_0 from V satisfying $|s_1 - s_0| < (1/2)\mathrm{dis}(s_1, \partial U_1)$. Since T_s is an E'-valued holomorphic function on V and s_0 is in V, we can expand T_s for every s near s_0 into a Laurent series or rather a Taylor series as

$$T_s = \sum_{k \in \mathbb{N}} c_k (s - s_0)^k$$

with c_k in E' for all k in $\mathbb{N}$. Furthermore, since $T_s(\varphi)$ for every φ in E is holomorphic on the open disc

$$W = \{s \in \mathbb{C};\ |s - s_0| < \mathrm{dis}(s_0, \partial U_1)\},$$

we get

$$T_s(\varphi) = \lim_{k \to \infty} (\sum_{0 \leq p \leq k} c_p (s - s_0)^p)(\varphi)$$

for every s in W. Therefore T_s is in E' for every s in W by the completeness of E' and s_1 is in W. If s_1 is not in W, there exists a point s_2 of ∂U_1 satisfying $|s_1 - s_0| \geq |s_0 - s_2|$ and that brings the following contradiction:

$$\mathrm{dis}(s_1, \partial U_1) \leq |s_1 - s_2| \leq |s_1 - s_0| + |s_0 - s_2| \leq 2|s_1 - s_0| < \mathrm{dis}(s_1, \partial U_1).$$

Since W is open, we see that s_1 is in V, a contradiction.

We call the extended T_s in Proposition 5.2.1 the *holomorphic continuation* of the original T_s to U_1. If further $U_1 \subset U_2 \subset \mathbb{C}$, in which U_2 is open in $\mathbb{C}$ and $U_2 \backslash U_1$ is discrete in U_2, such that the extended T_s has every point of $U_2 \backslash U_1$ as a pole, then it is called the *meromorphic continuation* of the original T_s to U_2.

5.3 Local zeta function $Z_\Phi(\omega)$

We shall start with two lemmas. We have stated them with proof for the sake of completeness.

Lemma 5.3.1 *Let (X, dx) denote a measure space, e.g., a nonempty open subset of $\mathbb{R}^n$ equipped with the usual measure, U a nonempty open subset of $\mathbb{C}$, and f a $\mathbb{C}$-valued measurable function on $X \times U$, e.g., a continuous function if X is an open subset of $\mathbb{R}^n$, with the following properties: (i) If C is any compact subset of U, there exists an integrable function $\phi_C \geq 0$ on X satisfying*

$$|f(x, s)| \leq \phi_C(x)$$

for all (x,s) in $X \times C$; (ii) $f(x,\cdot)$ is a holomorphic function on U for every x in X. Then

$$F(s) = \int_X f(x,s)\ dx$$

defines a holomorphic function F on U.

Proof. We have only to show that the restriction of F to every open disc in U is holomorphic. Therefore we may assume that U is connected and simply connected. We shall use some theorems which we have recalled in Chapter 1.1. Firstly F is a continuous function on U. In fact, if s_0 is any point of U, then by Lebesgue's theorem we get

$$\begin{aligned}\lim_{s\to s_0} F(s) &= \lim_{s\to s_0} \int_X f(x,s)\ dx \\ &= \int_X (\lim_{s\to s_0} f(x,s))\ dx = \int_X f(x,s_0)\ dx = F(s_0).\end{aligned}$$

Secondly if C is any closed curve of finite length in U, then by using theorems of Fubini and Cauchy we get

$$\int_C F(s)\ ds = \int_C (\int_X f(x,s)\ dx)\ ds = \int_X (\int_C f(x,s)\ ds)\ dx = 0.$$

Therefore F is holomorphic on U by Morera's theorem.

Lemma 5.3.2 *Let V denote a nonempty open subset of $X = \mathbb{R}^n$ with a piecewise smooth boundary ∂V, φ a continuously differentiable function on the closure $\bar{V}$ of V in X with polynomial growth, i.e.,*

$$|\varphi(x)| \le M \cdot \max(1, r(x)^m)$$

for some $M, m \ge 0$ and for all x in $\bar{V}$, such that $\varphi\big|\partial V = 0$. Then for every Φ in $\mathcal{S}(X)$ and for $1 \le i \le n$ we have

$$\int_V (\partial\varphi/\partial x_i)\Phi(x)\ dx = \int_V \varphi(x)(-\partial\Phi/\partial x_i)\ dx.$$

Proof. We take a large $R \ge 1$ so that $V_R = \{x \in V;\ r(x) < R\}$ is not empty, put

$$\theta = \varphi\Phi \cdot (-1)^{i-1} dx_1 \wedge \ldots \wedge dx_{i-1} \wedge dx_{i+1} \wedge \ldots \wedge dx_n,$$

and apply Gauss' theorem recalled in Chapter 1.1 to the integral of $d\theta$ over V_R. If we denote by W_R the intersection of V and the sphere S_R in X defined by $r(x) = R$, then by using $\varphi\big|\partial V = 0$ we get

$$\int_{W_R} \theta = \int_{V_R} (\partial(\varphi\Phi)/\partial x_i)\ dx.$$

If we denote by $d\sigma$ the surface element of S_R, then we will have

$$|\mathrm{LHS}| \le M \cdot \int_{S_R} r(x)^{m+n} |\Phi(x)| r(x)^{-n}\ d\sigma \le M \cdot \|r^{m+n}\Phi\|_\infty \cdot \Omega_n R^{-1},$$

in which Ω_n denotes the area of S_1. If we take the limit as $R \to \infty$, then we get the formula in the lemma.

If we use Lemma 5.3.2 repeatedly, then we shall be talking about the shifting of a differential operator P applied to one factor to another as its adjoint operator P^*. We have $x_i^* = x_i$, $(\partial/\partial x_i)^* = -\partial/\partial x_i$ for $1 \leq i \leq n$. We observe that if $D_n = K[x, \partial/\partial x]$ is the Weyl algebra, where K is any field with $\mathrm{char}(K) = 0$, then the above prescription uniquely extends to a K-involution $P \mapsto P^*$ of D_n, i.e., a K-linear map from D_n to itself satisfying $(P_1P_2)^* = P_2^*P_1^*$ and $(P^*)^* = P$. In fact, in the notation of Lemma 4.1.1, the tensor algebra $T(E)$ has a K-involution defined by $\xi_i^* = \xi_i$, $\eta_i^* = -\eta_i$ for $1 \leq i \leq n$ under which the ideal $I(E)$ is stable. For instance, we have

$$(\xi_i \otimes \eta_j - \eta_j \otimes \xi_i + \delta_{ij})^* = -\eta_j \otimes \xi_i + \xi_i \otimes \eta_j + \delta_{ij}$$

for all i, j. This implies the above assertion.

In the following theorem $\Gamma(s)$ denotes the gamma function. We shall give a self-contained exposition of the theory of $\Gamma(s)$ in Chapter 6.2, which can be read separately. For the time being, we shall only use the well-known facts that $\Gamma(s)$ is holomorphic on $\mathbb{C}_0$, $1/\Gamma(s)$ is holomorphic on $\mathbb{C}$, $\Gamma(s+1) = s\Gamma(s)$ for every s in $\mathbb{C}\backslash(-\mathbb{N})$, and $\Gamma(1) = 1$.

Theorem 5.3.1 *We take $f(x)$ arbitrarily from $\mathbb{R}[x_1, \ldots, x_n]\backslash\mathbb{R}$, define an open subset V of $X = \mathbb{R}^n$ as $V = \{x \in X;\ f(x) > 0\}$, and for any s in the right-half plane $\mathbb{C}_0$ and any Φ in $\mathcal{S}(X)$ we put*

$$f_+^s(\Phi) = \int_V f(x)^s \Phi(x)\, dx$$

with the understanding that $f_+^s(\Phi) = 0$ if $V = \emptyset$. Then f_+^s becomes an $\mathcal{S}(X)'$-valued holomorphic function on $\mathbb{C}_0$. Furthermore, if we put

$$b_f(s) = \prod_\lambda (s + \lambda), \quad \gamma_f(s) = \prod_\lambda \Gamma(s + \lambda),$$

in which $b_f(s)$ is the Bernstein polynomial of $f(x)$, then $f_+^s/\gamma_f(s)$ has a holomorphic continuation to the whole $\mathbb{C}$.

Proof. We shall prove the first part. If we put $d = \deg(f)$ and

$$M_1 = \max(1, \sup_{r(x) \leq 1} |f(x)|), \quad M_2 = \max(1, \sup_{r(x) \geq 1} |r(x)^{-d} f(x)|),$$

then $1 \leq M_1, M_2 < \infty$. We take any compact subset C of $\mathbb{C}_0$ and denote by σ_0 the maximum of $\mathrm{Re}(s)$ for all s in C. Finally, we denote by χ_1 (resp. χ_2) the characteristic function of $\{x \in X;\ r(x) \leq 1\}$ (resp. $\{x \in X;\ r(x) \geq 1\}$) and put

$$\phi_C(x) = M_1^{\sigma_0} \|\Phi\|_\infty \cdot \chi_1(x) + M_2^{\sigma_0} \|r^{d\sigma_0 + n + 1} \Phi\|_\infty \cdot r(x)^{-n-1} \chi_2(x)$$

for every x in X. Then for every (x,s) in $V \times C$ we have $|f(x)^s\Phi(x)| \leq \phi_C(x)$ and

$$\begin{aligned} |f_+^s(\Phi)| \leq \int_V \phi_C(x)\ dx &\leq \int_X \phi_C(x)\ dx \\ &= M_1' \cdot \|\Phi\|_\infty + M_2' \cdot \|r^{d\sigma_0+n+1}\Phi\|_\infty, \end{aligned}$$

in which

$$M_1' = M_1^{\sigma_0}\Omega_n/n, \quad M_2' = M_2^{\sigma_0}\Omega_n$$

are both finite and independent of Φ. In particular, $f_+^s(\Phi)$ is defined and f_+^s converts every null sequence in $\mathcal{S}(X)$ into a null sequence in $\mathbb{C}$. Furthermore, by applying Lemma 5.3.1 to this case with V, $\mathbb{C}_0$, $f(x)^s\Phi(x)$ respectively as X, U, $f(x,s)$, we see that $f_+^s(\Phi)$ is a holomorphic function on $\mathbb{C}_0$. Therefore, f_+^s is an $\mathcal{S}(X)'$-valued holomorphic function on $\mathbb{C}_0$.

As for the second part, for the sake of simplicity, we shall write $b(s)$, $\gamma(s)$ instead of $b_f(s)$, $\gamma_f(s)$. By Bernstein's theorem, i.e., Theorem 4.1.1, there exists an element $P(s)$ of $\mathbb{R}[s,x,\partial/\partial x]$ satisfying

$$P(s)f(x)^{s+1} = b(s)f(x)^s$$

for every x in V. More precisely $f(x)^s$ is well defined for every x in V and $P(s)$ is applied to $f(x)^{s+1}$ as a differential operator. If we take s from $\mathbb{C}_\sigma$ for a large $\sigma > 0$ depending on the order of $P(s)$, then Lemma 5.3.2 becomes repeatedly applicable and we get

$$b(s)f_+^s(\Phi) = \int_V (P(s)f(x)^{s+1})\Phi(x)\ dx = \int_V f(x)^{s+1}(P(s)^*\Phi(x))\ dx.$$

We observe that $\Phi_1 = P(s)^*\Phi$ is in $\mathcal{S}(X)$. Therefore we can keep on applying the above process and, after k-times application, we get

$$b(s)\dots b(s+k-1)f_+^s(\Phi) = \int_V f(x)^{s+k}\Phi_k(x)\ dx,$$

in which $\Phi_k = P(s+k-1)^*\dots P(s)^*\Phi$ is in $\mathcal{S}(X)$. In fact, Φ_k is a polynomial in s with coefficients in $\mathcal{S}(X)$. Since

$$\gamma(s)b(s)\dots b(s+k-1) = \gamma(s+k),$$

therefore, we get

$$\gamma(s)^{-1}f_+^s(\Phi) = \gamma(s+k)^{-1} \cdot \int_V f(x)^{s+k}\Phi_k(x)\ dx$$

under the assumption that s is in $\mathbb{C}_\sigma$ for a large $\sigma > 0$. We observe that the LHS is holomorphic on $\mathbb{C}_0$ while the RHS is holomorphic on $\mathbb{C}_{-k}$. Since k is arbitrary in $\mathbb{N}$, the above relation implies that $f_+^s(\Phi)/\gamma(s)$ has a holomorphic continuation to $\mathbb{C}$. Therefore we see by Proposition 5.2.1 that $f_+^s/\gamma(s)$ has a holomorphic continuation to $\mathbb{C}$.

We recall that an arbitrary element ω of $\Omega(\mathbb{R}^\times)$ has the form

$$\omega(a) = |a|_{\mathbb{R}}^s (a/|a|)^p, \quad |a|_{\mathbb{R}} = |a|,$$

in which s is in $\mathbb{C}$ and $p = 0, 1$. We observe that if ω is in $\Omega_0(\mathbb{R}^\times)$, i.e., if $\sigma(\omega) = \mathrm{Re}(s) > 0$, then ω has a continuous extension to $\mathbb{R}$ as $\omega(0) = 0$. We introduce the *local zeta function* $Z_\Phi(\omega)$ of $f(x)$ in $\mathbb{R}[x_1, \ldots, x_n]\backslash\mathbb{R}$ for ω in $\Omega_0(\mathbb{R}^\times)$ and Φ in $\mathcal{S}(X)$ as

$$Z_\Phi(\omega) = \int_X \omega(f(x))\Phi(x)\, dx.$$

The integral does not change even if we replace X by $X\backslash f^{-1}(0)$, which is the disjoint union of $\{x \in X;\ f(x) > 0\}$ and $\{x \in X; -f(x) > 0\}$. Therefore, if we introduce $f_-^s(\Phi)$ as $(-f)_+^s(\Phi)$, we can write

$$Z_\Phi(\omega) = \omega(f)(\Phi) = f_+^s(\Phi) + (-1)^p f_-^s(\Phi).$$

Theorem 5.3.1 then shows that $Z_\Phi(\omega)$ has a meromorphic continuation to $\Omega(\mathbb{R}^\times)$. Furthermore, since $b_{-f}(s) = b_f(s)$, the poles of $Z_\Phi(\omega)$ on the s-plane are in the union of $-\lambda - \mathbb{N}$ as $-\lambda$ runs over the set of zeros of $b_f(s)$. The theorem also shows that the order of a pole of $Z_\Phi(\omega)$ is at most equal to the order of the corresponding zero of $b_f(s)$.

If now $f(x)$ is in $\mathbb{C}[x_1, \ldots, x_n]\backslash\mathbb{C}$, then $V = \mathbb{C}^n\backslash f^{-1}(0)$ is an analogue of $\{x \in \mathbb{R}^n; f(x) > 0\}$. However $f(x)^s$ is not well defined on V. With this situation in mind we proceed as follows: Suppose that s_1, s_2 are elements of $\mathbb{C}$ with $s_1 - s_2$ in $\mathbb{Z}$ and a is arbitrary in $\mathbb{C}^\times$; denote by $\bar{a}$ the complex conjugate of a and put

$$s = (s_1 + s_2)/2, \quad p = s_1 - s_2, \quad \text{i.e., } s_1 = s + p/2, \quad s_2 = s - p/2.$$

Then

$$a^{s_1}\bar{a}^{s_2} = |a|_{\mathbb{C}}^s (a/|a|)^p, \quad |a|_{\mathbb{C}} = |a|^2 = a\bar{a}$$

is well defined. We shall apply the above observation to $a = f(x)$ for x in V. We also make the following observation. If we put $u_\alpha = \mathrm{Re}(x_\alpha)$, $v_\alpha = \mathrm{Im}(x_\alpha)$ so that $x_\alpha = u_\alpha + iv_\alpha$, $\bar{x}_\alpha = u_\alpha - iv_\alpha$ for $1 \le \alpha \le n$, then $\mathbb{C}^n$ becomes $\mathbb{R}^{2n}$ under the correspondence $(x_1, \ldots, x_n) \mapsto (u_1, v_1, \ldots, u_n, v_n)$. Furthermore, if φ is any differentiable function on a nonempty open subset of $\mathbb{C}^n$, then

$$\partial\varphi/\partial x_\alpha = (1/2)(\partial\varphi/\partial u_\alpha - i\partial\varphi/\partial v_\alpha), \quad \partial\varphi/\partial\bar{x}_\alpha = (1/2)(\partial\varphi/\partial u_\alpha + i\partial\varphi/\partial v_\alpha)$$

and Cauchy-Riemann's equations become $\partial\varphi/\partial\bar{x}_\alpha = 0$ for $1 \le \alpha \le n$. Finally, we have

$$dx_1 \wedge d\bar{x}_1 \wedge \ldots \wedge dx_n \wedge d\bar{x}_n = (-2i)^n du_1 \wedge dv_1 \wedge \ldots \wedge du_n \wedge dv_n$$

and, accordingly, we shall use 2^n-times the usual measure on $\mathbb{R}^{2n}$ as the Haar measure dx on $\mathbb{C}^n$.

In the above notation, if for any element $\varphi(x)$ of $\mathbb{C}(s_1)[x, 1/f(x)]$ we regard s_1 as a complex variable, then

$$(\partial/\partial x_i)(\varphi(x)f(x)^{s_1}\bar{f}(\bar{x})^{s_2}) = (\partial/\partial x_i \cdot \varphi(x))f(x)^{s_1}\bar{f}(\bar{x})^{s_2}$$

for every variable x in V and for $1 \leq i \leq n$. Therefore Bernstein's theorem becomes applicable. Namely, there exists an element $P(s)$ of $\mathbb{C}[s, x, \partial/\partial x]$ satisfying

$$P(s_1)f(x)^{s_1+1}\bar{f}(\bar{x})^{s_2} = b_f(s_1)f(x)^{s_1}\bar{f}(\bar{x})^{s_2}$$

for every x in V. In the following theorem $\gamma_f(s)$ is as in Theorem 5.3.1

Theorem 5.3.2 *If we take $f(x)$ arbitrarily from $\mathbb{C}[x_1, \ldots, x_n]\backslash\mathbb{C}$, s from $\mathbb{C}_0$, p from $\mathbb{Z}$, Φ from $\mathcal{S}(X)$, where $X = \mathbb{C}^n$, and put $V = X\backslash f^{-1}(0)$, $s_1 = s + p/2, s_2 = s - p/2$, then*

$$f^{s_1}\bar{f}^{s_2}(\Phi) = \int_V f(x)^{s_1}\bar{f}(\bar{x})^{s_2}\Phi(x)\ dx$$

defines an $\mathcal{S}(X)'$-valued holomorphic function $f^{s_1}\bar{f}^{s_2}$ of s in $\mathbb{C}_0$, and further $f^{s_1}\bar{f}^{s_2}/\gamma_f(s_1)$ has a holomorphic continuation to the whole $\mathbb{C}$.

Proof. We apply an entirely similar argument to $f^{s_1}\bar{f}^{s_2}(\Phi)$ as in the proof of Theorem 5.3.1, and we get the first part. As for the second part, also as in the proof of Theorem 5.3.1, we get

$$\gamma_f(s_1)^{-1}f^{s_1}\bar{f}^{s_2}(\Phi) = \gamma_f(s_1 + k)^{-1} \cdot \int_V f(x)^{s_1+k}\bar{f}(\bar{x})^{s_2}\Phi_k(x)\ dx$$

for $\mathrm{Re}(s_1)$ sufficiently large, in which $\Phi_k = P(s_1 + k - 1)^* \ldots P(s_1)^*\Phi$ is in $\mathcal{S}(X)$ for all k in $\mathbb{N}$. Since

$$f(x)^{s_1+k}\bar{f}(\bar{x})^{s_2} = |f(x)|_{\mathbb{C}}^{s+k/2}(f(x)/|f(x)|)^{p+k}$$

for every x in V, the RHS of the above relation is holomorphic on $\mathbb{C}_{-k/2}$, and this implies the second part.

Remark. We observe that if we put $Q(s) = \bar{P}(s, \bar{x}, \partial/\partial\bar{x})$ for $P(s) = P(s, x, \partial/\partial x)$, then we have

$$Q(s_2)f(x)^{s_1}\bar{f}(\bar{x})^{s_2+1} = \bar{b}_f(s_2)f(x)^{s_1}\bar{f}(\bar{x})^{s_2},$$

in which $\bar{P}, \bar{b}_f$ are as $\bar{f}$ the images of P, b_f under the complex-conjugation applied to their coefficients. In particular, if $b_f(s)$ is written as in Theorem 5.3.1, then

$$\bar{b}_f(s) = \prod_{\lambda}(s + \bar{\lambda}),$$

and this is the Bernstein polynomial of $\bar{f}(x)$. We define $\bar{\gamma}_f$ similarly. More precisely, we define $\bar{\gamma}_f(s)$ as the product of $\Gamma(s + \bar{\lambda})$. Then in the notation of the above proof we have

$$\bar{\gamma}_f(s_2)^{-1}f^{s_1}\bar{f}^{s_2}(\Phi) = \bar{\gamma}_f(s_2 + k)^{-1} \cdot \int_V f(x)^{s_1}\bar{f}(\bar{x})^{s_2+k}\Psi_k(x)\ dx,$$

in which $\Psi_k = Q(s_2 + k - 1)^* \ldots Q(s_2)^*\Phi$ is in $\mathcal{S}(X)$ for all k in $\mathbb{N}$.

We recall that an arbitrary ω in $\Omega(\mathbb{C}^\times)$ has the form

$$\omega(a) = |a|_{\mathbb{C}}^s(a/|a|)^p,$$

in which s is in $\mathbb{C}$ and p is in $\mathbb{Z}$. We introduce the *local zeta function* $Z_\Phi(\omega)$ of $f(x)$ for ω in $\Omega_0(\mathbb{C}^\times)$ and Φ in $\mathcal{S}(X)$ as

$$Z_\Phi(\omega) = \int_X \omega(f(x))\Phi(x)\ dx.$$

If s_1, s_2 are as above, i.e., as in Theorem 5.3.2, then we can write

$$Z_\Phi(\omega) = \omega(f)(\Phi) = f^{s_1}\bar{f}^{s_2}(\Phi).$$

Therefore, $Z_\Phi(\omega)$ is holomorphic on $\Omega_0(\omega)$, and it has a meromorphic continuation to the whole $\Omega(\mathbb{C}^\times)$. Furthermore, the poles of $Z_\Phi(\omega)$ on the p-th s-plane are in the union of $-\lambda - p/2 - \mathbb{N}$ as $-\lambda$ runs over the set of zeros of $b_f(s)$ and the order of a pole of $Z_\Phi(\omega)$ is at most equal to the order of the corresponding zero of $b_f(s)$. The above remark shows that the poles of $Z_\Phi(\omega)$ on the p-th plane are also in the union of $-\bar{\lambda} + p/2 - \mathbb{N}$ as $-\lambda$ runs over the set of zeros of $b_f(s)$ with the same information about their orders.

Finally, in the special case where $\Phi(x) = \exp(-\pi^t xx)$ for $K = \mathbb{R}$ and $\Phi(x) = \exp(-2\pi^t x\bar{x})$ for $K = \mathbb{C}$, we shall write $Z(s)$ instead of $Z_\Phi(\omega_s)$, i.e., we put

$$Z(s) = \int_{K^n} |f(x)|_K^s \Phi(x)\ dx.$$

We shall later explain the computation of $Z(s)$ in some cases.

5.4 Complex power $\omega(f)$ via desingularization

If K is $\mathbb{R}$ or $\mathbb{C}$, $f(x)$ is in $K[x_1, \ldots, x_n]\backslash K$ for some n, and $X = K^n$, then the $\mathcal{S}(X)'$-valued holomorphic function $\omega(f)$ on $\Omega_0(K^\times)$, especially

$$\omega_s(f) = |f|_K^s,$$

is called the *complex power* of $f(x)$. We have seen that it has a meromorphic continuation to the whole $\Omega(K^\times)$ with some information about its poles via the Bernstein polynomial $b_f(s)$. We might repeat a short history about complex powers. (This time with references.) In the Amsterdam Congress of 1954 I.M. Gel'fand proposed the problem of their meromorphic continuation. His joint book with G.E. Shilov [16] contains instructive discussions of complex powers in some special cases. Also M. Sato's theory of prehomogeneous vector spaces [48] contains complex powers of some group invariants. In the general case the problem was settled jointly by I.N. Bernstein and S.I. Gel'fand [2] and also by M.F. Atiyah [1] by the same method, i.e., by using Hironaka's desingularization theorem. Bernstein later obtained another solution in [3], which we have explained. We shall now explain their original solution because it provides some additional information about the poles of complex powers. We shall make use of the results already obtained to simplify the argument.

In general if φ is any, say, $\mathbb{C}$-valued function on a topological space, we call the closure of the set of all x where $\varphi(x) \neq 0$ the *support* of φ and denote it by $\mathrm{Supp}(\varphi)$. We go back to section 5.2 and for any $\varepsilon > 0$ and x in $X = \mathbb{R}^n$ we put

$$\rho_\varepsilon(x) = k\varepsilon^{-n}\theta_0(r((2\varepsilon)^{-1}x)), \quad \text{i.e., } \rho_\varepsilon(x) = k\varepsilon^{-n}\exp(-1/(1 - r(\varepsilon^{-1}x)^2))$$

for $r(x) < \varepsilon$ and $\rho_\varepsilon(x) = 0$ for $r(x) \geq \varepsilon$. We determine $k > 0$ as

$$k \cdot \int_{r(x)<1} \exp(-1/(1-r(x)^2))\ dx = 1$$

so that the integral of ρ_ε over X becomes 1. We are using the same notation as in L. Schwartz [51], I, p. 22. If φ is any $\mathbb{C}$-valued continuous function on X with compact support, then the convolution of φ and ρ_ε is defined as

$$(\varphi * \rho_\varepsilon)(x) = \int_X \varphi(y)\rho_\varepsilon(x-y)\ dy.$$

We see immediately that $\varphi * \rho_\varepsilon$ is a C^∞-function on X which vanishes outside the ε-neighborhood of $\mathrm{Supp}(\varphi)$, i.e., the union of open balls of radius ε centered at all points of $\mathrm{Supp}(\varphi)$. Furthermore we have

$$\|\varphi * \rho_\varepsilon - \varphi\|_\infty \leq \sup_{r(x-y)\leq\varepsilon} |\varphi(x) - \varphi(y)|.$$

Since φ is uniformly continuous, the RHS tends to 0 as $\varepsilon \to 0$. We keep in mind that if $\varphi \geq 0$, i.e., if $\varphi(x) \geq 0$ for every x in X, then $\varphi * \rho_\varepsilon \geq 0$. We shall use the *partition of unity* only in the following form:

Lemma 5.4.1 *Let X denote an n-dimensional $\mathbb{R}$-analytic manifold and C a compact subset of X which is covered by a family of open subsets U_α of X. Then there exists an open subset Ω of X containing C and a finite set $\{p_i;\ i \in I\}$ of C^∞-functions $p_i \geq 0$ on Ω with the closure of $\{x \in \Omega;\ p_i(x) > 0\}$ taken in X contained in some U_α such that*

$$\sum_{i\in I} p_i(x) = 1$$

for every x in C.

Proof. In Chapter 1.1 we have recalled the following fact with proof: Let X denote a locally compact space and U a neighborhood of any point a of X. Then there exists a continuous function φ_a on X with compact support contained in U such that $0 \leq \varphi_a \leq 1$ and $\varphi_a(a) = 1$. If now $\{(U, \phi_U)\}$ is an atlas on X, by replacing each U by many subsets with compact closure contained in U we may assume that every $\bar{U}$ is compact and local coordinates are valid on $\bar{U}$. Then by replacing U_α by $U_\alpha \cap U$ we may assume for every α that $\bar{U}_\alpha$ is compact and local coordinates are valid on $\bar{U}_\alpha$. We then construct φ_a for every a in C so that $\mathrm{Supp}(\varphi_a)$ is contained in some U_α. Since C is compact, we can find a finite set $\{a_i;\ i \in I\}$ such that if we put $\varphi_i = \varphi_a$ for $a = a_i$, then for every x in C we will have $\varphi_i(x) > 0$ for some i in I. If we denote by φ the sum of all φ_i, then φ has a positive minimum η on C. Furthermore if for every i we choose U_α containing $\mathrm{Supp}(\varphi_i)$, denote it by U_i, and replace $\bar{U}_i$ by its bicontinuous image in $\mathbb{R}^n$, then

$$\delta = \min_{i\in I}\{\mathrm{dis}(\mathrm{Supp}(\varphi_i), \partial U_i)\} > 0.$$

We now choose $\varepsilon > 0$ so small that $\varepsilon < \delta$ and $\|\varphi * \rho_\varepsilon - \varphi\|_\infty < \eta$, in which $\varphi * \rho_\varepsilon$ is defined as the sum of all $\varphi_i * \rho_\varepsilon$. Then $\mathrm{Supp}(\varphi_i * \rho_\varepsilon)$ is contained in U_i for every i and $(\varphi * \rho_\varepsilon)(x) > 0$ for every x in C. Therefore, we have only to put

$$\Omega = \{x \in X;\ (\varphi * \rho_\varepsilon)(x) > 0\}, \quad p_i(x) = (\varphi_i * \rho_\varepsilon)(x)/(\varphi * \rho_\varepsilon)(x)$$

for every x in Ω.

We also need the fact that the n-fold tensor product over $\mathbb{C}$ of $\mathcal{D}(\mathbb{R})$ or, equivalently by Lemma 5.2.2, of $\mathcal{S}(\mathbb{R})$ is dense in $\mathcal{S}(\mathbb{R}^n)$. This follows from the following lemma which contains additional information.

Lemma 5.4.2 *The set of functions of the form* $\exp(-\lambda \cdot r(x-a)^2)$ *for all* $\lambda > 0$ *and* a *in* $X = \mathbb{R}^n$ *spans a dense subspace* $\mathcal{G}(X)$ *of* $\mathcal{S}(X)$.

Proof. We have remarked in section 5.2 that $\mathcal{G}(X)$ is contained in $\mathcal{S}(X)$. We take Φ from $\mathcal{S}(X)$ and show that it can be approximated by an element of $\mathcal{G}(X)$. In doing so we may assume that $C = \mathrm{Supp}(\Phi)$ is compact. If for any $\varepsilon > 0$ we put

$$\chi_\varepsilon(x) = \varepsilon^{-n} \cdot \exp(-\pi \cdot r(\varepsilon^{-1}x)^2),$$

then χ_ε is in $\mathcal{S}(X)$, in fact in $\mathcal{G}(X)$, and its integral over X is 1. We shall first show that for any i, j in $\mathbb{N}^n$ we have

$$\lim_{\varepsilon \to 0} \|\Phi * \chi_\varepsilon - \Phi\|_{i,j} = 0.$$

By $|j|$-times application of Lemma 5.3.2 we see that the convolution by χ_ε and $(\partial/\partial x)^j$ commute. By replacing $(\partial/\partial x)^j \Phi$ by Φ, therefore, we may assume that $j = 0$. If $i = 0$ also, without using the compactness of $\mathrm{Supp}(\Phi)$, we can proceed as follows: If we put

$$M = \|(\sum_{1 \le i \le n} (\partial\Phi/\partial x_i)^2)^{1/2}\|_\infty,$$

then by using the mean-value theorem in calculus and the Schwarz inequality we get $|\Phi(x) - \Phi(y)| \le M \cdot r(x-y)$ for every x, y in X. This implies

$$|(\Phi * \chi_\varepsilon - \Phi)(x)| \le M \cdot \int_X r(x)\chi_\varepsilon(x)\ dx = M\Omega_n\varepsilon \cdot \int_{r \ge 0} r^n \exp(-\pi r^2)\ dr,$$

which tends to 0 as $\varepsilon \to 0$. If $m = |i| > 0$, we may replace x^i by $r(x)^m$. We have only to show that

$$\lim_{\varepsilon \to 0} |r(x)^m(\Phi * \chi_\varepsilon - \Phi)(x)| = 0$$

uniformly in x. We choose a large $r_0 > 0$ so that $\Phi(y) \ne 0$ implies $r(y) \le r_0$. Since the above proof takes care of the case where $r(x) \le 2r_0$, we shall assume that $r(x) \ge 2r_0$. If $\Phi(y) \ne 0$, then $r(x) \le 2 \cdot r(x-y)$ and $r(x-y) \ge r_0$. Since $\Phi(x) = 0$, therefore, if we put $r_1 = r_0\varepsilon^{-1}$, then

$$\begin{aligned} |r(x)^m(\Phi * \chi_\varepsilon - \Phi)(x)| &\le 2^m\|\Phi\|_\infty \cdot \int_{r(x) \ge r_0} r(x)^m \chi_\varepsilon(x)dx \\ &= (2\varepsilon)^m\Omega_n\|\Phi\|_\infty \cdot \int_{r \ge r_1} r^{m+n-1} \exp(-\pi r^2)\ dr, \end{aligned}$$

which tends to 0 as $\varepsilon \to 0$.

We shall next show that $\Phi * \chi_\varepsilon$ for any fixed $\varepsilon > 0$ can be approximated by an element of $\mathcal{G}(X)$. We subdivide X into small cubes with vertices in $k^{-1}\mathbb{Z}^n$ for a large k in $\mathbb{N}$. We denote by $\{\delta_i;\ i \in I_k\}$ the finite set of cubes which intersect C and choose y_i from $C \cap \delta_i$ for every i in I_k. We observe that

$$S_k(x) = (k\varepsilon)^{-n} \cdot \sum_{i \in I_k} \Phi(y_i) \exp(-\pi\varepsilon^{-2} \cdot r(x - y_i)^2)$$

is a Riemann sum for $(\Phi * \chi_\varepsilon)(x)$ and that it is in $\mathcal{G}(X)$. We shall show that S_k tends to $\Phi * \chi_\varepsilon$ as $k \to \infty$. We shall prove, more generally, that if φ is in $\mathcal{S}(X)$ and

$$S_k(x) = k^{-n} \cdot \sum_{i \in I_k} \Phi(y_i)\varphi(x - y_i),$$

then we will have

$$\lim_{k \to \infty} \|S_k - \Phi * \varphi\|_{i,j} = 0$$

for every i, j in $\mathbb{N}^n$. Since $(\partial/\partial x)^j S_k(x)$ is a Riemann sum for $(\Phi * (\partial/\partial x)^j \varphi)(x)$, we may assume as before that $j = 0$. We may also replace x^i by $r(x)^m$ where $m = |i|$. We shall show that for any given $\eta > 0$ we can make $|r(x)^m(S_k - \Phi * \varphi)(x)| < \eta$ for all x in X. If $r_1 \geq r_0$ and $r(x) \geq 2r_1$, then by using $r(x) \leq 2 \cdot r(x - y)$ and $r(x - y) \geq r_1$ for $\Phi(y) \neq 0$ we get

$$\begin{aligned} |r(x)^m(S_k - \Phi * \varphi)(x)| &\leq |r(x)^m S_k(x)| + |r(x)^m(\Phi * \varphi)(x)| \\ &\leq 2^m \|\Phi\|_\infty \|r^{m+1}\varphi\|_\infty (\mathrm{card}(I_k)k^{-n} + \mu(C))r_1^{-1}, \end{aligned}$$

in which $\mu(C)$ denotes the total measure of C. Since $\mathrm{card}(I_k)k^{-n}$ tends to $\mu(C)$ as $k \to \infty$, the RHS becomes less than η for a large r_1 and for all large k. We shall fix such an r_1 and take x from the remaining part, i.e., from the compact ball in X defined by $r(x) \leq 2r_1$. Since $\mathrm{Supp}(\Phi)$ is also compact, clearly $\Phi(y)\varphi(x - y)$ is equicontinuous in y, i.e., uniformly continuous in y with the uniformity independent of x. Therefore we will have $(2r_1)^m|(S_k - \Phi * \varphi)(x)| < \eta$ for all large k.

Remark. If $\Phi(x)$ for every x in X is a holomorphic function of s in a fixed nonempty open subset V of $\mathbb{C}$, then in $S_k(x)$ in the above proof s appears only in $\Phi(y_i)$ for i in I_k. Therefore Φ can be approximated by

$$\sum c_i(s)(\varphi_{i1} \otimes \cdots \otimes \varphi_{in})$$

with φ_{ij} in $\mathcal{S}(\mathbb{R})$ and c_i holomorphic on V.

Theorem 5.4.1 *Suppose that $f(x)$, $h : Y \to X = K^n$, and $\mathcal{E} = \{E\}$, where each E is equipped with a pair of positive integers (N_E, n_E), are as in Theorem 3.2.1. Then the poles of the complex power $\omega(f)$ on the p-th s-plane are contained in the union of*

$$-(1/N_E)(n_E + \mathbb{N}) \quad (K = \mathbb{R}), \qquad -|p|/2 - (1/N_E)(n_E + \mathbb{N}) \quad (K = \mathbb{C})$$

for all E in $\mathcal{E}$ with their orders at most equal to the dimension of the nerve complex $\mathcal{N}(\mathcal{E})$ of $\mathcal{E}$ increased by 1. Therefore the poles of $\omega(f)$ are all negative rational numbers and their orders are at most equal to $n = \dim(X)$.

Proof. We take ω from $\Omega_0(K^\times)$. We already know that $\omega(f)$ has a meromorphic continuation to $\Omega(K^\times)$, and we are interested in its poles on the p-th s-plane. We know by Proposition 5.2.1 that every coefficient c of Laurent expansions of $\omega(f)$ at its poles is an element of $\mathcal{S}(X)'$ and we are interested in whether or not $c = 0$. By Lemma 5.2.2 this can be detected by $c(\Phi)$ for Φ in $\mathcal{D}(X)$. Therefore we have only to examine the meromorphic continuation of $\omega(f)(\Phi)$ for Φ in $\mathcal{D}(X)$, i.e., under the assumption that $\mathrm{Supp}(\Phi)$ is compact. Since the map h is proper, we see that $C = h^{-1}(\mathrm{Supp}(\Phi))$ is also compact. We know by Theorem 3.2.1 that at every point b of Y there exist local coordinates $(y_1, \dots, y_n)$ of Y around b such that

$$f \circ h = \varepsilon \cdot \prod_{j \in J} y_j^{N_j}, \quad h^*\Big(\bigwedge_{1 \le k \le n} dx_k \Big) = \eta \cdot \prod_{j \in J} y_j^{n_j - 1} \cdot \bigwedge_{1 \le k \le n} dy_k,$$

in which $(N_j, n_j) = (N_E, n_E)$ with J bijective to the set of all E containing b and ε, η are units of the local ring $\mathcal{O}_b$ of Y at b. We choose a small neighborhood U_b of b over which the above local coordinates are valid and $\varepsilon^{\pm 1}, \eta^{\pm 1}$ are all K-analytic. We apply Lemma 5.4.1 to Y, C, $\{U_b\}$ instead of X, C, $\{U_\alpha\}$. In that way we get a partition of unity $\{p_i;\ i \in I\}$ such that $\sum p_i(y) = 1$ for every y in C. This implies

$$\omega(f)(\Phi) = \sum_{i \in I} \prod_{j \in J} \omega(y_j)^{N_j} |y_j|_K^{n_j - 1} (\omega(\varepsilon)|\eta|_K (\Phi \circ h) p_i).$$

We observe that $\Psi(y) = \omega(\varepsilon(y))|\eta(y)|_K \Phi(h(y)) p_i(y)$ can be considered as an element of $\mathcal{D}(K^n)$ and for a fixed y it has a holomorphic continuation to the whole s-plane. Furthermore, since the Bernstein polynomial of y_j is $s + 1$, by the general results in section 5.3 for $n = 1$ we see that for every j and s in $\mathbb{C}_0$

$$\omega(y_j)^{N_j} |y_j|_K^{n_j - 1} = |y_j|_K^{N_j s + n_j - 1} (y_j / |y_j|)^{N_j p}$$

for y_j in $K^\times$ has a meromorphic continuation to the whole s-plane with its poles defined by the condition that "$N_j s + n_j - 1$ is in $-1 - N_j|p|/2 - \mathbb{N}$," i.e., s is in $-|p|/2 - (1/N_j)(n_j + \mathbb{N})$, with the understanding that $p = 0$ for $K = \mathbb{R}$. Finally, for a similar reason as before, we can apply Lemma 5.4.2 and its remark to replace the above Ψ by a tensor product of elements of $\mathcal{S}(K)$ without losing any pole. In that way we get the description of the poles of $\omega(f)$ as stated in the theorem.

5.5 An application

We shall give an application of Theorem 5.4.1 after recalling some basic facts on Fourier transformations in $\mathcal{S}(X)$ and $\mathcal{S}(X)'$ for $X = \mathbb{R}^n, n > 0$. We reserve the notation Φ for an arbitrary element of $\mathcal{S}(X)$, and we shall not repeat "for all Φ in $\mathcal{S}(X)$" all the time. We first observe that every $\mathbb{C}$-valued continuous function φ on X with polynomial growth gives rise to an element T_φ of $\mathcal{S}(X)'$ as

$$T_\varphi(\Phi) = \int_X \varphi(x) \Phi(x)\ dx.$$

In fact, by assumption we have $|\varphi(x)| \leq M \cdot \max(1, r(x)^m)$ for some $M, m \geq 0$. Then by splitting X into two parts as $r(x) \leq 1$ and $r(x) \geq 1$ we get

$$|T_\varphi(\Phi)| \leq M\Omega_n(n^{-1}\|\Phi\|_\infty + \|r^{m+n+1}\Phi\|_\infty).$$

This implies that T_φ converts every null sequence in $\mathcal{S}(X)$ into a null sequence in $\mathbb{C}$. The correspondence $\varphi \mapsto T_\varphi$ is clearly $\mathbb{C}$-linear and $T_\varphi = 0$ implies $\varphi = 0$. In fact if $\varphi \neq 0$, then $\varphi(a) \neq 0$ for some a in X. Then $\Phi(x) = \rho_\varepsilon(x - a)$, where ρ_ε is as in section 5.4, is in $\mathcal{D}(X)$ and $T_\varphi(\Phi) \neq 0$ if ε is small. We shall sometimes write φ instead of T_φ. We shall now define some operations on elements of $\mathcal{S}(X)'$ in such a way that they are compatible with the identification of φ and T_φ.

If φ is any C^∞-function on X such that all its derivatives have polynomial growth, then $\Phi \mapsto \varphi\Phi$ gives a $\mathbb{C}$-linear continuous map of $\mathcal{S}(X)$ to itself. Therefore if T is in $\mathcal{S}(X)'$, then

$$(\varphi T)(\Phi) = T(\varphi\Phi)$$

defines an element of φT of $\mathcal{S}(X)'$. Similarly, if P is any element of $\mathbb{C}[x, \partial/\partial x]$ and P^* is its adjoint operator, then

$$(PT)(\Phi) = T(P^*\Phi)$$

defines an element PT of $\mathcal{S}(X)'$. If now φ is any $\mathbb{C}$-valued continuous integrable function on X and $[x, y] = \sum x_i y_i$ for every x, y in X with x_i, y_i as their i-th coordinates for $1 \leq i \leq n$, then

$$(\mathcal{F}\varphi)(x) = \int_X \varphi(y)\mathbf{e}([x, y])\ dy,$$

where $\mathbf{e}(t) = \exp(2\pi i t)$, defines a uniformly continuous function $\mathcal{F}\varphi$ or simply φ^* on X satisfying

$$\|\mathcal{F}\varphi\|_\infty \leq \int_X |\varphi(x)|\ dx = \|\varphi\|_1.$$

The correspondence $\varphi \mapsto \mathcal{F}\varphi$ is clearly $\mathbb{C}$-linear and $\mathcal{F}$ is called a *Fourier transformation*. We observe that

$$\|\Phi\|_1 \leq \Omega_n(n^{-1}\|\Phi\|_\infty + \|r^{n+1}\Phi\|_\infty).$$

Furthermore by using Lemma 5.3.2 we get

$$x_p\ \Phi^*(x) = -\frac{1}{2\pi i} \cdot \int_X (\partial\Phi/\partial y_p)\ \mathbf{e}([x, y])\ dy,$$

$$\partial\Phi^*/\partial x_p = 2\pi i \cdot \int_X (y_p\Phi(y))\ \mathbf{e}([x, y])\ dy$$

for $1 \leq p \leq n$. This implies

$$x^\alpha(\partial/\partial x)^\beta\Phi^*(x) = (-1)^{|\alpha|}(2\pi i)^{|\beta|-|\alpha|}((\partial/\partial x)^\alpha x^\beta\Phi)^*(x),$$

hence

$$\begin{aligned}\|\Phi^*\|_{\alpha,\beta} &\leq (2\pi)^{|\beta|-|\alpha|}\|(\partial/\partial x)^\alpha x^\beta \Phi\|_1 \\ &\leq \text{const} \cdot \|\max(1, r^{n+1})(\partial/\partial x)^\alpha x^\beta \Phi\|_\infty\end{aligned}$$

for every α, β in $\mathbb{N}^n$. Therefore $\mathcal{F}\Phi = \Phi^*$ is in $\mathcal{S}(X)$ and further $\mathcal{F}$ gives a continuous map from $\mathcal{S}(X)$ to itself. On the other hand, the following formula:

$$\int_{\mathbb{R}} \exp(-\pi\lambda x^2 + 2ax)\ dx = \lambda^{-1/2}\exp(a^2/\pi\lambda)$$

for $\lambda > 0$ and a in $\mathbb{R}$ is known in calculus. If we put

$$\varphi(x) = \exp(-\pi\lambda r(x)^2 + 2[a, x])$$

for x in X and a in $\mathbb{C}^n$, then by using a holomorphic continuation of the above formula we get

$$\varphi^*(x) = \lambda^{-n/2} \cdot \exp(-\pi\lambda^{-1} r(x)^2 + 2[i\lambda^{-1}a, x] + (\pi\lambda)^{-1} r(a)^2),$$

and this implies $(\varphi^*)^*(x) = \varphi(-x)$ for every x in X. Since the $\mathbb{C}$-span of the above φ for all $\lambda > 0$ and a in X is dense in $\mathcal{S}(X)$ by Lemma 5.4.2 and since $\mathcal{F}$ is continuous, we get $(\Phi^*)^*(x) = \Phi(-x)$ for every x in X. In particular, $\mathcal{F}$ is bicontinuous. Furthermore if φ is any continuous integrable function on X, then by using Fubini's theorem we get

$$\int_X \varphi(x)\Phi^*(x)\ dx = \int\int_{X\times X} \varphi(x)\Phi(y)\mathbf{e}([x, y])\ dxdy = \int_X \varphi^*(x)\Phi(x)\ dx.$$

Therefore if we define the Fourier transform $\mathcal{F}T = T^*$ of any T in $\mathcal{S}(X)'$, as

$$T^*(\Phi) = T(\Phi^*),$$

then T^* is in $\mathcal{S}(X)'$ and $T_{\varphi^*} = (T_\varphi)^*$. We shall formulate its immediate consequence as a proposition for our later use.

Proposition 5.5.1 *If φ is a continuous integrable function on $X = \mathbb{R}^n$ with integrable Fourier transform φ^*, then the Fourier inversion formula*

$$(\varphi^*)^*(x) = \varphi(-x)$$

holds for every x in X.

In fact, if we put $\psi(x) = \varphi(-x)$, then we will have

$$T_{(\varphi^*)^*}(\Phi) = ((T_\varphi)^*)^*(\Phi) = T_\varphi((\Phi^*)^*) = T_\psi(\Phi),$$

hence $(\varphi^*)^* = \psi$.

We shall give two examples of T^*. Firstly

$$1^*(\Phi) = T_1^*(\Phi) = T_1(\Phi^*) = (\Phi^*)^*(0) = \Phi(0) = \delta_0(\Phi),$$

hence $1^* = \delta_0$, the *Dirac measure* on X supported by 0. If we express an element $f(x)$ of $\mathbb{C}[x_1, \ldots, x_n]\backslash\mathbb{C}$ as $f(x) = \sum c_\alpha x^\alpha$ with c_α in $\mathbb{C}$ for α in $\mathbb{N}^n$ and define an element P of $\mathbb{C}[\partial/\partial x_1, \ldots, \partial/\partial x_n]$ as

$$P = \sum_\alpha (2\pi i)^{-|\alpha|} c_\alpha (\partial/\partial x)^\alpha,$$

then for any T in $\mathcal{S}(X)'$ we will have

$$(fT)^* = PT^*.$$

In fact,

$$(fT)^*(\Phi) = \sum_\alpha c_\alpha T(x^\alpha \Phi^*) = \sum_\alpha (-2\pi i)^{-|\alpha|} c_\alpha T^*((\partial/\partial x)^\alpha \Phi) = PT^*(\Phi).$$

We might remark that if $f(x)$ is any element of $\mathbb{R}[x_1, \ldots, x_n]\backslash\mathbb{R}$, then the hypersurface $f^{-1}(0)$ in X is of measure 0. This can be proved, e.g., by using the Weierstrass preparation theorem. We are ready to explain an elegant proof by M.F. Atiyah [1] of the following theorem:

Theorem 5.5.1 *If $f(x)$ is any element of $\mathbb{C}[x_1, \ldots, x_n]\backslash\mathbb{C}$, there exists an element T of $\mathcal{S}(X)'$ for $X = \mathbb{R}^n$ satisfying $fT = 1$.*

Proof. We may assume that $f(x)$ is in $\mathbb{R}[x_1, \ldots, x_n]\backslash\mathbb{R}$ and $f \geq 0$. In fact, if $(f\bar{f})S = 1$ for some S in $\mathcal{S}(X)'$, then $T = \bar{f}S$ is in $\mathcal{S}(X)'$ and $fT = 1$. By assumption $f_-^s = 0$, hence $\omega_s(f) = f_+^s$, which we shall denote by f^s. If we put $V = \{x \in X; f(x) > 0\}$, then by definition

$$f^s(\Phi) = \int_V f(x)^s \Phi(x)\, dx$$

for s in $\mathbb{C}_0$. We know that f^s has a meromorphic continuation to $\mathbb{C}$. Let

$$f^s = \sum_{k \in \mathbb{Z}} c_k (s+1)^k$$

denote its Laurent expansion at -1 with c_k in $\mathcal{S}(X)'$ for all k. Since the poles of f^s are negative rational numbers by Theorem 5.4.1, we see that $f^{s+1} = ff^s$ is holomorphic at $s = -1$. Therefore $fc_k = 0$ for all $k < 0$ and

$$f^{s+1} = fc_0 + \sum_{k>0} (fc_k)(s+1)^k.$$

Since $X\backslash V = f^{-1}(0)$ is of measure 0, by using Lebesgue's theorem we get

$$\begin{aligned} \lim_{s \to -1} f^{s+1}(\Phi) &= \int_V \left(\lim_{s \to -1} f(x)^{s+1} \right) \Phi(x)\, dx \\ &= \int_V \Phi(x)\, dx = \int_X \Phi(x)\, dx = T_1(\Phi), \end{aligned}$$

hence $fc_0 = T_1 = 1$. We have only to take c_0 as T.

Corollary 5.5.1 *If P is any element of $\mathbb{C}[\partial/\partial x_1, \ldots, \partial/\partial x_n]\backslash\mathbb{C}$, then there exists an elementary solution for the differential operator P, i.e., an element S of $\mathcal{S}(X)'$ for $X = \mathbb{R}^n$ satisfying $PS = \delta_0$.*

In fact, we can write

$$P = \sum_{\alpha} (2\pi i)^{-|\alpha|} c_\alpha (\partial/\partial x)^\alpha$$

with c_α in $\mathbb{C}$. If we put $f(x) = \sum c_\alpha x^\alpha$, then by Theorem 5.5.1 we will have $fT = 1$ for some T in $\mathcal{S}(X)'$. If we put $S = T^*$, then S is in $\mathcal{S}(X)'$ and

$$PS = (fT)^* = 1^* = \delta_0.$$

A classical example of an elementary solution, sometimes called a "fundamental solution," is as follows: If Δ denotes the Laplacian and φ is in $\mathcal{D}(X)$ for $X = \mathbb{R}^n$, $n \neq 2$, then Poisson's formula

$$\Delta \cdot \int_X r(x-y)^{-n+2}\ \varphi(y)\ dy = -(n-2)\ \Omega_n\ \varphi(x)$$

can be proved by using Gauss' theorem. This shows that $-1/(n-2)\Omega_n r^{n-2}$ is an elementary solution for Δ. The readers can learn the significance and further examples of an elementary solution in Schwartz [51] and also in Gel'fand and Shilov [16].

https://doi.org/10.1090/amsip/014/06

Chapter 6

Prehomogeneous vector spaces

6.1 Sato's b-function $b(s)$

We shall explain M. Sato's theory of prehomogeneous vector spaces. More precisely, we shall only explain regular prehomogeneous vector spaces up to their b-functions. We start from the beginning: We say that a group G acts on a nonempty set X if there exists a map $G \times X \to X$ denoted by $(g, x) \mapsto gx$ satisfying $(gg')x = g(g'x)$, $1x = x$ for every g, g' in G and x in X. In that case for every ξ in X

$$G_\xi = \{g \in G;\ g\xi = \xi\}, \qquad G\xi = \{g\xi;\ g \in G\}$$

are called respectively the *fixer* of ξ in G and the *G-orbit* of ξ. We say that the action of G on X is transitive and also X is a *G-homogeneous space* if X itself is a G-orbit. In general, X becomes a disjoint union of G-orbits. We observe that G_ξ is a subgroup of G and the map $G \to X$ defined by $g \mapsto g\xi$ gives rise to a bijection from the coset space G/G_ξ to $G\xi$.

We shall now consider the case where $X = \mathbb{C}^n$ and G is a subgroup of $\mathrm{GL}_n(\mathbb{C})$ which is algebraic in the sense that it is the set of all common zeros of some polynomials in the n^2 entries of g with coefficients in $\mathbb{C}$. We shall assume that the closed topological subgroup G of $\mathrm{GL}_n(\mathbb{C})$ is connected. If we regard elements of X as column vectors, then G acts on X by matrix-multiplication. If X has a dense G-orbit, then (G, X) is called a *prehomogeneous vector space*. If further there exists an irreducible polynomial $f(x)$ in $\mathbb{C}[x_1, \ldots, x_n]$ such that $X \backslash f^{-1}(0)$ becomes a G-orbit, then the prehomogeneous vector space (G, X) is called *regular*.

Proposition 6.1.1 *If (G, X) is a regular prehomogeneous vector space with G acting transitively on $X \backslash f^{-1}(0)$, then $f(x)$ is homogeneous and it is a relative G-invariant in the sense that*

$$f(gx) = \nu(g) f(x)$$

for every g in G with ν in $\Omega(G) = Hom(G, \mathbb{C}^\times)$. Furthermore, if $F(x)$ is any relative G-invariant, then $F(x)$ is either 0 or a power of $f(x)$ up to a factor in $\mathbb{C}^\times$.

Proof. Since $X \backslash f^{-1}(0)$ is a G-orbit, every g in G keeps $f^{-1}(0)$ invariant, i.e., $gf^{-1}(0) = f^{-1}(0)$. Therefore if, for a moment, we put $f_g(x) = f(gx)$ then

$f_g^{-1}(0) = f^{-1}(0)$. We observe that $f_g(x)$ is also irreducible. Therefore by Hilbert's Nullstellensatz, we see that $f_g(x)$ and $f(x)$ divide each other, hence they differ by a factor $\nu(g)$ in $\mathbb{C}^\times$ necessarily satisfying $\nu(gg') = \nu(g)\nu(g')$ for every g, g' in G. Furthermore $\nu(g)$ is a polynomial in the entries of g, hence ν is continuous. Therefore ν is an element of $\Omega(G)$. If now $F(x)$ is any relative G-invariant different from 0, then $F^{-1}(0)$ is G-invariant. If $F^{-1}(0)$ intersects the G-orbit $X\backslash f^{-1}(0)$, then $F^{-1}(0)$ will contain $X\backslash f^{-1}(0)$, which is dense in X, hence $F(x) = 0$. Since this is not the case, $F^{-1}(0)$ is contained in $f^{-1}(0)$. Then by Hilbert's Nullstellensatz $F(x)$ divides $f(x)^e$ for some positive integer e. Since $f(x)$ is irreducible, this implies that $F(x)$ is a power of $f(x)$ up to a factor in $\mathbb{C}^\times$. Finally, write

$$f(x) = \sum_{i \geq d} f_i(x), \qquad f_d(x) \neq 0$$

with $f_i(x)$ homogeneous of degree i for all $i \geq d$. Then $f(gx) = \nu(g)f(x)$ implies $f_i(gx) = \nu(g)f_i(x)$ for every g in G and for all i. By what we have just shown, there exists a positive integer e satisfying $f_d(x) = cf(x)^e$ for some c in $\mathbb{C}^\times$. By comparing the degrees of both sides, we get $c = e = 1$ and $f_i(x) = 0$ for all $i > d$.

We call $f(x)$ in Proposition 6.1.1 a *basic relative invariant* of (G, X); it is unique up to a factor in $\mathbb{C}^\times$. We observe that if γ is an arbitrary element of $\mathrm{GL}_n(\mathbb{C})$, then $(\gamma G\gamma^{-1}, X)$ is also a regular prehomogeneous vector space with $(\gamma f)(x) = f(\gamma^{-1}x)$ as its basic relative invariant. We say that (G, X) and $(\gamma G\gamma^{-1}, X)$ are equivalent. This is clearly an equivalence relation. In the special case where γ, hence also γ^{-1}, is contained in the normalizer $N(G)$ of G, i.e., if $\gamma G\gamma^{-1} = G$, then $f(\gamma x)$ is another basic relative invariant of (G, X), hence it differs from $f(x)$ by a factor in $\mathbb{C}^\times$. Therefore, ν extends to $N(G)$ as $f(\gamma x) = \nu(\gamma)f(x)$ for every γ in $N(G)$.

We shall assume from now on that G is reductive. This condition is known to imply the existence of γ in $\mathrm{GL}_n(\mathbb{C})$ such that $\gamma G\gamma^{-1}$ is invariant under $g \mapsto {}^t g^{-1}$. Therefore we shall *simply assume* that G satisfies this condition, i.e., ${}^t G = G$. We keep in mind that $\gamma G\gamma^{-1}$ also satisfies this condition if and only if ${}^t\gamma\gamma$ is in $N(G)$.

Corollary 6.1.1 *If $f(x)$ is a basic relative invariant of (G, X), then there exists an element $B(s)$ of $\mathbb{C}[s]$ satisfying*

$$f(\partial/\partial x) \cdot f(x) = B(s).$$

If $B(s) \neq 0$, then $\deg(B) \leq \deg(f)$ and $\nu({}^t g) = \nu(g)$ for every g in G. Furthermore, $B(s)$ depends, up to a factor in $\mathbb{C}^\times$, only on the equivalence class of (G, X).

Proof. If $\deg(f) = d$, then by definition we can write

$$f(\partial/\partial x) \cdot f(x) = \phi_0(x) + \phi_1(x)s + \ldots + \phi_d(x)s^d$$

with $\phi_i(x)$ in $\mathbb{C}[x_1, \ldots, x_n, 1/f(x)]$ for $0 \leq i \leq d$. We shall obtain some information about the above expression assuming that it is different from 0. If we specialize s to an element k of $\mathbb{N}$, then we will have

$$f(\partial/\partial x)f(x)^{k+1} = \Big(\sum_{0 \leq i \leq d} \phi_i(x)k^i \Big) f(x)^k.$$

If we denote the LHS by $F_k(x)$, then in view of $\partial/\partial(gx) = {}^tg^{-1}(\partial/\partial x)$ we have

$$F_k(gx) = \chi(g)F_k(x), \qquad \chi(g) = \nu({}^tg)^{-1}\nu(g)^{k+1}$$

for every g in G. If we exclude at most d values of k, then $F_k(x) \neq 0$ and $\deg(F_k) = dk$. Therefore, by Proposition 6.1.1 we see that $F_k(x) = B(k)f(x)^k$ for some $B(k)$ in $\mathbb{C}^\times$. This implies $\chi(g) = \nu(g)^k$, hence $\nu({}^tg) = \nu(g)$ for every g in G. Furthermore, $\phi_0(x)+\phi_1(x)k+\ldots+\phi_d(x)k^d = B(k)$ for $d+1$ distinct k, in fact for infinitely many k, in $\mathbb{N}$, hence $\phi_i(x)$ is in $\mathbb{C}$ for $0 \leq i \leq d$. Finally, if γ is any element of $\mathrm{GL}_n(\mathbb{C})$ such that $g = {}^t\gamma\gamma$ is in $N(G)$, then by replacing x in $f(\partial/\partial x)\cdot f(x) = B(s)$ by $\gamma^{-1}x$ we get

$$(\gamma f)(\partial/\partial x)\cdot(\gamma f)(x) = \nu(g)^{-1}B(s).$$

Therefore the $B(s)$ for $(\gamma G\gamma^{-1}, X)$ is $\nu({}^t\gamma\gamma)^{-1}B(s)$.

We shall obtain more precise information about $B(s)$ after reviewing the following fact: If g is in $M_n(\mathbb{C})$, we denote by $\bar{g}$ the image of g under the complex-conjunction applied to its entries. If G is any subset of $M_n(\mathbb{C})$, we denote by $\bar{G}$ the image of G under $g \mapsto \bar{g}$. If now G is a connected reductive algebraic subgroup of $\mathrm{GL}_n(\mathbb{C})$, then by replacing G by $\gamma G\gamma^{-1}$ for some γ in $\mathrm{GL}_n(\mathbb{C})$ we can achieve not only ${}^tG = G$ but also $\bar{G} = G$. We refer to G.D. Mostow [43] for the details. In view of this situation, we shall proceed *simply assuming* that ${}^tG = \bar{G} = G$.

We order the set of monomials X^α for $\alpha = (\alpha_1, \ldots, \alpha_n)$ in $\mathbb{N}^n$ lexicographically. Since $\bar{G} = G$ and $\bar{X} = X$, we see that $\bar{f}(x)$ is also a basic relative invariant of (G, X), hence $\bar{f}(x)$ differs from $f(x)$ by a factor in $\mathbb{C}^\times$. If we normalize $f(x)$ by the condition that the coefficient of the highest monomial in $f(x)$ is 1, then we will have $\bar{f}(x) = f(x)$, i.e., $f(x)$ is in $\mathbb{R}[x_1, \ldots, x_n]$. This implies that $B(s)$ is in $\mathbb{R}[s]$. We shall prove two lemmas.

Lemma 6.1.1 *If $F(x) = \sum c_\alpha x_\alpha$ in $\mathbb{C}[x_1, \ldots, x_n]$ is homogeneous, then*

$$\bar{F}(\partial/\partial x)F(x) = \sum_\alpha \alpha!\ |c_\alpha|^2,$$

in which $\alpha! = \alpha_1!\cdots\alpha_n!$ with the understanding that $0! = 1$.

Proof. We have

$$\bar{F}(\partial/\partial x)F(x) = \sum_{\alpha,\beta} \bar{c}_\alpha c_\beta (\partial/\partial x)^\alpha x^\beta,$$

in which

$$(\partial/\partial x)^\alpha x^\beta = \prod_{1\leq i\leq n} \beta_i(\beta_i-1)\cdots(\beta_i-\alpha_i+1)x_i^{\beta_i-\alpha_i}$$

if $\beta_i \geq \alpha_i$ for all i; otherwise it is 0. Since $F(x)$ is homogeneous by assumption, we have $|\alpha| = |\beta| = \deg(F)$, hence $(\partial/\partial x)^\alpha x^\beta \neq 0$ implies $\alpha = \beta$ and $(\partial/\partial x)^\alpha x^\alpha = \alpha!$.

Lemma 6.1.2 *We have*

$$\log k! = k\log k(1+o(1)),$$

i.e., $\log k!/k\log k$ tends to 1, as $k \to \infty$.

Proof. This is an immediate consequence of Stirling's formula. In the above form it can be proved as follows: Since $\log t$ is a monotone increasing function of t for $t > 0$ and $\log t > 0$ for $t > 1$, if k is in $\mathbb{N}$ and $k > 1$, then

$$\log k! > \int_1^k \log t \; dt = k \log k - k + 1$$

on one hand and

$$\log k! < \int_2^{k+1} \log t \; dt = (k+1)\log(k+1) - k - 2\log 2 + 1$$

on another. We have only to put these together.

Theorem 6.1.1 *We have $B(s) = b_0 b(s)$, in which $b_0 > 0$ and $b(s)$ is a monic polynomial of degree $d = \deg(f)$ in $\mathbb{R}[s]$.*

Proof. If x^α is the highest monomial in $f(x)$, then its coefficient is 1 by the above normalization. Furthermore, $x^{\alpha(k+1)}$ is the highest monomial in $f(x)^{k+1}$ and

$$f(\partial/\partial x)^{k+1} f(x)^{k+1} = \prod_{0 \le j \le k} B(j)$$

for every k in $\mathbb{N}$. Since $f(x)$ is in $\mathbb{R}[x_1, \ldots, x_n]$, by Lemma 6.1.1 we get

$$f(\partial/\partial x)^{k+1} f(x)^{k+1} \ge \prod_{1 \le i \le n} (\alpha_i(k+1))!.$$

Since $|\alpha| = d$, by Lemma 6.1.2 we get

$$\log\Big(\prod_{1 \le i \le n} (\alpha_i(k+1))! \Big) = dk \log k(1 + o(1)),$$

hence

$$\prod_{0 \le j \le k} B(j) \ge \exp\{dk \log k(1 + o(1))\},$$

and hence

$$(*) \qquad \prod_{0 \le j \le k} B(j)/k^{\delta k} \to \infty$$

as $k \to \infty$ for any δ in $\mathbb{R}$ satisfying $\delta < d$. In particular $B(k) \ne 0$ for every k in $\mathbb{N}$ and if $b_0 s^{d_0}$ is the highest term in $B(s)$, then $d_0 > 0$. Furthermore, since $B(k) = b_0 k^{d_0}(1 + o(1))$ as $k \to \infty$, we also have $b_0 > 0$ and for any $b_1 > b_0$ there exists k_0 in $\mathbb{N}$ such that $B(k) \le b_1 k^{d_0}$ for all $k \ge k_0$. This implies

$$\prod_{0 \le j \le k} B(j) \le c \cdot b_1^k (k!)^{d_0}$$

for all $k \geq k_0$, in which c is independent of k. Therefore, by using $(*)$ we get $k \log k(d_0 - \delta + o(1)) \to \infty$ as $k \to \infty$, hence $d_0 \geq \delta$. Since δ is arbitrary in $\mathbb{R}$ subject to $\delta < d$, we get $d_0 \geq d$, hence $d_0 = d$ by $d_0 \leq d$.

The monic polynomial $b(s)$ in Theorem 6.1.1 depends only on the equivalence class of (G, X), and it is called *Sato's b-function* of (G, X). If $f(x)$ denotes the basic relative invariant of (G, X), then we see that its Bernstein polynomial $b_f(s)$ divides $b(s)$. Actually, they are known to be equal. We shall give a proof to this fact in section 6.3 after reviewing some major properties of the Γ-function.

6.2 The Γ-function (a digression)

A standard definition of the Γ-function $\Gamma(s)$ is

$$\Gamma(s) = \int_{x>0} x^s e^{-x}\, d\log x, \qquad \mathrm{Re}(s) > 0.$$

By using, e.g., Lemma 5.3.1, we see that $\Gamma(s)$ is a holomorphic function on $\mathbb{C}_0$. Furthermore, by integration by parts we see that

$$\Gamma(s+1) = s\Gamma(s)$$

for $\mathrm{Re}(s) > 0$. Since $\Gamma(1) = 1$ by definition, we conclude that $\Gamma(s)$ has a meromorphic continuation to $\mathbb{C}$ with a pole of order 1 at every point of $-\mathbb{N}$. These are well-known elementary properties of $\Gamma(s)$. Now by Weierstrass

$$s \cdot \prod (1 + s/n) e^{-s/n},$$

where the product is for $n = 1, 2, \ldots$, defines an entire function, i.e., a holomorphic function on the whole $\mathbb{C}$, with a zero of order 1 at every point of $-\mathbb{N}$. Therefore, the product of $\Gamma(s)$ and the above entire function is an entire function. A basic theorem on $\Gamma(s)$ states that if C is the *Euler constant* defined by

$$C = \lim_{n\to\infty} (1 + 1/2 + \ldots + 1/n - \log n),$$

then the product is $\exp(-Cs)$. Finally, if we put $\sigma = \mathrm{Re}(s)$, $t = \mathrm{Im}(s)$ so that $s = \sigma + it$ and restrict s as $|\sigma| \leq R$ for any $R > 0$, then

$$|\Gamma(s)| = (2\pi)^{1/2} |t|^{\sigma - 1/2} \exp(-(\pi/2)|t|)(1 + o(1))$$

with $o(1)$ uniform in σ as $|t| \to \infty$. Since the product-representation and the above important asymptotic behavior of $\Gamma(s)$ are seldom included in the basic course, we shall give their proofs. We shall follow the presentation by H. Mellin [40] because the proof by the Mellin transformation seems most appropriate.

Firstly if we express $\log n$ as the integral of $1/t$ from 1 to n and rewrite the n-th term of the sequence defining C as

$$\Big\{ \sum_{1 \leq k < n} 1/k - \log n \Big\} + 1/n = 1 - \Big\{ \log n - \sum_{1 < k \leq n} 1/k \Big\},$$

then we see that both $\{\cdot\}$ are positive and increase with n. Therefore, the sequence is between 0 and 1, and monotone decreasing, hence the limit C exists. In the following $\log(1+x)$ is defined for $|x| < 1$ by its power series expansion taking the value 0 at $x = 0$. We leave it as an exercise to show that if $|x| \le 1/2$, then $|\log(1+x) - x| \le |x|^2$. Also we keep in mind that $\mathrm{Re}(\log x) = \log|x|$ is well defined for every x in $\mathbb{C}^\times$. We now start with

$$1/G(s) = e^{Cs} s \cdot \prod_{n\ge 1} (1 + s/n) e^{-s/n}.$$

If $|s| \le R$ for any $R > 0$, then

$$|\log((1 + s/n)e^{-s/n})| \le (R/n)^2$$

for all $n \ge 2R$. Therefore, the above infinite product is absolutely and uniformly convergent for $|s| \le R$, hence it defines an entire function of s with a zero of order 1 at every point of $-\mathbb{N}$. Furthermore, if s is not in $-\mathbb{N}$, then

$$G(s+1)/G(s) = se^{-C} \cdot \lim_{n\to\infty} \Big\{ n/(s+n+1) \cdot \exp\big(\sum_{1\le k\le n} 1/k - \log n \big) \Big\} = s.$$

This implies

$$G(s+1) = sG(s)$$

for all s in $\mathbb{C}$. Since $1/sG(s)$ takes the value 1 at $s = 0$, we get $G(1) = 1$. Furthermore,

$$\pi/G(s)G(1-s) = -\pi/sG(s)G(-s) = \pi s \cdot \prod_{n\ge 1} (1 - (s/n)^2),$$

and the RHS is known in complex analysis to represent $\sin(\pi s)$, hence

$$G(s)G(1-s) = \pi/\sin(\pi s).$$

Since we have

$$\prod_{n\ge 1} (1 + 1/n)^s e^{-s/n} = \lim_{n\to\infty} \Big\{ (n+1)^s \exp\big(-(\sum_{1\le k\le n} 1/k)s \big) \Big\} = e^{-Cs},$$

we can also write

$$(*) \qquad G(s) = (1/s) \prod_{n\ge 1} (1 + 1/n)^s/(1 + s/n).$$

We shall prove the asymptotic formula for $G(s)$. Since $G(s)$ becomes its complex conjugate under the complex conjugation of s and

$$G(s)G(-s) = -\pi/(s \cdot \sin(\pi s)),$$

by replacing s by it we get

$$\begin{aligned} |G(it)| &= (2\pi)^{1/2} |t|^{-1/2} |e^{\pi t} - e^{-\pi t}|^{-1/2} \\ &= (2\pi)^{1/2} |t|^{-1/2} \exp(-(\pi/2)|t|)(1 + o(t)) \end{aligned}$$

as $|t| \to \infty$. In the general case we first observe that $(*)$ implies

$$G(\sigma + it)/G(it) = 1/(1 + \sigma/it) \cdot \prod_{n \geq 1} (1 + 1/n)^{\sigma}/(1 + \sigma/(n + it)),$$

hence

$$|G(\sigma + it)/|t|^{\sigma} G(it)| = \prod_{n \geq 0} |1 + 1/(n + it)|^{\sigma}/|1 + \sigma/(n + it)|,$$

and hence

$$\log(\ |G(\sigma + it)/|t|^{\sigma} G(it)|\ ) = \mathrm{Re}\Big\{ \sum_{n \geq 0} \sigma \log(1 + 1/(n + it)) - \log(1 + \sigma/(n + it)) \Big\}.$$

If now $|x|,\ |\sigma x| < 1$, then

$$\sigma \log(1 + x) - \log(1 + \sigma x) = x^2 P(x),$$

in which

$$P(x) = \sigma \cdot \sum_{k \geq 1} (-1)^k (1 - \sigma^k)/(k + 1) \cdot x^{k-1}$$

is absolutely convergent. Furthermore, if for $|\sigma| \leq R$ we replace x by $1/(n + it)$, where n is in $\mathbb{N}$ and $|t| \geq R + 1$, then $|x| \leq 1/(1 + R),\ |\sigma x| \leq 1/(1 + 1/R)$, hence $|P(x)| \leq M$ for some $M > 0$ depending only on R. Therefore, we get

$$\log(\ |G(\sigma + it)/|t|^{\sigma} G(it)|\ ) = \mathrm{Re}\Big\{ \sum_{n \geq 0} 1/(n + it)^2 \cdot P(1/(n + it)) \Big\},$$

in which

$$|\mathrm{RHS}| \leq M \cdot \sum_{n \geq 0} 1/(n^2 + t^2) \leq M t^{-2} (1 + \pi |t|/2),$$

hence

$$\begin{aligned} |G(\sigma + it)| &= |t|^{\sigma} |G(it)| (1 + o(1)) \\ &= (2\pi)^{1/2} |t|^{\sigma - 1/2} \exp(-(\pi/2)|t|)(1 + o(1)) \end{aligned}$$

with $o(1)$ uniform in σ as $|t| \to \infty$.

In order to show that $G(s) = \Gamma(s)$, we shall use the following consequence of Fourier's inversion formula:

Proposition 6.2.1 *Let $\varphi(x)$ denote a continuous function on $\mathbb{R}_+^{\times}$ such that the integral*

$$\phi(s) = \int_{x > 0} x^s \varphi(x)\ d \log x$$

is absolutely convergent for some $s = \sigma + it$; assume that $t \mapsto \phi(\sigma + it)$ is an integrable function on $\mathbb{R}$. Then we can recover $\varphi(x)$ from $\phi(s)$ as

$$\varphi(x) = \frac{1}{2\pi} \int_{\mathbb{R}} \phi(\sigma + it) x^{-\sigma - it}\ dt = \frac{1}{2\pi i} \int_{\sigma + i\mathbb{R}} \phi(s) x^{-s}\ ds.$$

Furthermore, if $t \mapsto \phi(s) = \phi(\sigma + it)$ is a continuous integrable function on $\mathbb{R}$ so that $\varphi(x)$ is defined by the second integral, then we can recover $\phi(s)$ by the first integral provided that it is absolutely convergent.

Proof. If we put $y = \log x/2\pi$, hence $x = \exp(2\pi y)$, and

$$\psi(y) = 2\pi x^\sigma \varphi(x),$$

then $\psi(y)$ becomes a continuous integrable function on $\mathbb{R}$ with its Fourier transform $\psi^*(t) = \phi(\sigma + it)$ also integrable on $\mathbb{R}$. Therefore by Proposition 5.5.1, we get $(\psi^*)^*(-y) = \psi(y)$. This implies the above proposition.

Now $G(s)$ is a meromorphic function on $\mathbb{C}$ with a pole of order 1 at every point of $-\mathbb{N}$. Furthermore, $G(s+1) = sG(s),\ G(1) = 1$ imply

$$\lim_{s \to -k} (s+k)G(s)x^{-s} = (-x)^k/k!$$

for every $x > 0$ and k in $\mathbb{N}$. The asymptotic formula for $G(\sigma + it)$ as $|t| \to \infty$ guarantees that $G(\sigma + it)$ is an integrable function of t if σ is not in $-\mathbb{N}$. We take $0 < \sigma < 1$ and determine

$$\varphi(x) = \frac{1}{2\pi i} \int_{\sigma + i\mathbb{R}} G(s)x^{-s}\ ds.$$

We take n from $\mathbb{N}$ and $R > 0$, and consider the following path of integration:

$$\sigma - i\,\infty \to \sigma - iR \to \sigma - n - iR \to \sigma - n + iR \to \sigma + iR \to \sigma + i\,\infty.$$

The asymptotic formula again shows that the integrals along the two horizontal paths tend to 0 as $R \to \infty$. Therefore by Cauchy's theorem we get

$$\varphi(x) = \sum_{0 \le k < n} (-x)^k/k! + \frac{1}{2\pi i} \int_{\sigma - n + i\mathbb{R}} G(s)x^{-s}\ ds,$$

in which

$$\left| \int_{\sigma - n + i\mathbb{R}} G(s)x^{-s}\ ds \right| \le\ x^{-\sigma} \cdot \int_{\mathbb{R}} |G(\sigma + it)|\ dt \cdot x^n\ /\ \prod_{1 \le k \le n} (k - \sigma).$$

Therefore, by taking the limit as $n \to \infty$ we get

$$\varphi(x) = \sum_{n \ge 0} (-x)^n/n! = e^{-x}.$$

We have chosen $0 < \sigma < 1$. However, since $G(s)$ is holomorphic on $\mathbb{C}_0$, by the above process of shifting the vertical line of integration we can replace σ by any positive real number. Therefore, by Proposition 6.2.1 we get

$$G(s) = \int_{x>0} x^s e^{-x}\ d\log x = \Gamma(s)$$

for every $\sigma > 0$ because the RHS is absolutely convergent.

6.3 $b(s) = b_f(s)$ and the rationality of the zeros

We go back to Sato's b-function $b(s)$ of (G, X). We have assumed or rather normalized under the equivalence that ${}^tG = \bar{G} = G$ and that the basic relative invariant $f(x)$ of (G, X) is in $\mathbb{R}[x_1, \dots, x_n]$. We know by Theorem 6.1.1 that

$$f(\partial/\partial x) \cdot f(x) = b_0 b(s),$$

in which $b_0 > 0$ and $b(s)$ is a monic polynomial of degree $d = \deg(f)$. By replacing $f(x)$ by $(b_0)^{-1/2} f(x)$ we can further normalize $b_0 = 1$ so that $f(x)$ becomes unique up to sign.

Theorem 6.3.1 *If we normalize the basic relative invariant $f(x)$ of (G, X) to satisfy*

$$f(\partial/\partial x) \cdot f(x) = b(s) = \prod_{\lambda} (s + \lambda),$$

then $Z(s)$ can be computed explicitly, i.e.,

$$\int_X |f(x)|_{\mathbb{C}}^s \exp(-2\pi {}^t x \bar{x})\ dx = (2\pi)^{-ds} \cdot \prod_{\lambda} (\Gamma(s + \lambda)/\Gamma(\lambda))$$

for $Re(s) > 0$, in which $X = \mathbb{C}^n$ and $\Gamma(\lambda) \neq \infty$ for all λ.

Proof. We recall that $Z(s)$ is the LHS of the formula to be proved. If we write

$$|f(x)|_{\mathbb{C}}^s = f(x)^s f(\bar{x})^s = b(s)^{-1} f(\partial/\partial x) f(x)^{s+1} f(\bar{x})^s$$

and apply the same argument as in the proof of Theorem 5.3.2, then we get

$$b(s)\ Z(s) = (2\pi)^d\ Z(s + 1)$$

for $\mathrm{Re}(s) > 0$. Therefore, if we put

$$C(s) = (2\pi)^{ds} Z(s)\ /\ \prod_{\lambda} \Gamma(s + \lambda),$$

then $C(s + 1) = C(s)$ for $\mathrm{Re}(s) > 0$. Since $Z(s)$ is a holomorphic function on $\mathbb{C}_0$, we see that $C(s)$ is a periodic holomorphic function on $\mathbb{C}$ with period 1. Therefore $C(s)$ becomes a meromorphic function of $z = \mathbf{e}(s)$ on $\mathbb{C}^\times$ and its Laurent expansion at 0 can be written as

$$C(s) = \sum_{k \in \mathbb{Z}} c_k z^k = \sum_{k \in \mathbb{Z}} c_k \mathbf{e}(ks),$$

in which

$$c_k = \exp(2\pi k t) \cdot \int_{\mathbb{R}/\mathbb{Z}} C(\sigma + it)\ \mathbf{e}(-k\sigma)\ d\sigma.$$

This implies

$$|c_k| \leq \exp(2\pi k t) \cdot \int_{\mathbb{R}/\mathbb{Z}} (2\pi)^{d\sigma} |Z(\sigma + it)|\ /\ \prod_{\lambda} |\Gamma(\sigma + it + \lambda)| \cdot d\sigma.$$

We shall estimate $|Z(s)|$ for $s = \sigma + it$ in $\mathbb{C}_0$. If in the integral defining $Z(s)$ we write

$$x = ru, \quad r = r(x) = ({}^t x\bar{x})^{1/2}, \quad dx = 2^n\ r^{2n-1}\ dr du$$

and put

$$\phi(s) = 2^{n-1} \cdot \int_{r(u)=1} |f(u)|_{\mathbb{C}}^s\ du,$$

then we have

$$Z(s) = (2\pi)^{-ds-n}\ \phi(s)\ \Gamma(ds+n).$$

Furthermore,

$$|\phi(s)| \le 2^{n-1} \cdot \int_{r(u)=1} |f(u)|_{\mathbb{C}}^\sigma\ du.$$

If we denote by M the maximum of the RHS say for $1 \le \sigma \le 2$, then we have

$$|Z(s)| \le (2\pi)^{-d\sigma-n}\ M\ |\Gamma(ds+n)|$$

for $1 \le \sigma \le 2$.

If now we incorporate the asymptotic formula

$$|\Gamma(\sigma+it)| = (2\pi)^{1/2}|t|^{\sigma-1/2} \exp(-(\pi/2)|t|)\ (1+o(1))$$

as $|t| \to \infty$, in which $o(1)$ is uniform in σ restricted to any finite interval, then we get

$$|c_k| \le M_1 \cdot |t|^{\sigma_1} \exp(2\pi k t)\ (1+o(1))$$

with M_1 independent of s and

$$\sigma_1 = n - (1/2)(1-d) - \sum_\lambda \mathrm{Re}(\lambda).$$

We have tacitly used the fact that

$$\exp\Big(-(\pi/2)\big(d|t| - \sum_\lambda |t + \mathrm{Im}(\lambda)|\big)\ \Big) \le \exp\Big((\pi/2)\sum_\lambda |\mathrm{Im}(\lambda)|\Big).$$

At any rate, if $k \ne 0$, then for $t = -\mathrm{sgn}(k)\tau$ and $\tau \to \infty$ we get $c_k = 0$, hence $C(s) = c_0$. We have thus shown that

$$Z(s) = (2\pi)^{-ds} \cdot \prod_\lambda \Gamma(s+\lambda) \cdot c_0$$

for $\mathrm{Re}(s) > 0$. If we take the limit as $s \to 0$, then $Z(s)$ tends to 1, hence $c_0 = \prod \Gamma(\lambda)^{-1}$. Since $c_0 \ne 0$, we have $\Gamma(\lambda)^{-1} \ne 0$ for all λ.

Theorem 6.3.2 *If $b(s)$ is the Sato b-function of a regular prehomogeneous vector space and $b_f(s)$ is the Bernstein polynomial of its basic relative invariant $f(x)$, then $b(s) = b_f(s)$. Furthermore, all its zeros are negative rational numbers, hence $b(s)$ is in $\mathbb{Q}[s]$.*

Proof. Since $b_f(s)$ divides $b(s)$, after changing the notation in Theorem 6.3.1 we write

$$b_f(s) = \prod_{\lambda}(s+\lambda), \quad b(s) = b_f(s) \cdot \prod_{\lambda'}(s+\lambda');$$

also we put

$$\gamma_f(s) = \prod_{\lambda}\Gamma(s+\lambda), \quad \gamma'(s) = \prod_{\lambda'}\Gamma(s+\lambda').$$

According to that theorem, $Z(s)$ and $\gamma_f(s)\gamma'(s)$ differ by a holomorphic function on $\mathbb{C}$ with no zeros. On the other hand we know by Theorem 5.3.2 that $Z(s)/\gamma_f(s)$ is a holomorphic function on $\mathbb{C}$, hence $\gamma'(s)$ is also a holomorphic function on $\mathbb{C}$. This implies $\gamma'(s) = 1$, hence $b(s) = b_f(s)$. We know furthermore, by Theorem 5.4.1, that the poles of $Z(s)$ are negative rational numbers. Therefore all zeros of $b(s)$ are negative rational numbers.

Actually the zeros of $b_f(s)$ are known to be negative rational numbers for an arbitrary $f(x)$ by M. Kashiwara [33]. We might mention that Theorem 6.3.1, in a weaker form, is in [27]. We shall explain its counterpart in the real case:

Proposition 6.3.1 *If $f(x)$ is normalized as in Theorem 6.3.1 and further if every monomial in $f(x)$ is of the form $x_{i_1}\dots x_{i_d}$ where $i_1 < \dots < i_d$, then $Z(s)$ can be computed explicitly, i.e.,*

$$\int_X |f(x)|_{\mathbb{R}}^s \exp(-\pi^t xx)\ dx = \pi^{-ds/2} \cdot \prod_{\lambda}\Big(\Gamma((s+\lambda)/2)\Big/\Gamma(\lambda/2)\Big)$$

for $Re(s) > 0$, in which $X = \mathbb{R}^n$.

Proof. This can be proved in the same way as Theorem 6.3.1. We have

$$b(s)Z(s) = (2\pi)^d Z(s+2)$$

for $\mathrm{Re}(s) > 0$, hence

$$Z(s) = \pi^{-ds/2} \cdot \prod_{\lambda}\Gamma((s+\lambda)/2) \cdot C(s),$$

in which $C(s)$ is a periodic holomorphic function on $\mathbb{C}$ with period 2. Therefore,

$$C(s) = \sum_{k\in\mathbb{Z}} c_k\ \mathbf{e}(ks/2), \quad c_k = (1/2)\exp(\pi kt) \cdot \int_{\mathbb{R}/2\mathbb{Z}} C(\sigma+it)\ \mathbf{e}(-k\sigma/2)\ d\sigma.$$

The above expression for c_k implies, similarly as before, that

$$|c_k| \le M_1\ |t|^{\sigma_1}\ \exp(\pi kt)\ (1+o(1))$$

for some $M_1 > 0$ and σ_1, which are independent of t, as $|t| \to \infty$. Therefore, we get $c_k = 0$ for $k \neq 0$, hence $C(s) = c_0$. Since $Z(s)$ tends to 1 as $s \to 0$, we necessarily have $c_0 = \prod \Gamma(\lambda/2)^{-1}$.

We shall discuss a *classical example* from various viewpoints. We start with the following general remark. If we replace the normalized $f(x)$ by $a_0 f(x)$ for any a_0 in $\mathbb{R}^\times$, then we will have

$$f(\partial/\partial x) \cdot f(x) = a_0^2 \; b(s)$$

while $Z(s)$ in Theorem 6.3.1 (resp. Proposition 6.3.1) will be multiplied by $|a_0|_{\mathbb{C}}^s$ (resp. $|a_0|_{\mathbb{R}}^s$). Now we observe that $(\mathrm{GL}_n(\mathbb{C}), M_n(\mathbb{C}))$ is a regular prehomogeneous vector space with $\det(x)$ as its basic relative invariant. Actually there is a notational discrepancy. In fact, if we arrange the n columns of an element of $M_n(\mathbb{C})$ in the natural order to make up an element of "X" $= \mathbb{C}^N$ for $N = n^2$, then we have to take the isomorphic image of $\mathrm{GL}_n(\mathbb{C})$ in $\mathrm{GL}_N(\mathbb{C})$ as "G." At any rate the normalization condition ${}^tG = \bar{G} = G$ is satisfied, the coefficients of $f(x) = \det(x)$ are in $\mathbb{R}$, in fact in $\mathbb{Z}$, and further it satisfies the condition in Proposition 6.3.1. Therefore we will have $\det(\partial/\partial x) \cdot \det(x) = b_0 b(s)$ for some $b_0 > 0$. We shall compute

$$Z(s) = \int_X |\det(x)|_{\mathbb{R}}^s \; \exp(-\pi \; \mathrm{tr}({}^t x x)) \; dx$$

directly, in which $X = M_n(\mathbb{R})$ and $\mathrm{tr}(y)$ for any square matrix y denotes the trace of y. We denote the above $Z(s)$ by $Z_n(s)$ and show by an induction on n that

$$Z_n(s) = \pi^{-ns/2} \cdot \prod_{1 \le k \le n} \Big(\Gamma((s+k)/2)\Big/\Gamma(k/2)\Big).$$

In doing so we shall use the well-known formula

$$\Omega_n/2 = \pi^{n/2}/\Gamma(n/2)$$

in calculus, which becomes $1 = \pi^{1/2}/\Gamma(1/2)$ for $n = 1$. We have

$$Z_1(s) = \pi^{-(s+1)/2}\Gamma((s+1)/2) = \pi^{-s/2}\Gamma((s+1)/2)/\Gamma(1/2).$$

If $n > 1$, we write $x = (x_1 \; x')$ with x' in $M_{n,n-1}(\mathbb{R})$ and put $x_1 = ru$, where $r = r(x_1)$, so that u is on the unit sphere and $dx_1 = r^{n-1} dr du$. Then we get

$$Z_n(s) = \int r^{s+n-1} \exp(-\pi r^2) \; dr du \Big\{ \int |\det(u \; x')|_{\mathbb{R}}^s \exp(-\pi \; \mathrm{tr}({}^t x' x')) \; dx' \Big\}.$$

Since the group of rotations in $\mathbb{R}^n$ acts transitively on the unit sphere, we can write $u = ge_1$, where $e_1 = {}^t(10\ldots0)$, for some g in $\mathrm{GL}_n(\mathbb{R})$ satisfying ${}^t gg = 1$. In the integral $\{\cdot\}$ above if we replace x' by gx', then it becomes $Z_{n-1}(s)$, hence

$$Z_n(s) = Z_{n-1}(s) \cdot (\Omega_n/2) \; \pi^{-(s+n)/2}\Gamma((s+n)/2).$$

If we apply the induction assumption to $Z_{n-1}(s)$, we get the above expression for $Z_n(s)$.

If we compare the above result with Proposition 6.3.1, then we get

$$(*) \qquad \det(\partial/\partial x) \cdot \det(x) = b(s) = \prod_{1 \le k \le n} (s+k)$$

in view of the following obvious fact. Namely if I, I' are finite subsets of $\mathbb{C}$ and $\phi(s)$ is a holomorphic function on $\mathbb{C}$ with no zeros satisfying

$$\prod_{\lambda\in I}\Gamma(s+\lambda)=\phi(s)\cdot\prod_{\lambda'\in I'}\Gamma(s+\lambda'),$$

then $I=I'$. This is a roundabout way of computing $b(s)$. At any rate by Theorem 6.3.1 we also have

$$\int_X|\det(x)|_{\mathbb{C}}^s\exp(-2\pi\,{}^t x\bar{x})\,dx=(2\pi)^{-ns}\cdot\prod_{1\le k\le n}(\Gamma(s+k)/\Gamma(k)),$$

where $X=M_n(\mathbb{C})$.

We might mention that $(*)$ follows from Capelli's identity in invariant theory, cf., e.g., H. Weyl [60]. It can also be proved, after R. Sasaki, as follows: If for $1\le i_1<\ldots<i_k\le n$, $1\le j_1<\ldots<j_k\le n$ we put

$$P_{i_1\ldots i_k,j_1\ldots j_k}=\det(\partial/\partial x_{i_\alpha j_\beta})_{1\le\alpha,\beta\le k}$$

and denote by $X_{i_1\ldots i_k,j_1\ldots j_k}$ the coefficient of $x_{i_1j_1}\ldots x_{i_kj_k}$ in $\det(x)$, then we will have

$$P_{i_1\ldots i_k,j_1\ldots j_k}\cdot\det(x)=\Big(\prod_{1\le i\le k}(s+i)\Big)X_{i_1\ldots i_k,j_1\ldots j_k}.$$

In fact, it is obvious for $k=1$ and the general case is by an induction on k ending up with $(*)$ for $k=n$. We might also mention that, as we shall see much later, an entirely similar method of computation of $Z(s)$ as above works in the p-adic case for a polynomial such as $\det(x)$.

In the case where a connected algebraic subgroup G of $\mathrm{GL}_n(\mathbb{C})$ is irreducible, i.e., $X=\mathbb{C}^n$ and 0 are the only G-invariant subspaces of X, then G is reductive by a theorem of E. Cartan. Furthermore, if G is transitive on $X\backslash f^{-1}(0)$ for some polynomial $f(x)$, then $f(x)$ is necessarily a power of an irreducible polynomial, hence we may assume that it is irreducible. At any rate, in such a case (G,X) is called an *irreducible regular prehomogeneous vector space*. There is a classification theory of prehomogeneous vector spaces by M. Sato and T. Kimura [49] which includes all such (G,X). Furthermore, the problem of making $b(s)$ explicit was investigated by M. Kashiwara, T. Kimura, M. Muro, T. Oshima, I. Ozeki, M. Sato, and T. Yano. In particular $b(s)$ is now known for all irreducible regular prehomogeneous vector spaces. We just mention the fundamental paper [50] by M. Sato and others, and the valuable paper [34] by T. Kimura.

https://doi.org/10.1090/amsip/014/07

Chapter 7

Totally disconnected spaces and p-adic manifolds

7.1 Distributions in totally disconnected spaces

We shall start with a review of some properties of totally disconnected spaces and groups. We say that a Hausdorff space is *totally disconnected* if points are the only connected subsets of X. If X is such a space, then every nonempty subset of X is also totally disconnected. The following lemma, in a more general form, is in L. S. Pontrjagin [45], p. 104:

Lemma 7.1.1 *Let X denote a locally compact space. Then X is totally disconnected if and only if for every point a of X the set $\mathcal{T}_a$ of all compact open subsets of X which contain a forms a base at a.*

Proof. Since the if-part is clear, we shall prove the only-if part. We shall first show that if X is a compact totally disconnected space, hence X is a member of $\mathcal{T}_a$, and if C denotes the intersection of all members of $\mathcal{T}_a$, then $C = \{a\}$. Otherwise C is not connected, hence it becomes a disjoint union of nonempty closed subsets F_1, F_2 of C. Since C is compact, they are also compact, hence closed in X. We may assume that F_1 contains a. Since X is normal, F_1, F_2 are respectively contained in some disjoint open subsets G_1, G_2 and the complement F of their union is compact. We shall include the possibility that F is empty. Since C and F are disjoint and since C is the intersection of all members of $\mathcal{T}_a$, which are compact, there exists a finite intersection A of members of $\mathcal{T}_a$ such that A and F are disjoint. Then A is a member of $\mathcal{T}_a$, and it becomes the disjoint union of $A_i = A \cap G_i$ for $i = 1, 2$. We observe that A_1, A_2 are compact open subsets of X and A_1 contains a, hence it is a member of $\mathcal{T}_a$. On the other hand A_1 and F_2 are disjoint, hence A_1 does not contain C. This is a contradiction.

We are ready to prove the lemma. We take any neighborhood U of a and show that U contains a member of $\mathcal{T}_a$. Since X is locally compact, we may assume that $\bar{U}$ is compact. Since $\bar{U}$ is totally disconnected and a is not in the compact subset $\partial U = \bar{U} \backslash U$, by the above result applied to $\bar{U}$ there exists a compact open subset A of $\bar{U}$ which contains a such that A and ∂U are disjoint. Then A is contained in U and it is a member of $\mathcal{T}_a$.

We shall prove one more lemma here; it is in A. Weil [56], p. 19 and also in Pontrjagin [45], pp. 149-150.

Lemma 7.1.2 *Let G denote a locally compact group. Then G is totally disconnected if and only if the set of all compact open subgroups of G forms a base at its unit element* 1.

Proof. Since the if-part is clear, we shall again prove the only-if part. We take any neighborhood U of 1. Then by Lemma 7.1.1 there exists a member A of $\mathcal{T}_1$ contained in U. We introduce a subset B of G as

$$B = \{g \in G;\ gA \subset A\}.$$

Then B contains 1 and, since A contains 1, B is contained in A. We shall show that B is open. If g is arbitrary in B, then for every a in A, since A is a neighborhood of ga, there exist neighborhoods $V_a,\ W_a$ of $g,\ a$ respectively such that V_aW_a is contained in A. Since A is compact, we can cover A by a finite number of W_a and if V is the intersection of the corresponding V_a, then V is a neighborhood of g and VA is contained in A. This shows that V is contained in B, hence B is open. We shall show that B is also closed. If g is arbitrary in $G\backslash B$, then ga is not in A for some a in A. Since $G\backslash A$ is a neighborhood of ga, there exists a neighborhood V of g such that Va is contained in $G\backslash A$. This shows that V is contained in $G\backslash B$, hence $G\backslash B$ is open, and hence B is closed.

We have thus shown that B is a closed and open subset of the compact open subset A, hence B is compact open, and hence B^{-1} is also compact open. Therefore, $N = B \cap B^{-1}$ is compact open, and N consists of all g in G satisfying $gA = A$. Therefore, N is also a subgroup of G contained in A, hence in U.

We shall now fix a locally compact totally disconnected space X and denote by $\mathcal{T}(X)$ the set of all compact open subsets of X in which we include the empty set $\emptyset$. We observe that $\mathcal{T}(X)$ is closed under the taking of finite union and intersection, and difference. A $\mathbb{C}$-valued function φ on X is called *locally constant* if every point of X has a neighborhood U such that the restriction $\varphi|U$ becomes a constant function on U. A locally constant function is a counterpart of a C^∞-function and it is clearly continuous. The set $\mathcal{D}(X)$ of all locally constant functions on X with compact support forms a vector space over $\mathbb{C}$. We observe that if A is a member of $\mathcal{T}(X)$, then its characteristic function χ_A is locally constant with A as its support. Therefore, the $\mathbb{C}$-span of the set of χ_A for all A in $\mathcal{T}(X)$ forms a subspace of $\mathcal{D}(X)$. Actually, they coincide. In fact, if φ is in $\mathcal{D}(X)$, then the image I of X under φ is a finite subset of $\mathbb{C}$ and

$$\varphi = \sum_{\alpha \in I} \alpha \chi_{\varphi^{-1}(\alpha)}.$$

We observe that $\varphi^{-1}(\alpha)$ for $\alpha \neq 0$ in I is a member of $\mathcal{T}(X)$ and $\mathrm{Supp}(\varphi)$ is the union of all such $\varphi^{-1}(\alpha)$. In particular, $\mathrm{Supp}(\varphi) = \{x \in X;\ \varphi(x) \neq 0\}$ for every φ in $\mathcal{D}(X)$.

We take a finite subset F of $\mathcal{T}(X)$ and denote by $\mathcal{D}_F$ the $\mathbb{C}$-span of the set of characteristic functions of all members of F. Then $\mathcal{D}(X)$ becomes the union or rather the direct limit of $\mathcal{D}_F$ for all F, hence $\mathcal{D}(X)$ has the direct limit topology defined as follows: Every finite dimensional vector space over $\mathbb{C}$, in particular $\mathcal{D}_F$ above, has the usual product topology of $\mathbb{C}$. We define a subset of $\mathcal{D}(X)$ to be open

if and only if its intersection with $\mathcal{D}_F$ is open in $\mathcal{D}_F$ for all F. Let $\mathcal{D}(X)'$ denote the topological dual of $\mathcal{D}(X)$ with the so-defined topology. Then, since every $\mathbb{C}$-linear function on $\mathcal{D}_F$ is continuous, we see that $\mathcal{D}(X)'$ coincides with the dual space of $\mathcal{D}(X)$. In particular, $\mathcal{D}(X)'$ is complete. We call elements of $\mathcal{D}(X)'$ *distributions* in X.

We shall give another description of distributions in X. If T is in $\mathcal{D}(X)'$, for every A in $\mathcal{T}(X)$ we put $T(A) = T(\chi_A)$. Then we get a $\mathbb{C}$-valued simply additive function T on $\mathcal{T}(X)$ in the sense that if A is a necessarily finite disjoint union of $A_1, A_2, \dots$ in $\mathcal{T}(X)$, then $T(A) = T(A_1) + T(A_2) + \dots$. Conversely, suppose that T is such a function. Express an arbitrary φ in $\mathcal{D}(X)$ as $\alpha_1\chi_{A_1} + \alpha_2\chi_{A_2} + \dots$ with $\alpha_1, \alpha_2, \dots$ in $\mathbb{C}$, in which $A_1, A_2, \dots$ are disjoint members of $\mathcal{T}(X)$. Then we define $T(\varphi)$ as $\alpha_1 T(A_1) + \alpha_2 T(A_2) + \dots$. We shall show that $T(\varphi)$ is well defined. Suppose that $\beta_1\chi_{B_1} + \beta_2\chi_{B_2} + \dots$ is a similar expression of φ, and put $C_{ij} = A_i \cap B_j$ for all i, j. Then we get

$$\varphi = \sum_{i,j} \alpha_i \chi_{C_{ij}} = \sum_{i,j} \beta_j \chi_{C_{ij}}$$

with $\alpha_i = \beta_j$ for $C_{ij} \neq \emptyset$. Therefore, by the simple additivity of T we get

$$\sum_i \alpha_i T(A_i) = \sum_{i,j} \alpha_i T(C_{ij}) = \sum_{i,j} \beta_j T(C_{ij}) = \sum_j \beta_j T(B_j).$$

Furthermore, if φ, ψ are arbitrary in $\mathcal{D}(X)$, by a similar argument as above we can express φ, ψ as $\mathbb{C}$-linear combinations of characteristic functions of the same set of disjoint members of $\mathcal{T}(X)$. Then for any α, β in $\mathbb{C}$ we clearly have $T(\alpha\varphi + \beta\psi) = \alpha T(\varphi) + \beta T(\psi)$, hence T gives an element of $\mathcal{D}(X)'$. We have thus shown that distributions in X and simply additive functions on $\mathcal{T}(X)$ can be identified.

We shall discuss extensions and restrictions of distributions. We express X as a disjoint union of nonempty open and closed subsets Y and F, respectively. Then both Y and F are locally compact totally disconnected spaces. Furthermore we have an exact sequence of $\mathbb{C}$-linear maps:

$$(*) \qquad 0 \to \mathcal{D}(Y) \to \mathcal{D}(X) \to \mathcal{D}(F) \to 0.$$

In detail, if ψ is an element of $\mathcal{D}(Y)$, then the function ψ^X defined as

$$\psi^X\big|Y = \psi, \qquad \psi^X\big|F = 0$$

is an element of $\mathcal{D}(X)$; and if φ is an element of $\mathcal{D}(X)$, then $\varphi|F$ is an element of $\mathcal{D}(F)$. The point is that the above sequence defined by $\psi \mapsto \psi^X$ and $\varphi \mapsto \varphi|F$ is exact. Clearly, $\mathcal{D}(Y) \to \mathcal{D}(X)$ is injective. Suppose that φ in $\mathcal{D}(X)$ has the property that $\varphi|F = 0$. Then $\mathrm{Supp}(\varphi)$ is contained in Y, hence $\varphi = (\varphi|Y)^X$. This is the exactness at $\mathcal{D}(X)$. We shall show that $\mathcal{D}(X) \to \mathcal{D}(F)$ is surjective. We have only to show that if A_0 is an arbitrary member of $\mathcal{T}(F)$, there exists a member A of $\mathcal{T}(X)$ satisfying $\chi_A|F = \chi_{A_0}$, i.e., $A \cap F = A_0$. Since A_0 is an open subset of F, it can be expressed as an intersection of F and an open subset U of X. Take x arbitrarily from A_0. Then by Lemma 7.1.1 we can find a compact neighborhood V_x of x contained in U. Since A_0 is compact, it can be covered by a

finite number of V_x. If we denote by A the union of such V_x, then A is in $\mathcal{T}(X)$ and $A_0 = A \cap F$. Therefore, $(*)$ is indeed an exact sequence. Since every subspace of a vector space over a field has a supplement, i.e., another subspace so that the vector space becomes their direct sum, by dualizing $(*)$ we get a similar exact sequence. We shall formulate it as a proposition.

Proposition 7.1.1 *Let X denote a locally compact totally disconnected space and express it as a disjoint union of nonempty open and closed subsets Y and F, respectively. Then we have an exact sequence of $\mathbb{C}$-linear maps:*

$$0 \to \mathcal{D}(F)' \to \mathcal{D}(X)' \to \mathcal{D}(Y)' \to 0.$$

If T_0 is any element of $\mathcal{D}(F)'$, its image T_0^X in $\mathcal{D}(X)'$ is defined as $T_0^X(\varphi) = T_0(\varphi|F)$ for every φ in $\mathcal{D}(X)$, and if T is any element of $\mathcal{D}(X)'$, its image $T|Y$ in $\mathcal{D}(Y)'$ is defined as $(T|Y)(\psi) = T(\psi^X)$ for every ψ in $\mathcal{D}(Y)$.

We might mention that Proposition 7.1.1 holds trivially if either Y or F becomes $\emptyset$. At any rate, we accept the fact that for every T in $\mathcal{D}(X)'$, there exists the largest open subset $O(T)$ of X satisfying $T|O(T) = 0$ and define the support of T as $\mathrm{Supp}(T) = X \backslash O(T)$. Then Proposition 7.1.1 implies the following corollary:

Corollary 7.1.1 *If T is in $\mathcal{D}(X)'$ and $T \neq 0$, then there exists a unique T_0 in $\mathcal{D}(\mathrm{Supp}(T))'$ such that $T = T_0^X$.*

The existence of $O(T)$ can be proved by a partition of unity, which is as follows: Let C denote a compact subset of X which is covered by a family of open subsets U_α of X. Then there exists a finite set $\{A_i;\ i \in I\}$ of mutually disjoint members A_i of $\mathcal{T}(X)$ with each A_i contained in some U_α such that

$$\sum_{i \in I} \chi_{A_i}(x) = 1$$

for every x in C. The proof is quite simple. At every x in C we can find by Lemma 7.1.1 a compact neighborhood V_x of x contained in some U_α. Since C is compact, it can be covered by a finite number of V_x, say $W_1, W_2, \ldots$. We have only to put

$$A_i = W_i \backslash (W_1 \cup \ldots \cup W_{i-1})$$

for $i = 1, 2, \ldots$. We shall prove the existence of $O(T)$. Define $O(T)$ as the union of all open subsets Y of X such that $T|Y = 0$. We have only to show that $T(\varphi) = 0$ for every φ in $\mathcal{D}(X)$ with $\mathrm{Supp}(\varphi)$ contained in $O(T)$. If we apply the partition of unity to $C = \mathrm{Supp}(\varphi)$ and $U_\alpha = Y$ above, then we get

$$\varphi = \sum_{i \in I} \varphi \chi_{A_i}, \qquad T(\varphi) = \sum_{i \in I} T(\varphi \chi_{A_i}) = 0$$

because $\mathrm{Supp}(\varphi \chi_{A_i})$ is contained in A_i, hence in W_i, and hence in some Y.

7.2 The case of homogeneous spaces

We shall consider the case where a locally compact totally disconnected space X is continuously acted upon by a locally compact totally disconnected group G. We shall first show that $\Omega(G) = \mathrm{Hom}(G, \mathbb{C}^\times)$ consists of all locally constant homomorphisms from G to $\mathbb{C}^\times$. We have only to show that if ρ is any continuous homomorphism from G to $\mathbb{C}^\times$, then ρ is locally constant. We choose a small neighborhood of 1 in $\mathbb{C}^\times$ which does not contain any subgroup other than 1. We can, e.g., define U as $|a-1|<1$. By Lemma 7.1.2 there exists a compact open subgroup H of G such that $\rho(H)$ is contained in U. By the choice of U we then have $\rho(H)=1$. Since ρ is a homomorphism, it takes the value $\rho(g)$ on gH for every g in G.

After this remark we define the action of G on $\mathcal{D}(X)$ and $\mathcal{D}(X)'$ in the usual way, i.e., as

$$(g\cdot\varphi)(x)=\varphi(g^{-1}x), \qquad (g\cdot T)(\varphi)=T(g^{-1}\cdot\varphi)$$

for every g in G, x in X, and φ, T respectively in $\mathcal{D}(X), \mathcal{D}(X)'$. We keep in mind that $g\cdot\chi_A=\chi_{gA}$ for every g in G and A in $\mathcal{T}(X)$.

Lemma 7.2.1 *Let T denote an element of $\mathcal{D}(X)'$ satisfying*

$$g\cdot T=\rho(g)^{-1}T$$

with $\rho(g)$ in $\mathbb{C}^\times$ for every g in G and assume that $T\neq 0$. Then necessarily ρ is in $\Omega(G)$.

Proof. Since ρ clearly gives a homomorphism from G to $\mathbb{C}^\times$, it will be enough to show that $\rho|N=1$ for some open subgroup N of G. Since $T\neq 0$, we have $T(\varphi)\neq 0$ for some φ in $\mathcal{D}(X)$, hence $T(\chi_A)\neq 0$ for some $A\neq\emptyset$ in $\mathcal{T}(X)$. As in the proof of Lemma 7.1.2 we see that if $B=\{g\in G;\ gA\subset A\}$, then $N=B\cap B^{-1}$ is an open subgroup of G and $gA=A$, i.e., $g\cdot\chi_A=\chi_A$, for every g in N. This implies

$$\rho(g)T(\chi_A)=(g^{-1}\cdot T)(\chi_A)=T(g\cdot\chi_A)=T(\chi_A).$$

Since $T(\chi_A)\neq 0$, therefore, we get $\rho(g)=1$ for every g in N.

We shall review some basic theorems about Haar measures on locally compact groups and homogeneous spaces. We shall do so only in the totally disconnected case but with proof. A *measure* μ on X is an element of $\mathcal{D}(X)'$ satisfying $\mu(A)=\mu(\chi_A)\geq 0$ for every A in $\mathcal{T}(X)$. If φ is in $\mathcal{D}(X)$ we shall write

$$\mu(\varphi)=\int_X\varphi(x)\mu(x)=\int_X\varphi(x)\ d\mu(x).$$

By definition we have

$$\left|\int_X\varphi(x)\mu(x)\right|\leq\int_X|\varphi(x)|\mu(x)\leq\mu(\mathrm{Supp}(\varphi))\|\varphi\|_\infty$$

for every φ in $\mathcal{D}(X)$. In fact, if we express φ as $\sum a_i\chi_{A_i}=a_1\chi_{A_1}+a_2\chi_{A_2}+\dots$ with $a_1,a_2,\dots$ in $\mathbb{C}$, in which $A_1,A_2,\dots$ are disjoint members of $\mathcal{T}(X)$, then

$$|\mu(\varphi)|=|\sum\mu(A_i)a_i|\leq\sum\mu(A_i)|a_i|=\mu(|\varphi|)\leq\mu(\mathrm{Supp}(\varphi))\max\{|a_i|\}.$$

Therefore, if a sequence $\{\varphi_i\}$ in $\mathcal{D}(X)$ has the property that $\mu(|\varphi_i - \varphi_j|) \to 0$ as $i, j \to \infty$, then $\{\mu(\varphi_i)\}$ forms a Cauchy sequence in $\mathbb{C}$. In that case we say that φ_i converges to Φ as $i \to \infty$ and define its integral as the limit of $\mu(\varphi_i)$:

$$\int_X \Phi(x)\mu(x) = \lim_{i\to\infty} \int_X \varphi_i(x)\mu(x).$$

The above Φ is symbolic, but it can be interpreted as an integrable function on X. We shall not give further details to this well-known extension process of μ except for the following remark: If φ is a $\mathbb{C}$-valued continuous function on X with compact support, we can find a sequence $\{\varphi_i\}$ in $\mathcal{D}(X)$ with $\mathrm{Supp}(\varphi_i)$ contained in a fixed member of $\mathcal{T}(X)$ satisfying $\|\varphi_i - \varphi\|_\infty \to 0$ as $i \to \infty$. This implies $\|\varphi_i - \varphi_j\|_\infty \to 0$, hence $\mu(|\varphi_i - \varphi_j|) \to 0$ as $i, j \to \infty$. In such a case we identify the above symbolic Φ with φ.

We also mention that *Fubini's theorem* is quite simple in the totally disconnected case. If ν is a measure on a space Y similar to X and A, B are respectively in $\mathcal{T}(X)$, $\mathcal{T}(Y)$ and if $\varphi = \chi_A \otimes \chi_B$, i.e., $\varphi(x, y) = \chi_A(x)\chi_B(y)$ for every (x, y) in $X \times Y$, then

$$\int_X \Big(\int_Y \varphi(x, y)\nu(y) \Big)\ \mu(x) = \int_Y \Big(\int_X \varphi(x, y)\mu(x) \Big)\ \nu(y)$$

because both sides are equal to $\mu(A)\nu(B)$. If we accept the fact that $\mathcal{D}(X \times Y)$ is the $\mathbb{C}$-span of the set of functions of the form $\chi_A \otimes \chi_B$, then the above formula holds for every φ in $\mathcal{D}(X \times Y)$. Now we have seen that $\mathcal{D}(X \times Y)$ is the $\mathbb{C}$-span of the set of χ_C for all C in $\mathcal{T}(X \times Y)$ and we observe that every such C is a finite union of its subsets of the form $A \times B$. Therefore we have only to observe further that any intersection of sets of the form $A \times B$ is of that form and that if $A_1, \ldots, A_n$ are subsets of any set, the characteristic function of their union is the sum of the characteristic function of the intersection of $A_{i_1}, \ldots, A_{i_p}$ with the sign $(-1)^{p-1}$ for all $i_1 < \ldots < i_p$.

Now G continuously acts on G by left multiplication, i.e., as $g_0 \cdot g = g_0 g$. A *Haar measure* μ_G or simply μ on G is a G-invariant measure different from 0. We shall show that it exists and is unique up to a factor in $\mathbb{R}_+^\times$. We observe that if we have a finite number of members $A, B, \ldots$ of $\mathcal{T}(G)$, they can be expressed as disjoint unions of cosets gN by one compact open subgroup N of G. In fact, by Lemma 7.1.2 and by the compactness of $A, B, \ldots$ they can be expressed as finite unions of $g_i N_i$, where every N_i is a compact open subgroup of G. We can then take as N any compact open subgroup of G contained in all N_i. After this remark, we fix a compact open subgroup N_0 of G, choose N for A and $B = N_0$, and put

$$\mu(A) = \mathrm{card}(A/N)\ /\ \mathrm{card}(N_0/N),$$

in which, e.g., $\mathrm{card}(A/N)$ denotes the number of distinct cosets gN in A. Then $\mu(A)$ is well defined, i.e., it is independent of the choice of N, and $\mu(gA) = \mu(A)$ for every g in G. Furthermore, μ is a simply additive function on $\mathcal{T}(G)$. Therefore, μ is a Haar measure on G normalized as $\mu(N_0) = 1$. We observe that if T is any G-invariant element of $\mathcal{D}(G)'$, the above argument shows that $T(A) = T(N_0)\mu(A)$

for every A in $\mathcal{T}(G)$, i.e., $T = T(N_0)\mu$, with $T(N_0)$ in $\mathbb{C}$. If T is a Haar measure on G, then $T(N_0)$ is in $\mathbb{R}_+^\times$.

If μ is a Haar measure on G and g is in G, then $\mu'(A) = \mu(Ag)$ also gives a Haar measure on G, hence by the uniqueness we will have

$$\mu(Ag) = \Delta_G(g)\ \mu(A)$$

with $\Delta_G(g)$ in $\mathbb{R}_+^\times$ independent of A. If we define a new continuous action of G on G as $g_0 \cdot g = gg_0^{-1}$, then we can write $g \cdot \mu = \Delta_G(g)\mu$. Therefore by Lemma 7.2.1 we see that Δ_G, called the *module* of G, gives a locally constant homomorphism from G to $\mathbb{R}_+^\times$. We shall show that

$$\mu(A^{-1}) = \int_A \Delta_G(g^{-1})\ \mu(g)$$

for every A in $\mathcal{T}(G)$. We express A as a disjoint union of g_iN, in which N is a compact open subgroup of G such that $\Delta_G|N = 1$. Then A^{-1} becomes the disjoint union of Ng_i^{-1}, hence

$$\begin{aligned}\mu(A^{-1}) &= \sum_i \mu(Ng_i^{-1}) = \sum_i \Delta_G(g_i^{-1})\ \mu(N) \\ &= \sum_i \int_{g_iN} \Delta_G(g^{-1})\ \mu(g) = \int_A \Delta_G(g^{-1})\ \mu(g).\end{aligned}$$

Since

$$\chi_A(gg_0^{-1}) = \chi_{Ag_0}(g), \qquad \chi_A(g^{-1}) = \chi_{A^{-1}}(g),$$

the above properties of μ can also be expressed as

$$\int_G \varphi(gg_0^{-1})\ \mu(g) = \Delta_G(g_0) \int_G \varphi(g)\ \mu(g),$$

$$\int_G \varphi(g^{-1})\Delta_G(g^{-1})\ \mu(g) = \int_G \varphi(g)\ \mu(g)$$

for $\varphi = \chi_A$, hence for every φ in $\mathcal{D}(G)$.

We take an arbitrary closed subgroup H of G, hence H need not be compact or open, and consider the coset space G/H. Then $p(g) = gH$ for every g in G gives a surjection $p : G \to G/H$. We call a subset of G/H open if its preimage under p is open in G. The family of open subsets of G/H so defined is closed under the taking of arbitrary union and finite intersection, hence it converts G/H into a topological space. Furthermore p is open in the sense that it maps an open set to an open set. If $g_1H \neq g_2H$ for some g_1, g_2 in G, then 1 is not in $g_1Hg_2^{-1}$, hence $G\backslash g_1Hg_2^{-1}$ is a neighborhood of 1. By Lemma 7.1.2 there exists a compact open subgroup N of G contained in $G\backslash g_1Hg_2^{-1}$. Then N and $g_1Hg_2^{-1}$ are disjoint, hence $p(Ng_1)$ and $p(Ng_2)$ are disjoint, and hence G/H is a Hausdorff space. Furthermore, $p(Ng)$ is a compact neighborhood of $p(g)$ for every g in G and the set of $p(Ng)$ for all compact open subgroups N of G forms a base of $p(g)$. We could have

used gN instead of Ng above. At any rate we have shown that G/H is a locally compact totally disconnected space. We observe that G continuously acts on G/H as $g_0 \cdot p(g) = p(g_0 g)$. The action is transitive and p is equivariant.

Since H is a closed subgroup of G, it is also a locally compact totally disconnected group. Therefore H has a Haar measure μ_H. If φ is in $\mathcal{D}(G)$, then $\varphi(gh)$ as a function of h is in $\mathcal{D}(H)$, hence

$$\pi(\varphi)(gH) = \int_H \varphi(gh)\ \mu_H(h)$$

is defined for every g in G. In particular, if N is a compact open subgroup of G, then for any g_0 in G we can take $\chi_{g_0 N}$ as φ, and we get

$$\pi(\chi_{g_0 N})(gH) = \int_H \chi_{g_0 N}(gh)\ \mu_H(h).$$

If gh is in $g_0 N$, then g is in $g_0 NH$. In that case, the RHS becomes $\mu_H(H \cap N)$, hence

$$\pi(\chi_{g_0 N}) = \mu_H(H \cap N)\chi_{g_0 NH}.$$

This formula implies that π gives an equivariant $\mathbb{C}$-linear surjection from $\mathcal{D}(G)$ to $\mathcal{D}(G/H)$. In the following proposition $\mathcal{E}_X(\rho)$ denotes the vector space over $\mathbb{C}$ of all T in $\mathcal{D}(X)'$ satisfying $g \cdot T = \rho(g)^{-1}T$ for every g in G.

Proposition 7.2.1 *Let G denote a locally compact totally disconnected group, H a closed subgroup of G, and ρ an element of $\Omega(G)$. Then $\mathcal{E}_{G/H}(\rho) \neq 0$ if and only if*

$$\rho\Delta_G \big| H = \Delta_H.$$

In that case $\dim_{\mathbb{C}}(\mathcal{E}_{G/H}(\rho)) = 1$ and $\mathcal{E}_{G/H}(\rho)$ has a basis T_0 defined by

$$T_0(\pi(\varphi)) = \int_G \rho(g)\varphi(g)\mu(g)$$

for every φ in $\mathcal{D}(G)$.

Proof. This can be proved in the same way as the statement in italics on p. 45 in A. Weil [56]. Suppose that $T \neq 0$ is in $\mathcal{E}_{G/H}(\rho)$ and define S in $\mathcal{D}(G)'$ as $S(\varphi) = T(\pi(\varphi))$ for every φ in $\mathcal{D}(G)$. Then S is in $\mathcal{E}_G(\rho)$ and $S_1(\varphi) = S(\rho^{-1}\varphi)$ defines an element S_1 of $\mathcal{E}_G(1)$. Since $S_1 \neq 0$ by $T \neq 0$, we have $S_1 = c\mu$ for some c in $\mathbb{C}^\times$, hence $T(\pi(\varphi)) = c\mu(\rho\varphi)$. In particular, $\dim_{\mathbb{C}}(\mathcal{E}_{G/H}(\rho)) = 1$. If we take h_0 arbitrarily from H and replace $\varphi(g)$ by $\varphi_1(g) = \varphi(gh_0^{-1})$, then we get $\pi(\varphi_1) = \Delta_H(h_0)\pi(\varphi)$, hence

$$T(\pi(\varphi_1)) = \Delta_H(h_0)T(\pi(\varphi)), \qquad \mu(\rho\varphi_1) = \rho(h_0)\Delta_G(h_0)\mu(\rho\varphi).$$

This implies $\Delta_H(h_0) = \rho(h_0)\Delta_G(h_0)$, hence $\rho\Delta_G|H = \Delta_H$.

We shall show that if $\rho\Delta_G|H = \Delta_H$, then $T_0(\pi(\varphi)) = \mu(\rho\varphi)$ gives a well-defined element T_0 of $\mathcal{D}(G/H)'$. That will complete the proof because then T_0 is in $\mathcal{E}_{G/H}(\rho)$.

We have only to show therefore that $\pi(\varphi) = 0$ implies $\mu(\rho\varphi) = 0$. Now $\pi(\varphi) = 0$ implies

$$\int_H \varphi(gh^{-1})\Delta_H(h^{-1})\mu_H(h) = \int_H \varphi(gh)\mu_H(h) = 0$$

for every g in G. If we take any θ from $\mathcal{D}(G)$, multiply $(\rho\theta)(g)$ to the LHS of the above equation and integrate over G, then by using Fubini's theorem we get

$$\int_H \Delta_H(h^{-1})\Big\{ \int_G (\rho\theta)(g)\ \varphi(gh^{-1})\ \mu(g)\Big\}\ \mu_H(h) = 0,$$

in which

$$\int_G (\rho\theta)(g)\ \varphi(gh^{-1})\ \mu(g) = \Delta_G(h) \int_G (\rho\theta)(gh)\ \varphi(g)\ \mu(g).$$

Therefore, by using $\Delta_H(h) = \rho(h)\Delta_G(h)$ and Fubini's theorem again we get

$$\int_G (\rho\varphi)(g)\Big\{ \int_H \theta(gh)\ \mu_H(h)\Big\}\mu(g) = 0.$$

If we choose A from $\mathcal{T}(G)$ which contains $\mathrm{Supp}(\varphi)$, e.g., $A = \mathrm{Supp}(\varphi)$, and specialize θ to any element of $\mathcal{D}(G)$ satisfying $\pi(\theta) = \chi_{AH}$, then we finally get $\mu(\rho\varphi) = 0$.

We shall prove another proposition for our later use. As we have remarked in Chapter 5.1, if G is a compact group, then $\mathrm{Hom}(G, \mathbb{R}_+^\times) = 1$, hence $\Omega(G) = \mathrm{Hom}(G, \mathbb{C}_1^\times)$. If further G is commutative, then elements of $\Omega(G)$ are called *characters* of G. We keep in mind that if G is a finite abelian group, then G is isomorphic to a product of cyclic groups, hence $\Omega(G)$ and G have the same order.

Proposition 7.2.2 *Let G denote a compact totally disconnected abelian group and μ_G its Haar measure normalized as $\mu_G(G) = 1$; define an inner product (φ, φ') of every φ, φ' in $\mathcal{D}(G)$ as*

$$(\varphi, \varphi') = \int_G \varphi(g)\psi(g)\mu_G(g),$$

in which $\psi(g)$ is the complex conjugate of $\varphi'(g)$. Then $\Omega(G)$ forms an orthonormal basis for $\mathcal{D}(G)$, i.e., $(\chi, \chi') = 1$ or 0 according as $\chi = \chi'$ or $\chi \neq \chi'$ for every χ, χ' in $\Omega(G)$ and every φ in $\mathcal{D}(G)$ can be expressed as a finite sum

$$\varphi = \sum_{\chi \in \Omega(G)} c_\chi \chi$$

with $c_\chi = (\varphi, \chi)$ for every χ in $\Omega(G)$.

Proof. We shall first prove the orthonormality of $\Omega(G)$. Since $(\chi, \chi) = 1$ is clear, we shall show that $(\chi, \chi') = 0$ for $\chi \neq \chi'$. Since the complex conjugate of $\chi(g)$ is $\chi(g)^{-1}$, we have only to show that $I = (\chi, 1)$ represents 0 for $\chi \neq 1$. Now $\chi \neq 1$ means $\chi(g_0) \neq 1$ for some g_0 in G. If we replace $\chi(g)$ in the integral I by $\chi(g_0 g)$, then the new integral is still I because μ_G is a Haar measure and also equal to $\chi(g_0)I$ because $\chi(g_0 g) = \chi(g_0)\chi(g)$, hence $I = 0$. We shall show that $\Omega(G)$ is complete,

i.e., it spans $\mathcal{D}(G)$. Take φ arbitrarily from $\mathcal{D}(G)$. Since φ is locally constant, by Lemma 7.1.2 for every g in G there exists a compact open subgroup H_g of G such that $\varphi|gH_g$ becomes a constant function on gH_g. Since G is compact, it can be covered by a finite number of gH_g. Let H denote any compact open subgroup of G contained in all such H_g. Then φ becomes a $\mathbb{C}$-valued function on the finite abelian group G/H. We observe that the dimension over $\mathbb{C}$ of the vector space of all such φ is equal to the order of G/H, which is equal to the order of $\Omega(G/H)$ considered as a subgroup of $\Omega(G)$. The orthonormality implies that elements of $\Omega(G/H)$ are linearly independent over $\mathbb{C}$, hence they form a basis for the above vector space. Therefore, φ can be expressed as a linear combination of elements of $\Omega(G/H)$ with coefficients as stated.

We might mention that in the notation of Proposition 7.2.2 we have the following *Plancherel formula*:

$$\int_G |\varphi(g)|^2 \mu_G(g) = \sum_{\chi \in \Omega(G)} |c_\chi|^2.$$

Proposition 7.2.2 will be used mostly as

$$(\chi, 1) = \int_G \chi(g) \mu_G(g) = 0$$

for $\chi \neq 1$. We shall refer to this fact as the *orthogonality of characters*.

7.3 Structure of eigendistributions

We start with *Baire's theorem* in general topology. We say that a locally compact space X is *countable at* ∞ if X can be expressed as a union of countably many, i.e., at most countably many, compact subsets $F_1, F_2, \ldots$. The theorem then states that at least one F_i contains a nonempty open subset of X. For the sake of completeness we shall give a proof in the case where X is totally disconnected. Suppose otherwise and choose $A_1 \neq \emptyset$ from $\mathcal{T}(X)$. Assume by induction that $A_1 \supset \ldots \supset A_i$ has been chosen from $\mathcal{T}(X)$ such that $A_i \neq \emptyset$ and A_i is disjoint from $F_1, \ldots, F_{i-1}$ for some $i \geq 1$. Since $A_i \backslash F_i$ is nonempty and open by assumption, by Lemma 7.1.1 it contains $A_{i+1} \neq \emptyset$ in $\mathcal{T}(X)$. Then A_{i+1} is disjoint from $F_1, \ldots, F_i$. Therefore, the induction is complete. If now A_∞ denotes the intersection of all A_i, then A_∞ is nonempty and it is disjoint from F_i for all i, hence with their union, which is X. We thus have a contradiction.

We shall next recall a theorem of L. S. Pontrjagin. Let G denote a locally compact group acting continuously and transitively on a locally compact space X; let ξ denote any point of X and H the fixer of ξ in G. Then H is a closed subgroup of G and the continuous map $f : G \to X$ defined by $f(g) = g\xi$ gives rise to an equivariant continuous bijection $f_0 : G/H \to X$. The theorem states that if G is countable at ∞, then f_0 is bicontinuous. We shall again give a proof in the case where G and X are totally disconnected. We have only to show that f_0, or, equivalently, f is an open map. Namely if U is any nonempty open subset of G, then $f(U)$ is open in X. An arbitrary point of $f(U)$ can be written as $f(g) = g\xi$ for some

g in U. Since $g^{-1}U$ is a neighborhood of $1 = 1^{-1}1$, by Lemma 7.1.2 we can find a compact open subgroup N of G such that $N^{-1}N$ is contained in $g^{-1}U$. Since G is countable at ∞ by assumption, there exists a countable subset $\{g_i;\ i \in I\}$ of G such that G becomes the union of g_iN, hence X becomes the union of $f(g_iN) = g_if(N)$, for all i in I. Since the action of G on X is bicontinuous, every $g_if(N)$ is compact, hence X is countable at ∞, and hence by Baire's theorem $g_if(N)$ for some i contains a nonempty open subset of X. Then $f(N)$ itself contains a nonempty open subset say V of X. Take any point of V and express it as $f(g_0) = g_0\xi$ for some g_0 in N. Then $W = gg_0^{-1}V$ becomes a neighborhood of $g\xi = f(g)$ in X and by definition

$$W \subset gg_0^{-1}f(N) \subset gf(g_0^{-1}N) \subset gf(g^{-1}U) = f(U).$$

Therefore, $f(U)$ is open in X.

We have separated, for the sake of clarity, the following lemma from the next theorem; the proof will be given only in the totally disconnected case.

Lemma 7.3.1 *Let G denote a locally compact group acting continuously on a locally compact space X; assume that G is countable at ∞ and the number of G-orbits in X is countable. Then there exists an open orbit, i.e., a G-orbit which is open in X. Furthermore for every ξ in X the G-orbit $G\xi$ is the unique open orbit in its closure in X and if H is the fixer of ξ in G, then G/H is bicontinuous to $G\xi$ under $gH \mapsto g\xi$.*

Proof. If N is any compact open subgroup of G, since G is countable at ∞ by assumption, there exists a countable subset $\{g_i;\ i \in I\}$ of G such that G becomes the union of g_iN for all i in I. Also by assumption, we can choose a countable set of representatives $\{\xi_j;\ j \in J\}$ of all G-orbits in X. Then X becomes the union of countably many compact subsets $g_iN\xi_j$ for all i, j. Therefore, by Baire's theorem $g_iN\xi_j$ for some i, j contains a nonempty open subset of X. This implies that $N\xi_j$ contains a nonempty open subset say V of X. Then $G\xi_j$ for that j becomes the union of gV for all g in G, hence $G\xi_j$ is an open orbit. If for any ξ in X we put $Y = G\xi$, then G acts on the closure $\bar{Y}$ of Y in X. Since $\bar{Y}$ is locally compact and the number of G-orbits in $\bar{Y}$ is countable, we can apply the above observation to $\bar{Y}$ instead of X. We see that $\bar{Y}$ contains an open orbit say Y_0. If $Y \neq Y_0$, then they are disjoint, hence Y is contained in $\bar{Y}\backslash Y_0$. Since Y_0 is open in $\bar{Y}$, $\bar{Y}\backslash Y_0$ is closed in $\bar{Y}$, hence in X, and hence $\bar{Y}$ is contained in $\bar{Y}\backslash Y_0$. This is a contradiction. Therefore Y is the unique open orbit in $\bar{Y}$. The last part of the lemma follows from Pontrjagin's theorem.

We also make the following remark. Let G denote a locally compact totally disconnected group acting continuously on a locally compact totally disconnected space X. Then for every g in G, φ in $\mathcal{D}(X)$, and T in $\mathcal{D}(X)'$, we have

$$\mathrm{Supp}(g \cdot \varphi) = g \cdot \mathrm{Supp}(\varphi), \qquad \mathrm{Supp}(g \cdot T) = g \cdot \mathrm{Supp}(T).$$

Therefore, if T is in $\mathcal{E}_X(\rho)$ for some ρ in $\Omega(G)$, then $\mathrm{Supp}(T)$ is G-invariant. If now X is a disjoint union of closed and open subsets F and Y, respectively, and if they are G-invariant, then the $\mathbb{C}$-linear maps in the dual exact sequences

$$0 \to \mathcal{D}(Y) \to \mathcal{D}(X) \to \mathcal{D}(F) \to 0, \qquad 0 \to \mathcal{D}(F)' \to \mathcal{D}(X)' \to \mathcal{D}(Y)' \to 0$$

are all equivariant. For instance, if g is in G and T_0, T are respectively in $\mathcal{D}(F)'$, $\mathcal{D}(X)'$, then

$$(g \cdot T_0)^X = g \cdot T_0^X, \qquad (g \cdot T)\big|Y = g \cdot (T\big|Y).$$

The verifications are all straightforward. In particular, T_0^X is in $\mathcal{E}_X(\rho)$ if and only if T_0 is in $\mathcal{E}_F(\rho)$, and $T|Y$ is in $\mathcal{E}_Y(\rho)$ if T is in $\mathcal{E}_X(\rho)$.

Theorem 7.3.1 *Suppose that G is a locally compact totally disconnected group which is countable at ∞ and that it acts continuously with countably many orbits on a locally compact totally disconnected space X; suppose further that T is in $\mathcal{E}_X(\rho)$, i.e., T is an element of $\mathcal{D}(X)'$ satisfying $g \cdot T = \rho(g)^{-1}T$ for every g in G, and $T \neq 0$. Put $F =$Supp(T) and write $T = T_0^X$ for a unique T_0 in $\mathcal{D}(F)'$; choose ξ from any open orbit in F and denote by H the fixer of ξ in G. Then T_0 is in $\mathcal{E}_F(\rho)$, hence $T_0|G\xi$ is in $\mathcal{E}_{G\xi}(\rho)$, and $T_0|G\xi \neq 0$. Therefore*

$$\mathcal{E}_{G\xi}(\rho) = \mathbb{C}(T_0\big|G\xi), \qquad \rho\Delta_G\big|H = \Delta_H.$$

Furthermore, if μ_G, μ_H denote Haar measures on G, H and π the $\mathbb{C}$-linear surjection from $\mathcal{D}(G)$ to $\mathcal{D}(G\xi)$ defined by

$$(\pi(\varphi))(g\xi) = \int_H \varphi(gh)\ \mu_H(h),$$

then

$$(T_0\big|G\xi)(\pi(\varphi)) = c \cdot \int_G \rho(g)\varphi(g)\ \mu_G(g)$$

for every φ in $\mathcal{D}(G)$ with c in $\mathbb{C}^\times$ independent of φ.

Proof. In view of Lemma 7.3.1, the above remark, and Proposition 7.2.1, we have only to show that $T_0|G\xi \neq 0$. Suppose that $T_0|G\xi = 0$ and choose an open subset U of X satisfying $U \cap F = G\xi$. If we put $V = U \cup O(T)$, then V is open in X. Furthermore, if φ is in $\mathcal{D}(X)$ with Supp(φ) contained in V, then

$$\text{Supp}(\varphi\big|F) \subset V \cap F = U \cap F = G\xi,$$

hence $T(\varphi) = T_0^X(\varphi) = T_0(\varphi|F) = 0$ by the assumption that $T_0|G\xi = 0$. Therefore, $T|V = 0$, hence V is contained in $O(T)$, and hence U is contained in $O(T)$. This implies that $G\xi$ is empty, which is a contradiction.

We might mention that we have been motivated by A. Weil [58], Chapter 3, Lemma 16. An example of locally compact totally disconnected spaces which are not countable at ∞ is $\mathbb{R}$ but with discrete topology. We keep in mind that every locally compact space which is separable, i.e., has a countable base of open sets, is countable at ∞. We also keep in mind that the condition $\rho\Delta_G|H = \Delta_H$ will never be satisfied if $\rho|H$ is not $\mathbb{R}_+^\times$-valued.

7.4 Integration on p-adic manifolds

We take a complete field K with respect to a non-archimedean absolute value $|\cdot|_K$. We have already used such a field in Chapter 2.2. In the same notation as at that place we impose the following condition:

AV 4. The factor ring $O_K/\pi O_K$ is a finite field $\mathbb{F}_q$ with q elements.
We call such a K a *p-adic field* and normalize $|\cdot|_K$ once and for all as

$$|\pi|_K = q^{-1}$$

We observe that if we choose a subset R of O_K which is mapped bijectively to $\mathbb{F}_q$ under $O_K \to O_K/\pi O_K$, then K becomes the set of all series of the form

$$a = \sum_{i \geq k} a_i \pi^i = \pi^k (a_k + a_{k+1}\pi + \dots)$$

with $a_k, a_{k+1}, \dots$ in R for some k in $\mathbb{Z}$ depending on a. In particular, O_K is the set of all a above for $k = 0$, hence O_K becomes bijective to the product R^∞ under the correspondence $a \mapsto (a_0, a_1, \dots)$. We recall that K is a topological field and $\pi^i O_K$ for all i in $\mathbb{N}$ form a base at 0. Therefore, if R^∞ is equipped with the product topology, then the bijection $O_K \to R^\infty$ becomes bicontinuous, hence O_K is compact by Tychonoff's theorem. We could have said that O_K is the inverse limit of the sequence of finite rings $O_K/\pi O_K$, $O_K/\pi^2 O_K \dots$, hence O_K is a compact ring. At any rate, since $\pi^i O_K$ are compact open subgroups of the additive group K for all i in $\mathbb{Z}$ with K as their union, we see that K is a locally compact totally disconnected group which is countable at ∞. This implies that K^n is also such a group. We shall normalize its Haar measure as $\mu(O_K^n) = 1$ and denote it sometimes by μ_n and also by dx. We observe that every K-analytic manifold X for such a K or simply a *p-adic manifold* is locally compact and totally disconnected. In the following we shall explain the process of associating a measure to any K-analytic differential form on X of the highest degree. We shall start with an elementary divisor theorem.

We denote by $\mathrm{GL}_n(O_K)$ the subgroup of $\mathrm{GL}_n(K)$ consisting of all g in $M_n(O_K)$ with $\det(g)$ in $O_K^\times$. If we denote by 1_n the unit element of $\mathrm{GL}_n(K)$, then $1_n + \pi M_n(O_K)$ is a compact open normal subgroup of $\mathrm{GL}_n(O_K)$ with a finite factor group. Therefore, $\mathrm{GL}_n(O_K)$ is a compact open subgroup of $\mathrm{GL}_n(K)$. Furthermore, it contains all permutation matrices, i.e., matrices of determinant ± 1 with each row containing 1 once and having 0 for the remaining $n-1$ entries.

Lemma 7.4.1 *Every element a of $M_{m,n}(K)$ can be expressed as $a = gdg'$, in which g, g' are respectively in $\mathrm{GL}_m(O_K)$, $\mathrm{GL}_n(O_K)$ and d is a diagonal matrix, i.e., the (i,j)-entries are 0 for all $i \neq j$, such that its diagonal entries are powers of π with increasing exponents in $\mathbb{Z} \cup \infty$ and with the understanding that $\pi^\infty = 0$.*

Proof. After replacing a by ${}^t a$ if necessary, we may assume that $m \geq n$. Since we can take $d = 0$ if $a = 0$, we shall assume that $a \neq 0$. If $\pi^e u$ is an entry of a with u in $O_K^\times$ and with the smallest e, then after replacing a by $(\pi^e u)^{-1} a$ and multiplying $\pi^e u$ later, we may assume that a is in $M_{m,n}(O_K)$ with 1 as one of its entries. After multiplying permutation matrices from both sides, we may further assume that a has 1 as its $(1,1)$-entry. We express a by its entry matrices $a_{11} = 1$ and $1 \times (n-1)$, $(m-1) \times 1$, $(m-1) \times (n-1)$ matrices a_{12}, a_{21}, a_{22}. If we denote by g_1 the element of $\mathrm{GL}_m(O_K)$ with $1,\ 0,\ a_{21},\ 1_{m-1}$ as its entry matrices and by g_1' the element of $\mathrm{GL}_n(O_K)$ with $1,\ a_{12},\ 0,\ 1_{n-1}$ as its entry matrices, then we will have

$$a = g_1 a_1 g_1',$$

in which the entry matrices of a_1 are 1, 0, 0, a^* with $a^* = a_{22} - a_{21}a_{12}$. We have tacitly assumed that $n > 1$. If $n = 1$, then we simply have $g_1' = 1$. At any rate, by using elements of $\mathrm{GL}_m(O_K), \mathrm{GL}_n(O_K)$ with entry matrices of the form 1, 0, 0, g^* with g^* respectively in $\mathrm{GL}_{m-1}(O_K), \mathrm{GL}_{n-1}(O_K)$ we can simplify a^* in the same way as above, i.e., by an induction on n.

Lemma 7.4.2 *We have*

$$\mu_n(gA) = |\det(g)|_K \ \mu_n(A)$$

for every g in $\mathrm{GL}_n(K)$ and A in $\mathcal{T}(K^n)$.

Proof. We shall use general observations in section 7.2, especially Lemma 7.2.1. If we let $\mathrm{GL}_n(K)$ act on K^n by matrix-multiplication, then we will have

$$g^{-1} \cdot \mu_n = \rho(g)\ \mu_n, \qquad \text{i.e.,}\ \ \mu_n(gA) = \rho(g)\ \mu_n(A)$$

for every g in $\mathrm{GL}_n(K)$ and A in $\mathcal{T}(K^n)$ with ρ in $\mathrm{Hom}(\mathrm{GL}_n(K), \mathbb{R}_+^\times)$. If we write $g = \gamma d \gamma'$ with $\gamma,\ \gamma'$ in $\mathrm{GL}_n(O_K)$ by Lemma 7.4.1, since $\rho|\mathrm{GL}_n(O_K) = 1$ by the compactness of $\mathrm{GL}_n(O_K)$, we get $\rho(g) = \rho(d)$. We similarly have $|\det(g)|_K = |\det(d)|_K$. If $\pi^{e_1}, \dots, \pi^{e_n}$ are the diagonal entries of d, we choose e from $\mathbb{N}$ such that $e + e_i \geq 0$ for all i. Then, by using $\mathrm{card}(O_K/\pi^e O_K) = q^e = |\pi^e|_K^{-1}$, we get

$$\begin{aligned} \rho(d) = \mu_n(dO_K^n) &= \mathrm{card}(dO_k^n/\pi^e dO_K^n) \ / \ \mathrm{card}(O_K^n/\pi^e dO_K^n) \\ &= \prod_{1 \leq i \leq n} |\pi^{e_i}|_K = |\det(d)|_K, \end{aligned}$$

hence $\rho(g) = |\det(g)|_K$.

In the following lemma an SRP in $x_1, \dots, x_n$ is, as we have defined in Chapter 2.2, an element of $K[[x_1, \dots, x_n]]$ with the coefficient c_i of x^i in $\pi^{|i|-1}O_K$ for all $i \neq 0$ in $\mathbb{N}^n$ and $c_0 = 0$.

Lemma 7.4.3 *(i) Suppose that $f(x)$ in $O_K[[x_1, \dots, x_n]]$ is convergent at some a in O_K^n and $e > 0$ is in $\mathbb{N}$. Then*

$$g(x) = \pi^{-e}\big(f(a + \pi^e x) - f(a)\big)$$

is an SRP in $x_1, \dots, x_n$. (ii) If every $f_i(x)$ in $f(x) = (f_1(x), \dots, f_n(x))$ is an SRP in $x_1, \dots, x_n$ and

$$\partial(f_1, \dots, f_n)/\partial(x_1, \dots, x_n) \not\equiv 0 \bmod \pi,$$

then the bicontinuous map from O_K^n to itself defined by $y = f(x)$ is measure preserving.

Proof of (i). By assumption $f(x) = \sum c_i x^i$ with c_i in O_K for all i in $\mathbb{N}^n$, hence

$$f(a + \pi^e x) = f(a) + \sum_{|i| \geq 1} d_i (\pi^e x)^i$$

with d_i in O_K, and hence

$$g(x) = \sum_{|i|\geq 1} \pi^{k_i} d_i x^i,$$

in which $k_i = e(|i| - 1) \geq |i| - 1$ for all $i \neq 0$. Therefore, $g(x)$ is an SRP in $x_1, \ldots, x_n$.

Proof of (ii). We have only to show that the image of $a + \pi^e O_K^n$ under $y = f(x)$ is $f(a) + \pi^e O_K^n$ for every a in O_K^n and $e > 0$ in $\mathbb{N}$ because then

$$\mu_n(f(a) + \pi^e O_K^n) = \mu_n(\pi^e O_K^n) = \mu_n(a + \pi^e O_K^n),$$

hence $y = f(x)$ is measure preserving. We know by Corollary 2.2.1 that the inverse of $y = f(x)$ has a similar form as $y = f(x)$. Therefore, we have only to show that $f(a + \pi^e b)$ is contained in $f(a) + \pi^e O_K^n$ for every b in O_K^n. If we put $g(x) = \pi^{-e}(f(a + \pi^e x) - f(a))$, then the entries of $g(x)$ are all SRP's in $x_1, \ldots, x_n$ by (i), hence they are convergent at every b in O_K^n. Therefore, $g(b)$ is in O_K^n, hence $f(a + \pi^e b)$ is in $f(a) + \pi^e O_K^n$ for every b in O_K^n.

We are ready to prove a *change of variable formula* in the p-adic case. The formula is identical to the well-known formula in the archimedean case.

Proposition 7.4.1 *If every $f_i(x)$ in $f(x) = \big(f_1(x), \ldots, f_n(x)\big)$ is K-analytic around some point a of K^n and*

$$\partial(f_1, \ldots, f_n)/\partial(x_1, \ldots, x_n)(a) \neq 0$$

so that $y = f(x)$ gives a K-bianalytic map from a neighborhood U of a to a neighborhood V of $b = f(a)$, then

$$dy = |\partial(f_1, \ldots, f_n)/\partial(x_1, \ldots, x_n)|_K \; dx$$

with the understanding that $dx = \mu_n|U$ and $dy = \mu_n|V$.

Proof. We first observe that if the formula is valid on some small neighborhood of every point of U, then it is valid on U. Therefore, in proving the formula we can make U smaller if necessary. Also if the formula is valid for $y = f(x)$ and for a similar map $z = g(y)$, then by the chain rule of the jacobian it is valid for the composite map $z = g(f(x))$. Now the formula is valid for $y = gx + a$, in which g is in $\mathrm{GL}_n(K)$ and a is in K^n, this by Lemma 7.4.2 and by the fact that μ_n is a Haar measure on K^n. Also the formula is valid by Lemma 7.4.3 if every $f_i(x)$ is an SRP in $x_1, \ldots, x_n$ of the form

$$f_i(x) = x_i + \sum_{|j|\geq 2} c_{ij} x^j$$

for $1 \leq i \leq n$. Therefore, in the general case we may assume that $f_i(x)$ is of the above form with c_{ij} in K for all i, j. Since every $f_i(x)$ is a convergent power series by assumption, there exists e_0 in $\mathbb{N}$ such that $c_{ij}\pi^{e_0|j|}$ tends to 0 as $|j| \to \infty$ for $1 \leq i \leq n$. Then there exists e_1 in $\mathbb{N}$ such that

$$c_{ij}{}' = \pi^{e_1} \cdot c_{ij}\pi^{e_0|j|}$$

is in O_K for all i, j. If we choose $e \geq 2e_0 + e_1 + 1$ from $\mathbb{N}$ and put

$$g_i(x) = \pi^{-e} f_i(\pi^e x) = x_i + \sum_{|j| \geq 2} c_{ij}'' x^j,$$

we will have

$$c_{ij}'' = \pi^{k_j} \cdot \pi^{|j|-1} c_{ij}',$$

in which

$$k_j = (e - e_0 - 1)(|j| - 1) - e_0 - e_1 \geq (e_0 + e_1)(|j| - 2) \geq 0$$

for all $|j| \geq 2$. Therefore, as we have remarked, the formula is valid for $x \mapsto g(x) = (g_1(x), \ldots, g_n(x))$. Since $y = f(x)$ is the composition of $x \mapsto \pi^{-e}x,\ x \mapsto g(x),\ x \mapsto \pi^e x$, the formula is valid for $y = f(x)$.

After the above preparation, suppose that we have an n-dimensional p-adic manifold X defined by an atlas $\{(U, \phi_U)\}$ and a K-analytic differential form α of degree n on X; put $\phi_U(x) = (x_1, \ldots, x_n)$ for every x in U. Then $\alpha|U$ has an expression of the form

$$\alpha(x) = f_U(x)\ dx_1 \wedge \cdots \wedge dx_n,$$

in which f_U is a K-analytic function on U. If A is any member of $\mathcal{T}(X)$ small enough to be contained in U, then we define its measure $\mu_\alpha(A)$ as

$$\begin{aligned} \mu_\alpha(A) &= \int_A |f_U(x)|_K\ \mu_n(\phi_U(x)) \\ &= \sum_{e \in \mathbb{Z}} q^{-e} \cdot \mu_n\big\{\phi_U(f_U^{-1}(\pi^e O_K^\times) \cap A)\big\}. \end{aligned}$$

We observe that the above series is convergent because $f_U(A)$ is a compact subset of K, hence a subset of $\pi^{-e_0} O_K$ for some large e_0 in $\mathbb{N}$, and then the summation is restricted as $e \geq -e_0$. The point is that if $(U', \phi_{U'})$ is another chart and if A is also contained in U', then we will have the same $\mu_\alpha(A)$ relative to that chart. In fact, if $\phi_{U'}(x) = (x_1', \ldots, x_n')$, then

$$f_{U'}(x)\ \partial(x_1', \ldots, x_n')/\partial(x_1, \ldots, x_n) = f_U(x),$$

$$\mu_n(\phi_{U'}(x)) = |\partial(x_1', \ldots, x_n')/\partial(x_1, \ldots, x_n)|_K\ \mu_n(\phi_U(x))$$

for every x in $U \cap U'$, the first by definition and the second by Proposition 7.4.1. Therefore, we indeed have

$$\int_A |f_{U'}(x)|_K\ \mu_n(\phi_{U'}(x)) = \int_A |f_U(x)|_K\ \mu_n(\phi_U(x)).$$

If now A is arbitrary in $\mathcal{T}(X)$, we first express A as a disjoint union of small $A_1, A_2, \ldots$ in $\mathcal{T}(X)$ such that every A_i is contained in some U above depending on i, and then define $\mu_\alpha(A)$ as $\mu_\alpha(A) = \mu_\alpha(A_1) + \mu_\alpha(A_2) + \ldots$. In this way we get a well-defined measure μ_α on X, i.e., a simply additive function μ_α on $\mathcal{T}(X)$ such that $\mu_\alpha(A) \geq 0$ for every A in $\mathcal{T}(X)$. The measure μ_α is also denoted by $d\mu_\alpha$, $|\alpha|_K$, etc. At any rate, by the general procedure explained in sections 7.1 and 7.2 the integral of any φ in $\mathcal{D}(X)$ by μ_α is also defined.

7.5 Serre's theorem on compact p-adic manifolds

We shall explain a theorem of J.-P. Serre [52] which describes the structure of an arbitrary compact p-adic manifold by its invariant. The proof is by p-adic integration and short, and yet the result is very remarkable. We shall start with the following lemma:

Lemma 7.5.1 *Let K denote a p-adic field and X any compact n-dimensional K-analytic manifold for $n > 0$. Then X is K-bianalytic to the disjoint union $r \cdot O_K^n$ of r copies of O_K^n for some $0 < r < q$.*

Proof. We take an atlas $\{(U, \phi_U)\}$ on X. We may assume that every U is a compact open subset of X. Since X is compact by assumption, it is covered by a finite number of U's, say $U_1, U_2, \ldots$. After replacing $U_1,\ U_2,\ U_3,\ \ldots$ by $U_1,\ U_2 \backslash U_1,\ U_3 \backslash (U_1 \cup U_2),\ \ldots$, we may assume that they are disjoint. We know that each $\phi_U(U)$ for $U = U_1,\ U_2,\ \ldots$ is a disjoint union of a finite number of subsets of K^n of the form $a + \pi^e O_K^n$ for some a in K^n and e in $\mathbb{Z}$. We observe that O_K^n is K-bianalytic to $a + \pi^e O_K^n$ under $x \mapsto y = a + \pi^e x$. Therefore, X is K-bianalytic to $r \cdot O_K^n$ for some $r > 0$ in $\mathbb{N}$. If now $\{c_1, c_2, \ldots, c_q\}$ is a subset of O_K which is mapped bijectively to $\mathbb{F}_q$ under $c \mapsto c \bmod \pi$, then O_K becomes the disjoint union of $c_i + \pi O_K$ for $1 \leq i \leq q$. Therefore, O_K is K-bianalytic to $q \cdot O_K$, hence $O_K^n = O_K^{n-1} \times O_K$ is K-bianalytic to $q \cdot O_K^n$ for every $n > 0$. If we write the above r as $r = (q-1)i + r_0$ with i in $\mathbb{N}$ and $0 < r_0 < q$, then by an induction on i we see that X is K-bianalytic to $r_0 \cdot O_K^n$.

If X is any n-dimensional K-analytic manifold and α is a K-analytic differential form on X of degree n, then for any chart (U, ϕ_U) on X with $\phi_U(x) = (x_1, \ldots, x_n)$ we can write

$$\alpha(x) = f_U(x)\ dx_1 \wedge \cdots \wedge dx_n,$$

in which f_U is a K-analytic function on U. We say that α is a *gauge form* on X if f_U is $K^\times$-valued for every U. We are ready to state and prove the following theorem of Serre.

Theorem 7.5.1 *Suppose that K is a p-adic field, $n > 0$, and X is a compact n-dimensional K-analytic manifold. Then X possesses a gauge form α and $\mu_\alpha(X)$ is of the form N/q^m for some $N,\ m$ in $\mathbb{N}$ with $N > 0$. If we define $0 < i(X) < q$ in $\mathbb{N}$ as*

$$\mu_\alpha(X) \equiv i(X) \mod q - 1,$$

i.e., as $\mu_\alpha(X) - i(X)$ in $(q-1)\ \mathbb{Z}[1/q]$, then $i(X)$ depends only on X and X is K-bianalytic to $i(X) \cdot O_K^n$. Furthermore, X is K-bianalytic to another compact n-dimensional K-analytic manifold Y if and only if $i(X) = i(Y)$.

Proof. If X, Y are n-dimensional K-analytic manifolds and $f : X \to Y$ is a K-bianalytic map, and further if Y has a gauge form β, then clearly $\alpha = f^*(\beta)$ is a gauge form on X. Furthermore, if X, Y are compact, then $\mu_\alpha(X) = \mu_\beta(Y)$. We know by Lemma 7.5.1 that X is K-bianalytic to $r \cdot O_K^n$ for some $0 < r < q$. If we

take $Y = r \cdot O_K^n$ and define β on each O_K^n as $dx_1 \wedge \cdots \wedge dx_n$ so that $\mu_\beta = \mu_n$ in our notation, then β is a gauge form on Y, hence $\alpha = f^*(\beta)$ is a gauge form on X, and

$$\mu_\alpha(X) = \mu_\beta(r \cdot O_K^n) = r \cdot \mu_n(O_K^n) = r.$$

If now α, α' are any two gauge forms on X, then we can find an atlas $\{(U, \phi_U)\}$ on X with $\phi_U(x) = (x_1, \dots, x_n)$ such that

$$\alpha(x) = f_U(x)\ dx_1 \wedge \cdots \wedge dx_n, \qquad \alpha'(x) = f'_U(x)\ dx_1 \wedge \cdots \wedge dx_n,$$

in which f_U, f'_U are $K^\times$-valued K-analytic functions on U. Since $q^{\mathbb{Z}}$ is a discrete subset of $\mathbb{R}$, by subdividing U if necessary we may assume that

$$|f_U(x)|_K = q^{e_U}, \qquad |f'_U(x)|_K = q^{e'_U}$$

for all x in U, in which e_U, e'_U are in $\mathbb{Z}$ and independent of x. We may, as before, assume that the U's above are disjoint, hence finite. We then have

$$\mu_\alpha(X) = \sum_U q^{e_U} \cdot \mu_n(\phi_U(U)), \quad \mu_\alpha(X) - \mu_{\alpha'}(X) = \sum_U (q^{e_U} - q^{e'_U})\mu_n(\phi_U(U)),$$

in which $\mu_n(\phi_U(U))$ is a finite sum of elements of $q^{\mathbb{Z}}$. Therefore, $\mu_\alpha(X) = N/q^m$ as stated in the theorem and $\mu_\alpha(X) \equiv \mu_{\alpha'}(X) \bmod q - 1$. We have only to put these together.

7.6 Integration over the fibers

Let X, Y denote K-analytic manifolds which are respectively of dimensions n, m and $f : X \to Y$ a K-analytic map; let a denote an arbitrary point of X and put $b = f(a)$. Then f gives rise to a K-linear map $f^* : \Omega_b(Y) \to \Omega_a(X)$ and its dual map $T_a(X) \to T_b(Y)$. We say that f is *submersive* if $T_a(X) \to T_b(Y)$ is surjective, i.e., $\Omega_b(Y) \to \Omega_a(X)$ is injective, for every a. This clearly implies that $n \geq m$. We shall express the above condition in terms of local coordinates on X, Y. We choose charts (U, ϕ_U), (V, ψ_V) on X, Y, respectively such that $f(U)$ is contained in V, and we put $\phi_U(x) = (x_1, \dots, x_n)$, $\psi_V(y) = (y_1, \dots, y_m)$. We shall examine the condition that $f|U : U \to V$ is submersive. We have

$$f^*(dy_i) = d(y_i \circ f) = \sum_{1 \leq j \leq n} (\partial(y_i \circ f)/\partial x_j)\ dx_j$$

for $1 \leq i \leq m$. We denote by J_x the jacobian matrix with $\partial y_i/\partial x_j = \partial(y_i \circ f)/\partial x_j$ as its (i, j)-entry for $1 \leq i \leq m$, $1 \leq j \leq n$. Then $f|U$ is submersive if and only if the m rows of J_x are linearly independent, i.e., $\operatorname{rank}(J_x) = m$, for every x in U. In that case, after a permutation of $x_1, \dots, x_n$ and by making U smaller if necessary, we may assume that the first m columns of J_x are linearly independent. Then by the implicit function theorem $y_1 \circ f, \dots, y_m \circ f$, $x_{m+1}, \dots, x_n$ form local coordinates on X at every point of U. Therefore, we may replace x_i by $y_i \circ f$ for

$1 \leq i \leq m$ possibly after making U still smaller. This implies that every submersive map is open. Furthermore, it gives a simple description of the *fiber* $X_b = f^{-1}(b)$ of f over an arbitrary point b of Y. In fact, if b is not in $f(X)$, then $X_b = \emptyset$. If $b = f(a)$ for some a in X, we may assume that a is in the above U. If we put $\psi_V(b) = (b_1, \ldots, b_m)$, then $X_b \cap U$ is defined by $x_i - b_i = 0$ for $1 \leq i \leq m$. Therefore, if we put $p = n - m$, then X_b becomes a closed p-dimensional submanifold of X.

Now let α denote a K-analytic differential form of degree n on X and β a gauge form on Y. Then, in the above notation, we can write

$$\alpha(x) = A(x)\ dx_1 \wedge \cdots \wedge dx_n, \qquad \beta(y) = B(y)\ dy_1 \wedge \cdots \wedge dy_m,$$

in which A, B are K-analytic functions respectively on U, V and B is $K^\times$-valued. If we take a K-analytic differential form γ of degree p on U, then it can be written as

$$\gamma(x) = \sum C_{i_1 \ldots i_p}(x)\ dx_{i_1} \wedge \cdots \wedge dx_{i_p},$$

in which $C_{i_1 \ldots i_p}$ for every $1 \leq i_1 < \ldots < i_p \leq n$ is a K-analytic function on U. Furthermore, γ satisfies the condition

$$\alpha = f^*(\beta) \wedge \gamma$$

on U if and only if $A = (B \circ f) C_{m+1,\ldots,n}$ on U, and then

$$\gamma\big|(X_b \cap U) = (A/(B \circ f))\ dx_{m+1} \wedge \cdots \wedge dx_n\big|(X_b \cap U)$$

for $b = f(a)$. We observe that the LHS does not depend on the local expressions of α, β and the RHS is independent of γ. Therefore, the restriction of γ to X_b depends only on α, β, hence it gives rise to a K-analytic differential form θ_b of degree p on the whole X_b with the above local expression. We take a variable point y of Y and define θ_y on X_y as above if $X_y \neq \emptyset$ and $\theta_y = 0$ otherwise. We shall write

$$\theta_y = (\alpha / f^*(\beta))_y = \alpha / f^*(\beta) = \alpha / \beta.$$

We remark that if α is a gauge form on X, then $\theta_y = \alpha/\beta$ is a gauge form on X_y for every y in Y.

Theorem 7.6.1 *Let X, Y denote p-adic manifolds, $f : X \to Y$ a submersive map, and α, β gauge forms on X, Y respectively. Then for every φ in $\mathcal{D}(X)$ the $\mathbb{C}$-valued function F_φ on Y defined by*

$$F_\varphi(y) = \int_{X_y} \varphi(x)\ \mu_{\alpha/\beta}(x)$$

is in $\mathcal{D}(Y)$ and

$$\int_X \varphi(x)\ \mu_\alpha(x) = \int_Y F_\varphi(y)\ \mu_\beta(y).$$

Proof. Since F_φ and both sides of the integration-formula to be proved depend $\mathbb{C}$-linearly on φ, we may assume that $\varphi = \chi_W$ for some W in $\mathcal{T}(X)$. By subdividing W if necessary, we may further assume that W is arbitrarily small. Therefore, we shall assume from the beginning that W is contained in the U for a chart (U, ϕ_U) on X which we have used to define α/β and $\phi_U(W) = a + \pi^e O_K^n$ for some $a = (a_1, \dots, a_n)$ in K^n and e in $\mathbb{N}$. We recall that

$$\alpha(x) = A(x)\ dx_1 \wedge \cdots \wedge dx_n, \qquad \beta(y) = B(y)\ dy_1 \wedge \cdots \wedge dy_m,$$

and $x_i = y_i \circ f$ for $1 \le i \le m$. We put $x' = (x_1, \dots, x_m)$, $x'' = (x_{m+1}, \dots, x_n)$ and similarly $a' = (a_1, \dots, a_m)$, $a'' = (a_{m+1}, \dots, a_n)$. We shall, for the sake of simplicity, use the same notation for x and $\phi_U(x)$ and also for y and x', hence $W = a + \pi^e O_K^n$. We put $W' = a' + \pi^e O_K^m$, $W'' = a'' + \pi^e O_K^p$, where $p = n - m$. Since α, β are gauge forms, we have $A(a) \neq 0$, $B(a') \neq 0$ and we may assume that $|A(x)|_K = |A(a)|_K$, $|B(y)|_K = |B(a')|_K$ for every x, y respectively in W, W'. Then $F_\varphi(y) = 0$ if y is not in W' and

$$F_\varphi(y) = \int_{W''} |A(x)/B(x')|_K\ \mu_p(x'') = |A(a)/B(a')|_K\ \mu_p(W'')$$

if $y = x'$ is in W'. Therefore, $F_\varphi = F_\varphi(a')\ \chi_{W'}$, hence F_φ is in $\mathcal{D}(Y)$. Furthermore, the formula to be proved becomes

$$|A(a)|_K\ \mu_n(W) = |A(a)/B(a')|_K\ \mu_p(W'') \cdot |B(a')|_K\ \mu_m(W''),$$

which is a trivial identity.

Remark. In Theorem 7.6.1 the assumption that α is a gauge form on X is not really necessary. If we drop that assumption, then F_φ need not be in $\mathcal{D}(Y)$, but it is a $\mathbb{C}$-valued continuous function on Y with compact support, and the integration-formula holds. In fact, it holds for every $\mathbb{C}$-valued continuous function φ on X with compact support. This can easily be proved by using the fact already mentioned in section 7.2 that such a function is the uniform limit of a sequence in $\mathcal{D}(X)$ with support of each term contained in a fixed compact subset of X.

We shall explain, for our later use, a special case of $\theta_y = \alpha/\beta$. We take any element $f(x)$ of $K[x_1, \dots, x_n] \backslash K$ and denote by C_f the critical set of the K-analytic map $f : K^n \to K$ defined by $f(x)$. We assume that $C_f \neq K^n$, put $X = K^n \backslash C_f$, $Y = K$, hence $m = 1$, and denote the restriction of f to X also by f. Then the K-analytic map $f : X \to Y$ is clearly submersive. Furthermore, $dx_1 \wedge \cdots \wedge dx_n$ is a gauge form on K^n, hence its restriction α to X is a gauge form on X. If we denote the coordinate on Y by y, then $\beta = dy$ is a gauge form on Y. We shall show that if a is any point of X, hence $(\partial f/\partial x_i)(a) \neq 0$ for some i, and if U_i is the open subset of X defined by $\partial f/\partial x_i \neq 0$, then $\theta_b | (X_b \cap U_i)$ is given by

$$(-1)^{i-1}\ dx_1 \wedge \cdots \wedge dx_{i-1} \wedge dx_{i+1} \wedge \cdots \wedge dx_n\ /\ (\partial f/\partial x_i)\big|(X_b \cap U_i)$$

for $b = f(a)$. In fact, if for every x in U_i we put

$$\gamma(x) = (-1)^{i-1}\ dx_1 \wedge \cdots \wedge dx_{i-1} \wedge dx_{i+1} \wedge \cdots \wedge dx_n\ /\ (\partial f/\partial x_i),$$

then γ is a K-analytic differential form of degree $p = n - 1$ on U_i satisfying $\alpha = f^*(\beta) \wedge \gamma$ on U_i. This implies the above assertion.

https://doi.org/10.1090/amsip/014/08

Chapter 8

Local zeta functions (p-adic case)

8.1 Selfduality of K and some lemmas

Some arithmetic properties of p-adic fields were proved elementarily before the thesis of J. Tate [55] of 1950. He applied the fruitful method of Haar integration uniformly to all completions of an algebraic number field and to its adele groups. In an unpublished paper K. Iwasawa independently applied the same method to the idele group. Both authors had the same objective, i.e., to give a transparent proof to the functional equation of Hecke's zeta function. In the following we shall explain some of Tate's results.

If G is a locally compact abelian group, then the group $G^* = \mathrm{Hom}(G, \mathbb{C}_1^\times)$ is called the dual group or simply the dual of G. If $G \to G'$ is a continuous homomorphism from G to a similar group G', then we have the dual homomorphism $(G')^* \to G^*$. If $g,\ g^*$ are elements of $G,\ G^*$ respectively, then $g^*(g)$ will sometimes be denoted by $\langle g, g^* \rangle$. We shall denote by K a p-adic field as before and prove the *selfduality* of K in the following form:

Proposition 8.1.1 *There exists an element ψ of the dual K^* of K satisfying*

$$\psi|O_K = 1, \qquad \psi|\pi^{-1}O_K \neq 1.$$

Furthermore if for every a in K we define an element ψ_a of K^* as $\psi_a(x) = \psi(ax)$, then $\theta(a) = \psi_a$ gives an isomorphism $\theta : K \to K^*$.

Proof. We shall first prove the existence of ψ. If G is a finite abelian group, then as we have already explained $G,\ G^*$ have the same order. Therefore, if H is a subgroup of G, then the injective homomorphism $G^*/(G/H)^* \to H^*$ defined by $g^* \mapsto g^*|H$ is surjective because they have the same order. In particular, if we put $G_e = \pi^{-e}O_K/O_K$, the homomorphism $G_{e+1}^* \to G_e^*$ dual to the inclusion $G_e \to G_{e+1}$ is surjective for every e in $\mathbb{N}$. Therefore, if $\chi_1 \neq 1$ is given in G_1^*, we can find χ_e in G_e^* satisfying $\chi_{e+1}|G_e = \chi_e$ for every $e > 0$ in $\mathbb{N}$. If now a is arbitrary in K and $\bar{a}$ is its image in K/O_K, then $\bar{a}$ is contained in G_e for all large e. We observe that $\psi(a) = \chi_e(\bar{a})$ is independent of e and defines an element ψ of K^* satisfying $\psi|O_K = 1$ and $\psi|\pi^{-1}O_K \neq 1$.

We shall next show that $\theta : K \to K^*$, defined as $\theta(a)(x) = \psi(ax)$, is an isomorphism. If we let $K^\times$ act on K, K^* as $a_0 \cdot a = a_0 a$, $(a_0 \cdot a^*)(x) = a^*(a_0 x)$, then θ becomes equivariant. If $\theta(a) = 1$ for some a in K, then aK is contained in $\mathrm{Ker}(\psi)$, hence $a = 0$. Therefore, θ is injective. We shall show that θ is surjective, i.e., every a^* in K^* is in $\mathrm{Im}(\theta)$. We know by a general remark in Chapter 7.2 that a^* is locally constant, hence $a^*|\pi^e O_K = 1$, i.e., $\pi^e \cdot a^*|O_K = 1$, for some e in $\mathbb{N}$. Since $\mathrm{Im}(\theta)$ is $K^\times$-invariant, we may assume from the beginning that $a^*|O_K = 1$. Then $a^*|G_e = a_e^*$ is defined for every e in $\mathbb{N}$. On the other hand θ gives rise to an injective homomorphism $O_K/\pi^e O_K \to G_e^*$, which is surjective because they have the same order. Therefore, we get a sequence $\{a_e\}$ in O_K, where each a_e is unique mod π^e, such that $\theta(a_e)|G_e = a_e^*$ for every e in $\mathbb{N}$. Since $a_{e+1}^*|G_e = a_e^*$ by definition, we have $a_{e+1} \equiv a_e \bmod \pi^e$ for every e. Therefore $\{a_e\}$ is a Cauchy sequence in O_K, hence it has a limit a in O_K and $a^*|G_e = \theta(a)|G_e$ for all e, and hence $a^* = \theta(a)$.

We might remark that in the special case where $K = \mathbb{Q}_p$ an element such as ψ in Proposition 8.1.1 can be explicitly defined. We observe that if a is in $\mathbb{Q}_p$, then the coset $a + \mathbb{Z}_p$ can be represented by an element $\langle a \rangle$ of $\mathbb{Z}[1/p]$ unique mod $\mathbb{Z}$ and $e_p(a) = \mathbf{e}(\langle a \rangle)$ defines an element e_p of $\mathbb{Q}_p^*$ satisfying $e_p|\mathbb{Z}_p = 1$ and $e_p(1/p) = \mathbf{e}(1/p)$, hence $e_p|p^{-1}\mathbb{Z}_p \neq 1$.

We observe that $U = O_K^\times$ is a totally disconnected compact abelian group. Therefore, again by a general remark in Chapter 7.2, if χ is any element of $\Omega(U) = U^*$, then we will have $\chi|(1 + \pi^e O_K) = 1$ for some $e > 0$ in $\mathbb{N}$. We shall denote by $e(\chi) = e(\chi^{-1})$ the smallest e as above. In the following lemma, since $dx/|x|_K$ is a Haar measure on $K^\times$, its restriction du to the open subgroup U of $K^\times$ is a Haar measure on U.

Lemma 8.1.1 *If we put*

$$g(\chi) = \int_U \psi(\pi^{-e(\chi)}u)\chi(u)^{-1}\, du,$$

then $g(1) = -q^{-1}$ *and*

$$|g(\chi)|^2 = q^{-e(\chi)}$$

for every $\chi \neq 1$ *in* U^*.

Proof. Suppose first that $\chi = 1$, hence $e(\chi) = 1$. Then by expressing U as $O_K \backslash \pi O_K$ and using the orthogonality of characters, we get $g(1) = -q^{-1}$. Suppose next that $\chi \neq 1$ and, for the sake of simplicity, put $e = e(\chi)$. Then, since $|g(\chi)|^2$ is the product of $g(\chi)$ and its complex conjugate, we get

$$|g(\chi)|^2 = \int_U \Big\{ \int_U \psi(\pi^{-e}(u - v))\chi(u^{-1}v)\, du \Big\}\, dv.$$

If we replace u by uv in the integral by du and change the order of integration, then we get

$$\mathrm{RHS} = \int_U \chi(u)^{-1} \Big\{ \int_U \psi(\pi^{-e}(u - 1)v)\, dv \Big\}\, du.$$

Therefore, similarly to the previous case, we have

$$\begin{aligned} |g(\chi)|^2 &= \int_U \chi(u)^{-1}\Big\{\int_{O_K} \psi(\pi^{-e}(u-1)v)\ dv\Big\}\ du \\ &\quad -q^{-1}\cdot\int_U \chi(u)^{-1}\Big\{\int_{O_K} \psi(\pi^{-e+1}(u-1)v)\ dv\Big\}\ du \\ &= q^{-e}-q^{-1}\cdot\int_{U'}\chi(u)^{-1}\ du, \end{aligned}$$

in which $U' = U \cap (1+\pi^{e-1}O_K)$. We have only to show that the above integral I over U' is 0. If $e=1$, hence $U'=U$, then $I=0$ by the orthogonality of characters of U. If $e>1$, hence $U' = 1+\pi^{e-1}O_K$, then

$$I = q^{-e+1}\cdot\int_{O_K}\chi(1+\pi^{e-1}x)^{-1}dx.$$

Since $2(e-1)\geq e$ by $e>1$, $x\mapsto\chi(1+\pi^{e-1}x)^{-1}$ is a character of O_K different from 1, hence $I=0$ by the orthogonality of characters of O_K.

Lemma 8.1.2 *If $e>0$ is in $\mathbb{N}$, then*

$$\psi(\pi^{-e}u) = (1-q^{-1})^{-1}\cdot\sum_{e(\chi)=e} g(\chi)\chi(u)$$

for every u in $U=O_K^\times$.

Proof. Since $u\mapsto\psi(\pi^{-e}u)$ gives a function on $U/(1+\pi^eO_K)$, by Proposition 7.2.2 and the Plancherel formula we get

$$\psi(\pi^{-e}u) = \sum_{e(\chi)\leq e} c_\chi\chi(u), \qquad 1 = \sum_{e(\chi)\leq e}|c_\chi|^2.$$

If $e(\chi)=e$, then we have

$$g(\chi) = \int_U \psi(\pi^{-e}u)\chi(u)^{-1}\ du = (1-q^{-1})c_\chi.$$

Since $e(\chi)>0$, therefore, the formula holds for $e=1$. Suppose that $e>1$. Then we have

$$\mathrm{card}\{\chi;\ e(\chi)=e\} = \mathrm{card}\{U/(1+\pi^eO_K)\} - \mathrm{card}\{U/(1+\pi^{e-1}O_K)\},$$

which is $(1-q^{-1})^2q^e$, hence by Lemma 8.1.1 we get

$$\sum_{e(\chi)=e}|c_\chi|^2 = (1-q^{-1})^{-2}\cdot\sum_{e(\chi)=e}|g(\chi)|^2 = 1.$$

Therefore, $c_\chi=0$ for $e(\chi)<e$, hence the formula also holds.

Corollary 8.1.1 *If e is arbitrary in $\mathbb{Z}$ and χ is in U^*, then*

$$\int_U \psi(\pi^{-e}u)\chi(u)^{-1}\,du = \begin{cases} g(\chi) & e = e(\chi),\ e > 0 \\ 1 - q^{-1} & \chi = 1, \quad e \le 0 \\ 0 & \text{all other cases.} \end{cases}$$

In the following we shall denote $\mathcal{D}(K^n)$ by $\mathcal{S}(K^n)$. Actually, there is a general definition of $\mathcal{S}(X)$ for an arbitrary locally compact abelian group X by F. Bruhat [6], and it specializes to the Schwartz space for $X = \mathbb{R}^n$ and to $\mathcal{D}(K^n)$ for $X = K^n$. At any rate we shall denote elements of $\mathcal{S}(X)$ for $X = K^n$ by Φ, Ψ etc., and put $[x, y] = x_1y_1 + \ldots + x_ny_n$ for x, y in X as in the archimedean case.

Lemma 8.1.3 *We define the Fourier transform $\mathcal{F}\varphi$, also denoted by φ^*, of any integrable function φ on X as*

$$(\mathcal{F}\varphi)(x) = \int_X \varphi(y)\psi([x, y])\,dy.$$

Then $\mathcal{F}\Phi = \Phi^*$ is in $\mathcal{S}(X)$ for every Φ in $\mathcal{S}(X)$ and further $(\Phi^*)^*(x) = \Phi(-x)$ for every x in X. In particular, the Fourier transformation $\mathcal{F}$ gives a $\mathbb{C}$-linear bijection from $\mathcal{S}(X)$ to itself.

Proof. Since $\mathcal{S}(X)$ is the $\mathbb{C}$-span of χ_A for all A in $\mathcal{T}(X)$, we may assume that $\Phi = \chi_A$. We may further assume that $A = a + \pi^e O_K^n$ for some a in X and e in $\mathbb{Z}$. We then have

$$(\chi_A)^*(x) = q^{-ne} \cdot \psi([a, x])\chi_B(x), \qquad B = \pi^{-e}O_K^n$$

for every x in X. We observe that $x \mapsto \psi([a, x])$ is a locally constant function on X. Since $\mathrm{Supp}((\chi_A)^*) = B$, therefore, $(\chi_A)^*$ is an element of $\mathcal{S}(X)$. Furthermore, we have $((\chi_A)^*)^*(x) = \chi_A(-x)$ for every x in X.

There is a general theorem stating that the Fourier transform of an integrable function is continuous. We shall give a proof to this theorem in the special case we need. If φ is an integrable function on X such that $\Phi_e = \varphi\chi_A$ for $A = \pi^{-e}O_K^n$ is in $\mathcal{S}(X)$ for every e in $\mathbb{N}$, then

$$\lim_{e\to\infty} \|\varphi^* - (\Phi_e)^*\|_\infty \le \lim_{e\to\infty} \int_{X\setminus A} |\varphi(x)|\,dx = 0.$$

Therefore φ^*, as a uniform limit of a sequence of continuous functions on X, is itself continuous on X.

8.2 p-adic zeta function $Z_\Phi(\omega)$

We shall first make $\Omega(K^\times)$ explicit. Every element a of $K^\times$ can be written uniquely, but depending on the choice of π, as $a = \pi^e u$ with e in $\mathbb{Z}$ and u in $O_K^\times$. They

are called respectively the *order* and the *angular component* of a, abbreviated as $\mathrm{ord}(a)$ and $\mathrm{ac}(a)$. Therefore $K^\times$ is bicontinuously isomorphic to $\mathbb{Z}\times O_K^\times$ under $a\mapsto(\mathrm{ord}(a),\mathrm{ac}(a))$, hence $\Omega(K^\times)$ is isomorphic to $\mathbb{C}^\times\times(O_K^\times)^*$ as $\omega\mapsto(\omega(\pi),\omega|O_K^\times)$. In particular, $\Omega(K^\times)$ becomes the disjoint union of countable copies of $\mathbb{C}^\times$ with $(O_K^\times)^*$ as its index set. We observe that $(O_K^\times)^*$ is the union of finite groups $(O_K^\times/(1+\pi^eO_K))^*$ for $e=1,2,\dots$.

We define an element ω_s of $\Omega(K^\times)$ for every s in $\mathbb{C}$ as

$$\omega_s(a)=|a|_K^s=q^{-\mathrm{ord}(a)s}.$$

If, for every ω in $\Omega(K^\times)$, we choose s from $\mathbb{C}$ satisfying $\omega(\pi)=q^{-s}$, then we can write

$$\omega(a)=\omega_s(a)\chi(\mathrm{ac}(a)),$$

in which $\chi=\omega|O_K^\times$. We keep in mind that the above s is not unique. In fact, the correspondence $s\mapsto t=q^{-s}$ gives a bicontinuous isomorphism

$$\mathbb{C}\big/(2\pi i/\log q)\mathbb{Z}\to\mathbb{C}^\times.$$

We observe that a $\mathbb{C}$-valued function of t is holomorphic on $\mathbb{C}^\times$ if and only if it is a holomorphic function on the s-plane $\mathbb{C}$. At any rate, although s is not uniquely determined by ω, its real part $\mathrm{Re}(s)$ depends only on ω. If we denote it by $\sigma(\omega)$, then we will have

$$|\omega(a)|=\omega_{\sigma(\omega)}(a)$$

as in the archimedean case. As in that case, we define an open subset $\Omega_\sigma(K^\times)$ of $\Omega(K^\times)$ by $\sigma(\omega)>\sigma$ for any σ in $\mathbb{R}$.

Lemma 8.2.1 *Take a from K, e from $\mathbb{Z}$, ω from $\Omega_0(K^\times)$, and N, $n>0$ from $\mathbb{N}$, and put $t=\omega(\pi)$, $\chi=\omega|O_K^\times$. Then*

$$\int_{a+\pi^eO_K}\omega(x)^N|x|_K^{n-1}dx=\begin{cases}(1-q^{-1})(q^{-n}t^N)^e/(1-q^{-n}t^N) & a\in\pi^eO_K,\ \chi^N=1\\ q^{-e}\ \omega(a)^N\ |a|_K^{n-1} & a\notin\pi^eO_K,\ \chi^N\big|U'=1\\ 0 & \textit{all other cases.}\end{cases}$$

in which $U'=1+\pi^ea^{-1}O_K$.

Proof. We denote the LHS by I. Suppose first that a is in π^eO_K. Then the integrand is not an element of $\mathcal{S}(K)$. If we denote by χ_k the characteristic function of $\pi^eO_K\backslash\pi^kO_K$ for $k>e$ in $\mathbb{N}$ and put

$$\Phi_k(x)=\omega(x)^N|x|_K^{n-1}\chi_k(x),$$

then Φ_k is in $\mathcal{S}(K)$. Furthermore, if we put $U = O_K^\times$ as before, then

$$\begin{aligned} I = \lim_{k\to\infty} \int_K \Phi_k(x)\ dx &= \lim_{k\to\infty} \sum_{e\le j<k} \int_{\pi^j U} \omega(x)^N |x|_K^{n-1}\ dx \\ &= \lim_{k\to\infty} \sum_{e\le j<k} (q^{-n}t^N)^j \cdot \int_U \chi(u)^N\ du. \end{aligned}$$

If $\chi^N = 1$, since $|q^{-n}t^N| < 1$ in view of $|t| < 1$, we get the first expression for I. On the other hand, if $\chi^N \neq 1$, by the orthogonality of characters of U we get $I = 0$. Suppose next that a is not in $\pi^e O_K$ so that U' above becomes a subgroup of U. Then we simply have

$$I = \omega(a)^N |a|_K^n \cdot \int_{U'} \chi(u)^N du,$$

hence we get the second expression for I if $\chi^N|U' = 1$ and $I = 0$ otherwise.

We shall make one more preparation. Let ω denote any element of $\Omega(K^\times)$ and $u(y)$ a unit of the ring of convergent power series $K\langle\langle y_1, \dots, y_n\rangle\rangle$. Then, firstly, we have

$$u(y) = u(0)\big(1 + \sum_{|i|>0} c_i y^i\big)$$

with $u(0)$ in $K^\times$ and c_i in K for all $i \neq 0$ in $\mathbb{N}^n$ such that the series is convergent on $\pi^k O_K^n$ for some k in $\mathbb{N}$. Secondly, by making k larger if necessary, we may assume that $u(0)^{-1}u(y) - 1$ is contained in $\pi^{e(\chi)}O_K$ for all y in $\pi^k O_K^n$, where $\chi = \omega|O_K^\times$. Then we will have

$$|u(y)|_K = |u(0)|_K, \qquad \omega(u(y)) = \omega(u(0))$$

also for all y in $\pi^k O_K^n$.

Theorem 8.2.1 *Assume that char$(K) = 0$ and let $f(x)$ denote an arbitrary element of $K[x_1, \dots, x_n]\backslash K$; take ω, Φ respectively from $\Omega_0(K^\times)$, $\mathcal{S}(X)$, where $X = K^n$. Then*

$$\omega(f)(\Phi) = \int_{X\backslash f^{-1}(0)} \omega(f(x))\Phi(x)\ dx$$

defines an $\mathcal{S}(X)'$-valued holomorphic function $\omega(f)$ on $\Omega_0(K^\times)$, and it has a mermorphic continuation to the whole $\Omega(K^\times)$ such that $\omega(f)(\Phi)$ is a rational function of $t = \omega(\pi)$ for each $\chi = \omega|O_K^\times$ and Φ. Furthermore, if $h : Y \to X$, $\mathcal{E} = \{E\}$, and (N_E, n_E) for every E in $\mathcal{E}$ are as in Theorem 3.2.1, then

$$\prod_{E\in\mathcal{E}} (1 - q^{-n_E} t^{N_E}) \cdot \omega(f)$$

becomes holomorphic on the punctured t-plane $\mathbb{C}^\times$ for all χ in $(O_K^\times)^*$.

Proof. In the above definition of $\omega(f)(\Phi)$, since every ω in $\Omega_0(K^\times)$ has a continuous extension to K as $\omega(0) = 0$, we could have used X as the domain of integration.

We shall fix χ and Φ, and use Lemma 5.3.1 to prove the first part. Choose any compact subset C of $\Omega_0(K^\times)$, put

$$\sigma_0 = \max_{\omega\in C}(\sigma(\omega)), \quad A = \mathrm{Supp}(\Phi), \quad M = \max(1, \sup_{x\in A}|f(x)|_K),$$

and define ϕ_C as

$$\phi_C = \|\Phi\|_\infty \; M^{\sigma_0} \; \chi_A,$$

in which χ_A is the characteristic function of A. Then

$$|\omega(f(x)) \; \Phi(x)| \le \phi_C(x)$$

for every x in $X\backslash f^{-1}(0)$ and ω in C, and the integral of ϕ_C over $X\backslash f^{-1}(0)$ is finite. Since $\omega \mapsto \omega(f(x))$ for every x in $X\backslash f^{-1}(0)$ is a holomorphic function on $\Omega(K^\times)$, hence on $\Omega_0(K^\times)$, by that lemma $\omega(f)(\Phi)$ is holomorphic on $\Omega_0(K^\times)$, and this implies the first part.

As for the main part, at every point b of Y we can choose a chart (U, ϕ_U) such that U contains b, $\phi_U(y) = (y_1, \dots, y_n)$ and

$$f\circ h = \varepsilon\cdot\prod_{j\in J} y_j^{N_j}, \qquad h^*\Big(\bigwedge_{1\le k\le n} dx_k\Big) = \eta\cdot\prod_{j\in J} y_j^{n_j-1}\cdot\bigwedge_{1\le k\le n} dy_k,$$

in which $(N_j, n_j) = (N_E, n_E)$ with J bijective to the set of all E containing b and ε, η are units of the local ring $\mathcal{O}_b$ of Y at b with $\varepsilon(y)$, $\eta(y)$ having expansions similar to the expansion of $u(y)$ discussed before. Since h is proper and $A = \mathrm{Supp}(\Phi)$ is compact open, we see that $B = h^{-1}(A)$ is in $\mathcal{T}(Y)$. Therefore, we can express B as a necessarily finite disjoint union of members B_α of $\mathcal{T}(Y)$ such that each B_α is contained in some U above. Since Φ is locally constant, after subdividing B_α we may assume that $(\Phi\circ h)|B_\alpha = \Phi(h(b))$ and further that $\phi_U(B_\alpha) = c + \pi^e O_K^n$ for some $c = (c_1, \dots, c_n)$ in K^n and e in $\mathbb{N}$. Since $h : Y\backslash(f\circ h)^{-1}(0) \to X\backslash f^{-1}(0)$ is K-bianalytic, we then have

$$\omega(f)(\Phi) = \sum_\alpha \Phi(h(b)) \; \omega(\varepsilon(b)) \; |\eta(b)|_K \cdot \prod_{1\le i\le n}\int_{c_i+\pi^e O_K} \omega(y_i)^{N_i} \; |y_i|_K^{n_i-1} \; dy_i$$

with the understanding that $N_i = 0$, $n_i = 1$ for all i not in J. Actually, y_i for i in J is restricted by $y_i \ne 0$, but it makes no difference, and by Lemma 8.2.1 the RHS is a rational function of $t = \omega(\pi)$. Furthermore, the denominator of each term is the product of $1 - q^{-n_j}t^{N_j}$ for all j in J multiplied possibly by a power of t, which is holomorphic on $\mathbb{C}^\times$.

The above proof shows, as in the archimedean case, that the orders of the poles of $\omega(f)$ are at most equal to the dimension of the nerve complex $\mathcal{N}(\mathcal{E})$ of $\mathcal{E}$ increased by 1. Furthermore, the real parts of the poles of $\omega(f)$ on each s-plane $\mathbb{C}$ are among the finite set $\{-n_E/N_E;\ E\in\mathcal{E}\}$. As in the archimedean case, we call $\omega(f)$ the *complex power* of $f(x)$ and introduce the *local zeta function* $Z_\Phi(\omega)$ of $f(x)$ as $\omega(f)(\Phi)$. In the special case where Φ is the characteristic function of O_K^n, we shall write $Z(\omega)$

instead of $Z_\Phi(\omega)$ and, changing the notation slightly, we shall write $Z(s)$ instead of $Z(\omega_s)$. If $\sigma(\omega)$, $\mathrm{Re}(s) > 0$, therefore, we have

$$Z(\omega) = \int_{O_K^n} \omega(f(x))\ dx, \qquad Z(s) = \int_{O_K^n} |f(x)|_K^s\ dx.$$

We shall introduce the *Poincaré series* $P(t)$ of a polynomial $f(x)$ in $O_K[x_1, \dots, x_n] \backslash O_K$. We observe that if ξ, ξ' are in O_K^n, i is in $\mathbb{N}$, and $\xi \equiv \xi'$, $f(\xi) \equiv 0 \mod \pi^i$, then we also have $f(\xi') \equiv 0 \mod \pi^i$. Therefore, the number c_i of $\xi \mod \pi^i$ satisfying $f(\xi) \equiv 0 \mod \pi^i$ is well defined. In order to get some information about c_i, we introduce the following power series

$$P(t) = \sum_{i \geq 0} c_i\ (q^{-n}t)^i$$

in a complex variable t. Since $P(t)$ clearly has $\sum t^i$ as its dominant series, it is convergent for $|t| < 1$. On the other hand, we can express $P(t)$ by the $Z(s)$ for the above $f(x)$ as follows. If we denote by $f^{-1}(\pi^i O_K)$ the preimage of $\pi^i O_K$ under $f|O_K^n$, then it becomes the union of $\xi + \pi^i O_K^n$ for all ξ in O_K^n satisfying $f(\xi) \equiv 0 \mod \pi^i$, hence

$$\mu_n(f^{-1}(\pi^i O_K)) = c_i \cdot \mu_n(\pi^i O_K^n) = c_i \cdot q^{-ni},$$

and hence

$$\mu_n(f^{-1}(\pi^i O_K^\times)) = \mu_n(f^{-1}(\pi^i O_K \backslash \pi^{i+1} O_K)) = c_i \cdot q^{-ni} - c_{i+1} \cdot q^{-n(i+1)}$$

for all i in $\mathbb{N}$. Therefore, if $t = \omega_s(\pi) = q^{-s}$ for $\mathrm{Re}(s) > 0$, i.e., $|t| < 1$, then we get

$$\begin{aligned} Z(s) &= \int_{O_K^n \backslash f^{-1}(0)} |f(x)|_K^s\ dx = \sum_{i \geq 0} \int_{f^{-1}(\pi^i O_K^\times)} |f(x)|_K^s\ dx \\ &= \sum_{i \geq 0} (c_i q^{-ni} - c_{i+1} q^{-n(i+1)}) t^i = P(t) - t^{-1}(P(t) - 1). \end{aligned}$$

We have thus obtained the following theorem:

Theorem 8.2.2 *Let $f(x)$ denote an arbitrary element of $O_K[x_1, \dots x_n] \backslash O_K$ and define its Poincaré series $P(t)$ as*

$$P(t) = \sum_{i \geq 0} \mathrm{card}\{\xi \in O_K^n, \mod \pi^i;\ f(\xi) \equiv 0 \mod \pi^i\} \cdot (q^{-n}t)^i.$$

Then

$$P(t) = (1 - tZ(s))/(1 - t)$$

with s and t related as $t = q^{-s}$ for $Re(s) > 0$. In particular, $P(t)$ is a rational function of t.

We might mention that the Poincaré series of $f(x)$ was introduced and its rationality was conjectured in the joint book by S. I. Borewicz and I. R. Šafarevič [5], which is based on a course given by the second author at the Moscow University.

8.3 Weil's functions $F_\Phi(i)$ and $F^*_\Phi(i^*)$

We shall discuss Weil's functions F_Φ, F^*_Φ in the one-variable case; we shall only consider the p-adic case. We shall start with a review of these functions in the general form as A. Weil introduced them in [58]. This is just to give a good perspective and, therefore, no details will be given. If X, G are locally compact abelian groups, dx is a Haar measure on X, G^* is the locally compact dual group of G, and $f : X \to G$ is a continuous map, then F^*_Φ is the bounded uniformly continuous function on G^* defined by

$$F^*_\Phi(g^*) = \int_X \Phi(x)\ \langle f(x), g^*\rangle\ dx$$

for every Φ in the Schwartz-Bruhat space $\mathcal{S}(X)$ of X. In order to proceed further, Weil introduced the following condition:

Condition (A) *$|F^*_\Phi(g^*)|$ is integrable on G^* with respect to its Haar measure dg^* and the integral is convergent uniformly in Φ if it is restricted to a compact subset of $\mathcal{S}(X)$.*

He then showed the existence of a unique family of measures $\{\mu_g;\ g \in G\}$, each μ_g supported by the fiber $f^{-1}(g)$, such that the integral of $\Phi(x)$ over X by dx can be expressed as an integral over $f^{-1}(g)$ by μ_g followed by an integration over the base space G by the dual measure dg of dg^*. In particular,

$$\int_X \Phi(x)\langle f(x), g^*\rangle\ dx = \int_G \Big(\int_{f^{-1}(g)} \Phi(x)\ \mu_g(x)\Big)\langle g, g^*\rangle\ dg.$$

The function $F_\Phi(g)$ on G is then defined as the above integral of $\Phi(x)$ over the fiber $f^{-1}(g)$ by $\mu_g(x)$, and it is continuous.

We shall now make the following specialization: $X = K^n$ for a p-adic field K, $G = K$, and $f : X \to K$ is the K-analytic map defined by an arbitrary $f(x)$ in $K[x_1, \ldots, x_n]\backslash K$, and we shall examine F_Φ, F^*_Φ with all details. As we have shown in Proposition 8.1.1, the bicharacter $\psi(ab)$ of $K \times K$ puts K into a duality with itself. Therefore F^*_Φ becomes the function on K defined by

$$F^*_\Phi(i^*) = \int_X \Phi(x)\psi(i^* f(x))\ dx$$

for every Φ in $\mathcal{S}(X)$ and i^* in K, in which $dx = \mu_n$. We observe that F^*_Φ is bounded. In fact,

$$\|F^*_\Phi\|_\infty \le \int_X |\Phi(x)|\ dx \le \|\Phi\|_\infty \cdot \mu_n(C),$$

in which $C = \mathrm{Supp}(\Phi)$ is in $\mathcal{T}(X)$. Since $f(C)$ is a compact subset of K, it is contained in $\pi^{-e}O_K$ for some e in $\mathbb{N}$. We shall show that $F^*_\Phi|(i^*_0 + \pi^e O_K)$ is a constant function on $i^*_0 + \pi^e O_K$ for every i^*_0 in K. In other words, F^*_Φ is uniformly locally constant, hence uniformly continuous. The proof is simple. If i^* is in $i^*_0 + \pi^e O_K$, then

$$F^*_\Phi(i^*) - F^*_\Phi(i^*_0) = \int_X \Phi(x)\ \psi(i^*_0 f(x))\ \big\{\psi((i^* - i^*_0)f(x)) - 1\big\}\ dx,$$

in which $\psi((i^* - i_0^*)f(x)) = 1$ for every x in $\mathrm{Supp}(\Phi)$, hence the integral is 0, i.e., $F_\Phi^*(i^*) = F_\Phi^*(i_0^*)$.

In the special case where Φ is the characteristic function of O_K^n, we shall write F^* instead of F_Φ^*. If further the coefficients of $f(x)$ are in O_K, then we will have $F^*|O_K = 1$. We shall examine $F^*(i^*)$ for i^* in $K\backslash O_K$. If we write $i^* = \pi^{-e}u$ with $e = -\mathrm{ord}(i^*) > 0$ and u in $O_K^\times$, then

$$\begin{aligned} F^*(i^*) &= \sum_{\xi \in O_K^n, \mod \pi^e} \int_{\xi + \pi^e O_K^n} \psi(i^* f(x))\, dx \\ &= q^{-ne} \cdot \sum_{\xi \in O_K^n, \mod \pi^e} \psi(i^* f(\xi)). \end{aligned}$$

In the special case where $K = \mathbb{Q}_p$, $\psi = e_p$, and i^* is in $\mathbb{Z}[1/p]\backslash\mathbb{Z}$, we have

$$F^*(p^{-e}u) = p^{-ne} \cdot \sum_{\xi \in \mathbb{Z}^n, \mod p^e} \mathbf{e}(p^{-e}u f(\xi)),$$

in which u is in $\mathbb{Z}\backslash p\mathbb{Z}$. Such an expression is called an *exponential sum* or a *generalized Gaussian sum*.

We have seen that F_Φ^* is a nice function on K. However, it is not always integrable over K. Before we give such an example, we observe the following consequence of the orthogonality of characters of O_K. If i^* is in $K\backslash O_K$, then

$$\int_{O_K^2} \psi(i^* x_1 x_2)\, dx = \int_{O_K} \Big\{ \int_{O_K} \psi(i^* x_1 x_2)\, dx_1 \Big\}\, dx_2 = \mu_1((i^*)^{-1} O_K) = |i^*|_K^{-1}.$$

Therefore, if $n = 2m$ and $f(x) = x_1 x_{m+1} + \ldots + x_m x_{2m}$, then

$$F^*(i^*) = \max(1, |i^*|_K)^{-m}$$

for every i^* in K. This implies

$$\int_K |F^*(i^*)|\, di^* = 1 + \sum_{e>0} \int_{\pi^{-e} O_K^\times} |i^*|_K^{-m}\, di^* = 1 + (1 - q^{-1}) \sum_{e>0} q^{-(m-1)e},$$

and the above series is divergent if $m = 1$.

We have just seen that Condition (A) is not always satisfied even in the special case where $X = K^n$ and $f : X \to K$ is given by $f(x)$ in $K[x_1, \ldots, x_n]\backslash K$. We shall, therefore, use the classical observation in Weil [58], pp. 12-13 to define F_Φ. In fact, we know, by Theorem 7.6.1 that there is a function F_φ which has a similar property as F_Φ. We shall make this situation precise.

Let C_f and $V_f = f(C_f)$ denote the critical set and the set of critical values of f; for the sake of simplicity we put $S = V_f$. We have shown in Theorem 2.5.1 that if $\mathrm{char}(K) = 0$, then S is finite. Furthermore, even if $\mathrm{char}(K) \neq 0$, if $f(x)$ is homogeneous and $\mathrm{char}(K)$ does not divide $\deg(f)$, then $S = \{0\}$ unless $\deg(f) = 1$; in that case $S = \emptyset$. At any rate, if Φ is in $\mathcal{S}(X)$, then for every i in $K\backslash S$ we define

μ_i on $f^{-1}(i)$ as $\mu_{\alpha/\beta}$ in Chapter 7.4, where α is the restriction of $dx_1 \wedge \cdots \wedge dx_n$ to $X \backslash C_f$ and $\beta = dy$ or rather di in this case, and put

$$F_\Phi(i) = \int_{f^{-1}(i)} \Phi(x)\ \mu_i(x).$$

Then F_Φ becomes a locally constant function on $K \backslash S$ if S is closed in K, hence if S is finite. In fact, if U is a compact neighborhood in $K \backslash S$ of any i_0 in $K \backslash S$, then $F_\Phi | U$ remains the same even if Φ is replaced by $\Phi \chi_A$ for $A = f^{-1}(U)$. Therefore, we may assume that $\mathrm{Supp}(\Phi)$ is contained in $f^{-1}(U)$. Then by Theorem 7.6.1 applied to $f^{-1}(U)$, U, and $f | f^{-1}(U)$ instead of X, Y, and f we see that F_Φ is locally constant on U, hence on $K \backslash S$.

Lemma 8.3.1 *If A is in $\mathcal{T}(X)$, then*

$$\lim_{e \to \infty} \mu_n(f^{-1}(\pi^e O_K) \cap A) = 0.$$

Proof. This lemma can be proved elementarily by using the Weierstrass preparation theorem. In the case where $\mathrm{char}(K) = 0$, the case in which we shall be interested, it can also be proved as follows. If we put

$$c_e = \mu_n(f^{-1}(\pi^e O_K^\times) \cap A), \qquad t = q^{-s},$$

then for $\Phi = \chi_A$ and $\mathrm{Re}(s) > 0$ we have

$$Z_\Phi(\omega_s) = \int_{A \backslash f^{-1}(0)} |f(x)|_K^s\ dx = \sum_{e \in \mathbb{Z}} c_e t^e$$

with $c_e \neq 0$ only for a finitely many $e < 0$. By Theorem 8.2.1 we know that $Z_\Phi(\omega_s)$ is a rational function of t with poles possibly at 0 and outside the unit disc. Therefore by Cauchy-Hadamard's formula for the radius of convergence of a power series we get

$$\limsup_{e \to \infty} |c_e|^{1/e} < 1,$$

hence $0 \leq c_e \leq r^e$ for some $0 < r < 1$ and for all large e. We have only to observe, finally, that

$$\mu_n(f^{-1}(\pi^e O_K) \cap A) = \sum_{i \geq e} c_i \leq \sum_{i \geq e} r^i = r^e/(1-r)$$

for all large e with $r^e/(1-r) \to 0$ as $e \to \infty$.

Lemma 8.3.2 *Suppose that S is finite. Then we have*

$$\int_X \Phi(x)\ dx = \int_{K \backslash S} F_\Phi(i)\ di$$

for every Φ in $\mathcal{S}(X)$.

Proof. If we put $A = \mathrm{Supp}(\Phi)$ and

$$D_e = \bigcup_{i_0 \in S} (f^{-1}(i_0 + \pi^e O_K) \cap A), \qquad E_e = \bigcup_{i_0 \in S} (i_0 + \pi^e O_K),$$

then these unions become disjoint for all large e. Furthermore, since A is in $\mathcal{T}(X)$, by applying Lemma 8.3.1 to $f - i_0$ instead of f for every i_0 in S, we see that $\mu_n(D_e) \to 0$ as $e \to \infty$. Therefore, we get

$$\int_X \Phi(x)\ dx = \lim_{e\to\infty} \int_{X\setminus D_e} \Phi(x)\ dx = \lim_{e\to\infty} \int_{K\setminus E_e} F_\Phi(i)\ di = \int_{K\setminus S} F_\Phi(i)\ di.$$

We have used Theorem 7.6.1 to see that the two integrals under the limit signs are equal and the fact that the second limit exists because the first limit exists.

Theorem 8.3.1 *Suppose that $S = f(C_f)$ is finite and Φ is arbitrary in $\mathcal{S}(X)$. Then we have*

$$\begin{aligned} F^*_\Phi(i^*) &= \int_{K\setminus S} F_\Phi(i)\ \psi(ii^*)\ di, \\ F_\Phi(i) &= \lim_{e\to\infty} \int_{\pi^{-e}O_K} F^*_\Phi(i^*)\ \psi(-ii^*)\ di^* \end{aligned}$$

respectively for all i^* in K and all i in $K\setminus S$. Furthermore, the integral over $\pi^{-e}O_K$ becomes independent of e for all large e.

Proof. Since $\Phi_1(x) = \Phi(x)\psi(i^* f(x))$ is in $\mathcal{S}(X)$, by applying Lemma 8.3.2 to Φ_1 instead of Φ we get the first formula. In the proof of the second formula we replace i by i_1. Since i_1 is not in S and F_Φ is locally constant on $K\setminus S$, if we take e sufficiently large, then $i_1 + \pi^e O_K$ becomes disjoint from S and F_Φ becomes a constant function on $i_1 + \pi^e O_K$. Then by using the first formula, Fubini's theorem, and the orthogonality of characters of $\pi^{-e}O_K$ we get

$$\begin{aligned} \int_{\pi^{-e}O_K} F^*_\Phi(i^*)\psi(-i_1 i^*)\ di^* &= \int_{K\setminus S} F_\Phi(i)\Big\{ \int_{\pi^{-e}O_K} \psi((i-i_1)i^*)\ di^* \Big\}\ di \\ &= q^e \cdot \int_{i_1+\pi^e O_K} F_\Phi(i)\ di = F_\Phi(i_1). \end{aligned}$$

We observe that $F_\Phi(i) = 0$ if i is not contained in $f(\mathrm{Supp}(\Phi))$. In the special case where Φ is the characteristic function of O_K^n, we shall write F instead of F_Φ. If further the coefficients of $f(x)$ are in O_K, then we will have $F|(K\setminus O_K) = 0$. We shall examine $F(i)$ for i in $O_K\setminus S$. Since F is locally constant on $O_K\setminus S$, we have

$$F(i) = \lim_{e\to\infty} q^e \cdot \int_{i+\pi^e O_K} F(i')\ di' = \lim_{e\to\infty} q^e \cdot \mu_n(f^{-1}(i+\pi^e O_K) \cap O_K^n)$$

$$= \lim_{e\to\infty} \mathrm{card}\{\xi \in O_K^n, \mod \pi^e;\ f(\xi) \equiv i \mod \pi^e\}/q^{(n-1)e}$$

with the expression under the limit sign independent of e for all large e. Such an $F(i)$ is called a *local singular series*.

We shall determine F in the case where $f(x) = x_1x_{m+1} + \ldots + x_mx_{2m}$. We have seen that $F^*(i^*) = \max(1, |i^*|_K)^{-m}$ for every i^* in K. Since $C_f = \{0\}$, hence $S = \{0\}$, we take i from $O_K\backslash\{0\}$. Then by using Theorem 8.3.1 we can easily see that

$$F(i) = (1 - q^{-m}) \sum_{0 \le k \le \mathrm{ord}(i)} q^{-(m-1)k}.$$

In particular, if $m = 1$, then $F(i) \to \infty$ as $i \to 0$. Therefore, the locally constant function F on $K^\times$ does not have a continuous extension to K.

8.4 Relation of $F_\Phi(i)$ and $Z_\Phi(\omega)$

We shall assume that $V_f = f(C_f)$ is contained in $\{0\}$ and establish the relation of $F_\Phi(i)$ and $Z_\Phi(\omega)$. As we have remarked, the above condition is satisfied if $f(x)$ is homogeneous and $\mathrm{char}(K)$ does not divide $\deg(f)$. At any rate, if ω is in $\Omega_0(K^\times)$, then by Lemma 8.3.2 or rather by its proof we get

$$\begin{aligned} Z_\Phi(\omega) &= \lim_{e\to\infty} \int_{X\backslash f^{-1}(\pi^e O_K)} \Phi(x)\omega(f(x))\, dx \\ &= \lim_{e\to\infty} \int_{K\backslash \pi^e O_K} F_\Phi(i)\omega(i)\, di = \int_{K^\times} F_\Phi(i)\omega(i)\, di. \end{aligned}$$

We keep in mind that F_Φ is a locally constant function on $K^\times$. In order to proceed further, we need the following well-known lemma.

Lemma 8.4.1 *Let m denote a positive integer not divisible by $\mathrm{char}(K)$. Then for any $e > \mathrm{ord}(m)$ in $\mathbb{N}$ the m-th power map gives a surjection from $1 + \pi^e O_K$ to $1 + m\pi^e O_K$.*

Proof. we shall use the formula

$$(1 + \pi^e x)^m = 1 + m\pi^e \Big\{ x + \sum_{1<k\le m} \binom{m}{k} m^{-1} \pi^{(k-1)e} x^k \Big\}.$$

If $e \ge \mathrm{ord}(m)$ and a is in O_K, then it shows that $(1 + \pi^e a)^m$ is contained in $1 + m\pi^e O_K$. If further $e > \mathrm{ord}(m)$ and b is in O_K, then it shows that

$$P(x) = (m\pi^e)^{-1}\big\{(1 + \pi^e x)^m - (1 + m\pi^e b)\big\} + b$$

is an SRP in x. Therefore Corollary 2.2.1 shows that O_K is mapped bijectively to itself under $x \mapsto P(x)$. Hence $P(x) = b$, i.e., $(1 + \pi^e x)^m = 1 + m\pi^e b$ has a solution a in O_K.

Theorem 8.4.1 *Assume that char$(K) = 0$ and C_f is contained in $f^{-1}(0)$. Then there exists $e(\Phi) > 0$ in $\mathbb{N}$ depending on Φ such that $Z_\Phi(\omega) = 0$ unless $e(\chi) \leq e(\Phi)$ for $\chi = \omega|O_K^\times$. Furthermore, if ω is in $\Omega_0(K^\times)$, then*

$$Z_\Phi(\omega) = \int_{K^\times} F_\Phi(i)\ \omega(i)\ di$$

and if we put $t = \omega(\pi)$, then

$$F_\Phi(i) = ((1-q^{-1})|i|_K)^{-1} \cdot \sum_{e(\chi)\leq e(\Phi)} \mathrm{Res}_{t=0}(Z_\Phi(\omega)\ t^{-\mathrm{ord}(i)-1})\ \chi(\mathrm{ac}(i))^{-1}$$

for every i in $K^\times$, in which $\mathrm{Res}_{t=0}$ *means the taking of the residue at $t = 0$.*

Proof. We shall use the same notation as in the proof of Theorem 8.2.1 with the following modification. First of all, by multiplying a power of π to ϕ_U in (U, ϕ_U), we shall assume that $\varepsilon(b)^{-1}\varepsilon(y)$ is in $O_K[[y_1, \dots, y_n]]$ for all U. In the case where $i = f(h(b)) \neq 0$, hence $J = \emptyset$ and $f(h(y)) = \varepsilon(y)$, we shall assume that $y_1 = \varepsilon(b)^{-1}\varepsilon(y) - 1$ in $\phi_U(y) = (y_1, \dots, y_n)$. This is permissible because $f^{-1}(i)$ is disjoint from $f^{-1}(0)$, hence from C_f by assumption, and $h : Y \to X$ is K-bianalytic over $X \backslash C_f$. We put

$$m_0 = \max\{\mathrm{ord}(N_E);\ E\ \in\ \mathcal{E}\}$$

and, by making U smaller, we shall assume that $\phi_U(U)$ is contained in $\pi^{m_0+1}O_K^n$ for all U. This time, since χ is not fixed, we can only assume that $|\eta(y)|_K$ is constant on U. We recall that

$$Z_\Phi(\omega) = \sum_\alpha \Phi(h(b))\ |\eta(b)|_K \cdot \int_{c+\pi^e O_K^n} \omega(\varepsilon(y)) \prod_{j\in J} \omega(y_j)^{N_j}\ |y_j|_K^{n_j-1} \cdot dy$$

for some $e > m_0$, in which c is contained in $\pi^{m_0+1}O_k^n$. We shall show that

$$e(\Phi) = m_0 + e$$

will then have the required property, i.e., we shall derive a contradiction assuming that $Z_\Phi(\omega) \neq 0$ for $e(\chi) > e(\Phi)$. At any rate $Z_\Phi(\omega) \neq 0$ implies

$$I = \int_{c+\pi^e O_K^n} \omega(\varepsilon(y)) \prod_{j\in J} \omega(y_j)^{N_j}\ |y_j|_K^{n_j-1} \cdot dy \neq 0$$

for some c.

Suppose first that $J = \emptyset$. Then $\varepsilon(y) = \varepsilon(b)(1 + y_1)$, hence

$$I = q^{-(n-1)e}\omega(\varepsilon(b)) \cdot \int_{c_1+\pi^e O_K} \chi(1 + y_1)\ dy_1 \neq 0.$$

Since $1 + c_1$ is in $1 + \pi^{m_0+1}O_K$, hence in $O_K^\times$, this implies

$$\int_{1+\pi^e O_K} \chi(y_1)\ dy_1 \neq 0,$$

hence $\chi\big|(1+\pi^e O_K)=1$, i.e., $e(\chi)\le e$ contradicting $e(\chi)>e(\Phi)\ge e$.

Suppose next that $J\neq\emptyset$. Then we express $c+\pi^e O_K^n$ as a disjoint union of $c'+\pi^{e(\chi)}O_K^n$ observing that $e(\chi)>e(\Phi)\ge e$. Since $\varepsilon(b)^{-1}\varepsilon(y)$ is in $O_K[[y_1,\dots,y_n]]$, we then have

$$\omega(\varepsilon(y))\big|(c'+\pi^{e(\chi)}O_K^n)=\omega(\varepsilon(b))\chi(\varepsilon(b)^{-1}\varepsilon(c'))$$

for every c'. Since $I\neq 0$, therefore, we get

$$\int_{c'_j+\pi^{e(\chi)}O_K}\omega(y_j)^{N_j}|y_j|_K^{n_j-1}dy_j\neq 0$$

for some c' and j. If c'_j is in $\pi^{e(\chi)}O_K$, then $\chi^{N_j}=1$ by Lemma 8.2.1, hence $\chi^{N_j}=1$ on $1+\pi^{m_0+1}O_K$. Since $\mathrm{ord}(N_j)\le m_0$, we see by Lemma 8.4.1 that $\chi=1$ on $1+\pi^{2m_0+1}O_K$. This implies $e(\chi)\le 2m_0+1$ contradicting $e(\chi)>e(\Phi)\ge 2m_0+1$. If c'_j is not contained in $\pi^{e(\chi)}O_K$, then $m_0+1\le\mathrm{ord}(c'_j)<e(\chi)$ and $\chi^{N_j}=1$ on $1+\pi^{e(\chi)}(c'_j)^{-1}O_K$ by Lemma 8.2.1, hence $\chi^{N_j}=1$ on $1+\pi^{e(\chi)-m_0-1}O_K$. Since $e(\chi)-m_0-1>m_0\ge\mathrm{ord}(N_j)$, we see by Lemma 8.4.1 that $\chi=1$ on $1+\pi^{e(\chi)-1}O_K$ contradicting the definition of $e(\chi)$. We have thus proved the first part.

As for the second part, since the expression of $Z_\Phi(\omega)$ in terms of $F_\Phi(i)$ has already been proved, we shall prove the converse. Since F_Φ is a locally constant function on $K^\times$, for every e in $\mathbb{Z}$, not the above e, the function $u\mapsto F_\Phi(\pi^e u)$ is in $\mathcal{D}(O_K^\times)$. Therefore, by Proposition 7.2.2 we can write

$$F_\Phi(\pi^e u)=\sum_{\chi\in(O_K^\times)^*}c_{e,\chi}\ \chi(u)$$

with $c_{e,\chi}$ in $\mathbb{C}$. Then for every ω in $\Omega_0(K^\times)$ we will have

$$Z_\Phi(\omega)=\sum_{e\in\mathbb{Z}}\int_{\pi^e O_K^\times}F_\Phi(i)\ \omega(i)\ di=(1-q^{-1})\sum_{e\in\mathbb{Z}}c_{e,\chi^{-1}}\ (q^{-1}t)^e.$$

Therefore by the first part, $c_{e,\chi}=0$ for $e(\chi)>e(\Phi)$ and

$$(1-q^{-1})^{-1}q^e\cdot\sum_{e(\chi)\le e(\Phi)}\mathrm{Res}_{t=0}(Z_\Phi(\omega)t^{-e-1})\ \chi(u)^{-1}=\sum_{e(\chi)\le e(\Phi)}c_{e,\chi^{-1}}\ \chi(u)^{-1},$$

which is $F_\Phi(\pi^e u)$. This completes the proof.

We remark that in the finite sum expression of $F_\Phi(i)$ in Theorem 8.4.1 the number of terms depends on Φ but not on i. The meaning of the theorem is that it permits us to translate properties of $Z_\Phi(\omega)$ into the corresponding properties of Weil's functions $F_\Phi(i)$ and $F^*_\Phi(i^*)$. We might mention that our first paper on local zeta functions was written to develop such a theory uniformly not only for a p-adic field K but also for $\mathbb{R}$ and $\mathbb{C}$. At any rate, in the p-adic case the rationality of $Z_\Phi(\omega)$ as stated in Theorem 8.2.1 and supplemented by Theorem 8.4.1 is equivalent to a certain behavior of $F_\Phi(i)$ at its "singular point 0" and also to that of $F^*_\Phi(i^*)$ at its "singular point ∞", which can be expressed by certain asymptotic expansions respectively as $|i|_K\to 0$ and $|i^*|_K\to\infty$. We refer the reader to [23] for the details.

In the following, we shall only use the property of $Z_\Phi(\omega)$ being meromorphic on $\Omega(K^\times)$ and examine Condition (A) for a fixed Φ. In doing so, we shall use the following lemma:

Lemma 8.4.2 *Let $\phi(t)$ denote a meromorphic function on $|t| \leq r$, i.e., on an open set containing the closed disc, for some $r > 0$. Then a finite limit*

$$a = \lim_{e \to \infty} r^e \cdot \mathrm{Res}_{t=0}(\phi(t) t^{-e-1})$$

exists if and only if $\phi(t) - b/(1 - r^{-1}t)$ is holomorphic on $0 < |t| \leq r$ for some b in $\mathbb{C}$, and in that case $a = b$.

Proof. We consider the vector space over $\mathbb{C}$ of all meromorphic functions $\phi(t)$ on $|t| \leq r$ and denote the Laurent expansion of each $\phi(t)$ at 0 by

$$\phi(t) = \sum_{e \in \mathbb{Z}} c_e t^e, \qquad c_e = \mathrm{Res}_{t=0}(\phi(t) t^{-e-1}).$$

We introduce its subspaces E_n and E_c respectively with poles at most at 0 and with $r^e c_e$ having a finite limit as $e \to \infty$, and put

$$E = \mathbb{C} \cdot 1/(1 - r^{-1}t) + E_n.$$

Then the first part of the lemma can be restated as $E_c = E$. If $\phi(t)$ is in E_n, then it is convergent at r, hence $\{r^e c_e\}$ is a null sequence. Therefore, if $\phi(t) - b/(1 - r^{-1}t)$ is in E_n, then $r^e c_e$ tends to b as $e \to \infty$. Hence $E_c = E$ also implies the second part of the lemma. Since we have shown that E is contained in E_c, we have only to show that E_c is contained in E.

We observe that E_n, E_c, E are all stable under the multiplication by t, hence that they are $\mathbb{C}[t]$-modules. If $\phi(t)$ is in E_c, then the sequence $\{r^e c_e\}$ is bounded, hence $\phi(t)$ is holomorphic on $0 < |t| < r$, and hence

$$\phi(t) \equiv \sum_{|\alpha| = r} \sum_{1 \leq m \leq m_\alpha} c_{\alpha,m}/(1 - \alpha^{-1}t)^m \mod E_n$$

for some $c_{\alpha,m}$ in $\mathbb{C}$ with $c_{\alpha,m_\alpha} \neq 0$. We shall show that $m_\alpha \leq 1$ for all α. Suppose that $m_\alpha > 1$ for some α. Then E_c contains

$$(1 - \alpha^{-1}t)^{m_\alpha - 2} \cdot \prod_{\beta \neq \alpha} (1 - \beta^{-1}t)^{m_\beta} \cdot \phi(t) \equiv \sum_{e \in \mathbb{Z}} c_e{}' t^e \mod E_n,$$

in which

$$c_e{}' = (c_{\alpha,m_\alpha}(e+1) + c_{\alpha,m_\alpha - 1})\alpha^{-e}$$

for all e in $\mathbb{N}$. This contradicts the definition of E_c because the sequence $\{r^e c_e{}'\}$ is unbounded. We shall next show that $m_\alpha = 0$ for $\alpha \neq r$. Suppose that $m_\alpha = 1$ for some $\alpha \neq r$. Then E_c contains

$$\prod_{\beta \neq \alpha} (1 - \beta^{-1}t) \cdot \phi(t) \equiv \sum_{e \in \mathbb{Z}} c_e{}'' t^e \mod E_n,$$

in which $c_e{}'' = c_{\alpha,1}\alpha^{-e}$ for all e in $\mathbb{N}$. This again contradicts the definition of E_c because $r^e c_e{}''$ has no limit as $e \to \infty$. Therefore $\phi(t)$ is in E.

Theorem 8.4.2 *Assume that char(K) = 0 and C_f is contained in $f^{-1}(0)$. Then the following conditions on F_Φ, F_Φ^*, and Z_Φ are equivalent:*

(1) $F_\Phi(i)$ has a finite limit $F_\Phi(0)$ as $|i|_K \to 0$;

(2) F_Φ^* is an integrable function on K;

(3) $Z_\Phi(\omega)$ for $\chi \neq 1$ and $(1-q^{-1}t)Z_\Phi(\omega_s)$ are holomorphic on $0 < |t| \leq q$.

Furthermore, in that case

$$\mathrm{Res}_{t=q}(Z_\Phi(\omega_s)) = (1-q)F_\Phi(0)$$

and if q^σ is the smallest absolute value of the poles of $Z_\Phi(\omega)$ on $|t| > q$ and $\varepsilon > 0$, then

$$|F_\Phi^*(i^*)| \leq \gamma(\Phi) \cdot \max(1, |i^*|_K)^{-\sigma+\varepsilon}$$

for all i^* in K, in which $\gamma(\Phi) > 0$ is independent of i^*.

Proof. We have seen in section 8.1 that the Fourier transform of an integrable function is continuous. Therefore (2) implies (1) by Theorem 8.3.1. In the notation of the proof of the second part of Theorem 8.4.1 we see that (1) implies

$$\lim_{e\to\infty} c_{e,\chi} = (1-q^{-1})^{-1} \cdot \lim_{e\to\infty} \int_{O_K^\times} F_\Phi(\pi^e u)\ \chi(u)^{-1}\ du = \delta_1(\chi)\ F_\Phi(0),$$

in which $\delta_1(\chi) = 1$ or 0 according as $\chi = 1$ or $\chi \neq 1$. Therefore, by applying Lemma 8.4.2 to $\phi(t) = Z_\Phi(\omega)$ for $r = q$ we see that

$$Z_\Phi(\omega) - \delta_1(\chi)F_\Phi(0)(1-q^{-1})/(1-q^{-1}t)$$

is holomorphic on $0 < |t| \leq q$. Hence (1) implies (3) and also the residue formula for $Z_\Phi(\omega_s)$ at $t = q$. Finally, since the integral of $|i^*|_K^{-\sigma_0}$ over $K\backslash O_K$ is convergent for every $\sigma_0 > 1$, we have only to show that (3) implies the estimate for $|F_\Phi^*(i^*)|$ as stated in the theorem. By assumption the RHS power series in

$$\begin{aligned} Z_\Phi(\omega) &- \delta_1(\chi)b(1-q^{-1})/(1-q^{-1}t) \\ &\equiv (1-q^{-1})\sum_{e\geq 0}(c_{e,\chi^{-1}} - \delta_1(\chi)b)(q^{-1}t)^e \mod \mathbb{C}[t^{-1}] \end{aligned}$$

is holomorphic on $|t| < q^\sigma$ for some b in $\mathbb{C}$. Therefore, if we replace t in its *e-th* term by any r satisfying $0 < r < q^\sigma$, then we get a bounded sequence, i.e., we have

$$c_{e,\chi^{-1}} = \delta_1(\chi)b + O((qr^{-1})^e)$$

as $e \to \infty$. On the other hand, by using Theorem 8.3.1 and Corollary 8.1.1 we get

$$F_\Phi^*(\pi^{-e}u) = (1-q^{-1})\sum_{k\geq e} c_{k,1}\ q^{-k} + q^{-e} \cdot \sum_\chi c_{e-e(\chi),\chi^{-1}}\ q^{e(\chi)}\ g(\chi)\ \chi(u)$$

for every e in $\mathbb{Z}$ and u in $O_K^\times$, in which the summation in χ is finite. Since $e(1) = 1$ and $g(1) = -q^{-1}$, the contribution from the above series and the term for $\chi = 1$ is $O(r^{-e})$ while the contribution from each term for $\chi \neq 1$ is also $O(r^{-e})$ both as $e \to \infty$. If $\varepsilon > 0$, then we can take $r = q^{\sigma-\varepsilon}$. Therefore, we get

$$F_\Phi^*(i^*) = O(r^{\mathrm{ord}(i^*)}) = O(|i^*|_K^{-\sigma+\varepsilon})$$

as $|i^*|_K \to \infty$.

8.5 Poles of $\omega(f)$ for a group invariant f

We shall go back to the complex power $\omega(f)$ in Theorem 8.2.1 and obtain different kinds of information on the poles of $\omega(f)$ in the special case where $f(x)$ is a relative invariant. We start with a remark in the general case that if $Y = X\backslash f^{-1}(0)$, then $\omega(f)|Y$ is holomorphic on the whole $\Omega(K^\times)$. This can be proved in the same way as the first part of Theorem 8.2.1.

Suppose that $A = \mathrm{Supp}(\Phi)$ is contained in Y and put

$$m_0 = \min_{x\in A}(1, |f(x)|_K), \qquad m_1 = \max_{x\in A}(1, |f(x)|_K).$$

Then $0 < m_0 \le 1 \le m_1 < \infty$ and $m_0 \le |f(x)|_K \le m_1$ for every x in A. Restrict ω in $\Omega(K^\times)$ as $\sigma_0 \le \sigma(\omega) \le \sigma_1$, in which $\sigma_0 \le \sigma_1$ and otherwise arbitrary in $\mathbb{R}$. Then we will have

$$|\omega(f(x))| \le M = \max(m_0^{\sigma_0}, m_1^{\sigma_1})$$

for every x in A. Therefore, if we put $\phi = M\|\Phi\|_\infty\ \chi_A$, then $|\omega(f(x))\Phi(x)| \le \phi(x)$ for every x in X and

$$\int_X \phi(x)\ dx = M\|\Phi\|_\infty \mu_n(A) < \infty.$$

Since $\omega \mapsto \omega(f(x))$ for every x in Y is a holomorphic function on $\Omega(K^\times)$, we see by Lemma 5.3.1 that $\omega(f)(\Phi)$ is a holomorphic function on $\Omega(K^\times)$, hence $\omega(f)|Y$ is holomorphic on $\Omega(K^\times)$.

We shall assume that ω is a variable point of $\Omega(K^\times)$, i.e., $t = \omega(\pi)$ is a variable in $\mathbb{C}^\times$. If ϖ is a pole of $\omega(f)$ in $\Omega(K^\times)$ and

$$\omega(f) = \sum_{k\in\mathbb{Z}} c_k(t-\alpha)^k$$

is its Laurent expansion at $\alpha = \varpi(\pi)$, then all c_k are in $\mathcal{S}(X)'$ with $c_k = 0$ for $k < -n$ by Theorem 8.2.1 and with $\mathrm{Supp}(c_k)$ contained in $f^{-1}(0)$ for $k < 0$ by what we have just shown. We shall denote the order of the pole α by $m = m_\alpha$ and put $T = c_{-m}$. Then $0 < m \le n$, $T \ne 0$ and $\mathrm{Supp}(T)$ is contained in $f^{-1}(0)$. We shall obtain more precise information about T in the case where $f(x)$ is a relative invariant.

We recall that $\mathrm{GL}_n(K)$ is a locally compact totally disconnected group. In fact, the compact open subgroups $1_n + \pi^e M_n(O_K)$ of $\mathrm{GL}_n(K)$ for all $e > 0$ in $\mathbb{N}$ form a base at its unit element 1_n. Furthermore, if we denote the $n \times n$ diagonal matrix with $d_1, \dots, d_n$ as its diagonal entries by $\mathrm{diag}\{d_1, \dots, d_n\}$, then we see by Lemma 7.4.1 that

$$\mathrm{GL}_n(K) = \cup\ \mathrm{GL}_n(O_K)\ \mathrm{diag}\{\pi^{e_1}, \dots, \pi^{e_n}\}\mathrm{GL}_n(O_K),$$

in which the union is taken for all increasing sequences $(e_1, \dots, e_n)$ in $\mathbb{Z}$. Since all double cosets above are compact subsets of $\mathrm{GL}_n(K)$, it is countable at ∞. Consequently, if G is any closed subgroup of $\mathrm{GL}_n(K)$, then it is also a locally compact totally disconnected group which is countable at ∞. We observe that any subgroup

of $\mathrm{GL}_n(K)$ continuously acts on X by matrix-multiplication. We shall assume that the above $f(x)$ is a relative G-invariant, i.e., that $f(gx) = \nu(g)f(x)$ with $\nu(g)$ in $K^\times$ for every g in G. Then necessarily ν is in $\mathrm{Hom}(G, K^\times)$. We let G act on $\mathcal{S}(X)$ and $\mathcal{S}(X)'$ in the usual way, i.e., as

$$(g \cdot \Phi)(x) = \Phi(g^{-1}x), \qquad (g \cdot S)(\Phi) = S(g^{-1} \cdot \Phi)$$

respectively for every Φ in $\mathcal{S}(X)$ and S in $\mathcal{S}(X)'$. Then we have

$$g \cdot \omega(f) = \rho_\omega(g)^{-1}\omega(f),$$

in which $\rho_\omega(g) = \omega(\nu(g))|\det(g)|_K$ for every g in G. In fact, if ω is in $\Omega_0(K^\times)$, then by definition

$$(g \cdot \omega(f))(\Phi) = \int_Y \omega(f(x))\ \Phi(gx)\ dx.$$

If we replace x by $g^{-1}x$, then by using Lemma 7.4.2, we get

$$(g \cdot \omega(f))(\Phi) = \omega(\nu(g))^{-1}\ |\det(g)|_K^{-1}\ \omega(f)(\Phi) = \rho_\omega(g)^{-1}\ \omega(f)(\Phi).$$

This relation is preserved under holomorphic continuation.

If we incorporate the above information in the Laurent expansion of $\omega(f)$ at its pole ϖ, then we get

$$\sum_{k \geq -m} (g \cdot c_k)(t-\alpha)^k = \rho_\omega(g)^{-1} \cdot \sum_{k \geq -m} c_k(t-\alpha)^k$$

for ω close to ϖ, i.e., $\omega|O_K^\times = \varpi|O_K^\times$ and t close to α. Since

$$\omega(a) = (\alpha^{-1}t)^{\mathrm{ord}(a)}\varpi(a)$$

for every a in $K^\times$, we have

$$\rho_\omega(g) = (1 + \alpha^{-1}(t-\alpha))^{\mathrm{ord}(\nu(g))}\rho_\varpi(g)$$

for every g in G. Therefore, if we compare the coefficients of $(t-\alpha)^{-m}$ on both sides of the above relation, then we get

$$g \cdot T = \rho_\varpi(g)^{-1}T$$

for every g in G. In the notation of Chapter 7.2-7.3 this means that $T \neq 0$ is an element of $\mathcal{E}_X(\rho_\varpi)$. Therefore, if the number of G-orbits in X is countable, i.e., at most countable, then we can apply Theorem 7.3.1 to T. It gives the structure of the eigendistribution T as well as the following information about the pole ϖ of $\omega(f)$:

Theorem 8.5.1 *Suppose that a closed subgroup G of $\mathrm{GL}_n(K)$ acts on $X = K^n$ with countably many orbits and $f(x)$ in $K[x_1, \ldots, x_n]\backslash K$ is a relative G-invariant, i.e., $f(gx) = \nu(g)f(x)$ with $\nu(g)$ in $K^\times$ for every g in G; let ϖ denote any pole of $\omega(f)$ and*

$$\omega(f) = \sum_{k \geq -m} c_k(t-\alpha)^k, \qquad T = c_{-m} \neq 0$$

its Laurent expansion at $\alpha = \varpi(\pi)$ *where* $t = \omega(\pi)$. *Then Supp*(T) *is contained in* $f^{-1}(0)$. *Furthermore, if* ξ *is a point of any open* G*-orbit in Supp*(T) *and* H *is the fixer of* ξ *in* G, *then*

$$\varpi(\nu(g)) = \Delta_H(g) \ / \ (\Delta_G(g) \ |\det(g)|_K)$$

for every g *in* H. *In particular,* $\varpi \circ \nu$ *is* $\mathbb{R}_+^\times$*-valued on* H.

In the above theorem it is, of course, enough to assume that the number of G-orbits in $f^{-1}(0)$ is countable. The theorem can be applied to the case where $f(x)$ is a basic relative invariant of a regular prehomogeneous vector space. We might mention that the theorem was proved in that case under the assumption that the number of G-orbits in $f^{-1}(0)$ is finite. In fact, our proof in [25] is basically the same as the one we have just given. We might remark that the countability assumption on the number of G-orbits is very strong. However, it has been reported by A. Gyoja [18] that he succeeded in removing that restriction.

https://doi.org/10.1090/amsip/014/09

Chapter 9

Some homogeneous polynomials

9.1 Quadratic forms and Witt's theorem

We shall make ourselves familiar with those homogeneous polynomials for which we shall later compute $Z(s)$. We shall start with quadratic forms. We take an arbitrary field K and consider vector spaces over K all assumed to be finite dimensional. If X is such a vector space, as before we shall denote its dual space by X^* and put $[x, x^*] = x^*(x)$ for every (x, x^*) in $X \times X^*$. A *quadratic form* Q on X is a K-valued function on X satisfying the following conditions:

(Q1) $Q(\lambda x) = \lambda^2 Q(x)$ for every λ in K and x in X.

(Q2) $Q(x, y) = Q(x + y) - Q(x) - Q(y)$ is K-bilinear on $X \times X$.

It follows from the definition that $Q(x, y) = Q(y, x)$, $Q(x, x) = 2Q(x)$, and $Q|Y$ for any subspace Y of X is a quadratic form on Y. The value of Q on any K-linear combination $\lambda_1 x_1 + \ldots + \lambda_n x_n$ of $x_1, \ldots, x_n$ in X can be determined by the formula

$$Q\Big(\sum_{1 \le i \le n} \lambda_i x_i\Big) = \sum_{1 \le i \le n} Q(x_i)\lambda_i^2 + \sum_{1 \le i < j \le n} Q(x_i, x_j)\lambda_i \lambda_j,$$

which can easily be proved by an induction on n. If S is any subset of X, we denote by $\langle S \rangle$ the K-span of S, i.e., the set of all K-linear combinations of elements of S, and by $S^\perp$ the set of all x in X satisfying $Q(x, y) = 0$ for every y in S. By definition they are both subspaces of X. Furthermore, we denote by $Q^{-1}(0)$ the set of all x in X satisfying $Q(x) = 0$. If $X^\perp = 0$, then Q is called *nondegenerate* and if $Q^{-1}(0) = 0$, then Q is called *anisotropic*. We observe that $X^\perp \cap Q^{-1}(0)$ for any quadratic form Q is a subspace of X. If this subspace is 0, we propose to call Q *reduced* for the following reason. The set of all x_0 in X satisfying $Q(x + x_0) = Q(x)$ for every x in X forms a subspace of X and this subspace is $X^\perp \cap Q^{-1}(0)$. Therefore, Q is reduced if and only if it does not come from a quadratic form Q_0 on a factor space X/X_0 by a subspace $X_0 \neq 0$ as $Q(x) = Q_0(x + X_0)$. At any rate, if Q is either nondegenerate or anisotropic, then it is clearly reduced. If $\mathrm{char}(K) \neq 2$, then in view of $Q(x, x) = 2Q(x)$ every reduced quadratic form is nondegenerate. We might remark that if $X = Ka$, where $\mathrm{char}(K) = 2$ and $Q(a) \neq 0$, then Q is anisotropic, hence reduced, but degenerate, i.e., Q is not nondegenerate.

If Y, Y' are subspaces of X such that $Q(y, y') = 0$ for every y, y' in Y, Y', then they are called orthogonal. If Y_1, Y_2, ... are mutually orthogonal subspaces of X such that X becomes their direct sum, we write

$$X = Y_1 \oplus Y_2 \oplus \cdots$$

and call it an orthogonal direct sum. Suppose that Y is any subspace of X. Then $Q|Y$ is nondegenerate if and only if $Y \cap Y^\perp = 0$ and in that case

$$(*) \qquad \dim_K(Y^\perp) = \dim_K(X) - \dim_K(Y),$$

hence $X = Y \oplus Y^\perp$. One way to see $(*)$ is as follows. We take a K-basis say $\{w_1, \ldots, w_n\}$ for X such that the first p elements form a K-basis for Y and identify X with K^n as $x = \sum \lambda_i w_i \mapsto \lambda = {}^t(\lambda_1 \cdots \lambda_n)$. We denote by h the $p \times n$ matrix with $h_{ij} = Q(w_i, w_j)$ as its (i,j)-entry for $1 \leq i \leq p$, $1 \leq j \leq n$ and by h_0 the $p \times p$ submatrix of h composed of its first p columns. Then $Q|Y$ is nondegenerate if and only if $\det(h_0) \neq 0$ and x is in $Y^\perp$ if and only if $h\lambda = 0$. Since $\operatorname{rank}(h) = p = \dim_K(Y)$ and $n = \dim_K(X)$, therefore we get $(*)$. We observe that, in the case where $Q|Y$ is nondegenerate, if Q is nondegenerate (resp. reduced), then $Q|Y^\perp$ is nondegenerate (resp. reduced). We also remark that if $Q|Y$ and $Q|Y^\perp$ are both nondegenerate, then $(Y^\perp)^\perp = Y$ and the relation of Y and $Y^\perp$ is symmetric.

We shall prove Witt's theorem in [61], which is fundamental in the theory of quadratic forms. We shall start with three lemmas.

Lemma 9.1.1 *Let Y, Y' denote subspaces of a vector space X both different from X. Then their union is also different from X, i.e., strictly smaller than X.*

Proof. Suppose that X is the union of Y and Y'. Then, by replacing Y, Y' by larger subspaces if necessary, we may assume that they are both of codimension 1 in X. We can then write $X = Y + Ka$ for any a in $X \backslash Y$. Also we can express Y' as the set of all x satisfying $[x, a^*] = 0$ for some $a^* \neq 0$ in X^*. Since X is the union of Y and Y', we see that $y + \lambda a$ for every y in Y and $\lambda \neq 0$ in K is in Y', hence

$$[y + \lambda a, a^*] = [y, a^*] + [a, a^*]\lambda = 0.$$

We can take $y = 0$, and we get $[a, a^*] = 0$. Then $[y + \lambda a, a^*] = 0$ for every y in Y and λ in K, hence X is contained in Y'. This is a contradiction.

Lemma 9.1.2 *Suppose that Q is a reduced quadratic form on X and $Q(a) = 0$ for some $a \neq 0$ in X. Then $Q(a, b) = 1$ and $Q(b) = 0$ for some b in X. Furthermore, if we put $X' = \langle a, b\rangle^\perp$, then $Q|\langle a, b\rangle$ is nondegenerate, hence $Q|X'$ is reduced and X becomes the orthogonal direct sum*

$$X = \langle a, b\rangle \oplus X'.$$

Proof. Since Q is reduced and $Q(a) = 0$, $a \neq 0$, we see that a is not in $X^\perp$. Therefore, the K-linear map $x \mapsto Q(a, x)$ from X to K is surjective, hence $Q(a, b_0) = 1$ for some b_0 in X. If we put $b = b_0 - Q(b_0)a$, then $Q(a, b) = 1$ and $Q(b) = 0$. Futhermore, if λ, μ, λ', μ' are in K, then

$$Q(\lambda a + \mu b, \lambda' a + \mu' b) = \lambda\mu' + \mu\lambda',$$

hence $\langle a,b\rangle \cap \langle a,b\rangle^{\perp} = 0$. Therefore, $Q|\langle a,b\rangle$ is nondegenerate. The rest follows from our previous remark.

If Q, Q' are arbitrary quadratic forms on vector spaces X, X' respectively, then a K-linear injection $g : X \to X'$ satisfying $Q'(gx) = Q(x)$ for every x in X is called an *isometry* from X to X'. If Q is reduced, the group of all isometries from X to itself is called the *orthogonal group* of Q, and it will be denoted by $\mathrm{O}(Q)$.

Lemma 9.1.3 *Let Q denote a nondegenerate quadratic form on X and $X = \langle a,b\rangle \oplus X'$ as in Lemma 9.1.2. Then every isometry g from $Y = Kb + X'$ to itself uniquely extends to an element g^* of $\mathrm{O}(Q)$.*

Proof. We shall only assume, until the last moment, that Q is reduced. Since b is in $Y^{\perp}$ and $gY = Y$, we see that gb is in $Y^{\perp}$. Therefore, if we put $c = gb - Q(a,gb)b$, then c is in $Y^{\perp}$ and $Q(a,c) = 0$, hence c is in $X^{\perp}$. Since $Q(c) = Q(gb) = 0$ and Q is reduced, we get $c = 0$, hence $gb = Q(a,gb)b$ with $\tau_0 = Q(a,gb) \neq 0$. If x is in X', we can write $gx = (lx)b + \sigma x$ with K-linear maps $l : X' \to K$ and $\sigma : X' \to X'$. If $\sigma c' = 0$ for some c' in X', then $gx' = 0$ for $x' = -\tau_0^{-1}(lc')b + c'$, hence $x' = 0$, and hence $c' = 0$. Therefore, σ is an injection, hence a bijection, and the condition of g being an isometry simply becomes σ in $\mathrm{O}(Q|X')$.

We now take λ_0, μ_0 from K and x_0 from X', put $g^*a = \lambda_0 a + \mu_0 b + x_0$, and require that g^* acts on Y as g. Then the condition on the K-linear map $g^* : X \to X$ so defined to give an element of $\mathrm{O}(Q)$ becomes $\lambda_0 \neq 0$ and

$$(\lambda_0\mu_0 + Q(x_0))\lambda^2 + (\lambda_0\tau_0 - 1)\lambda\mu + (\lambda_0(lx) + Q(x_0,\sigma x))\lambda = 0$$

for all λ, μ in K and x in X'. If we take $\lambda = 1$, $\mu = 0$, $x = 0$, we get $\lambda_0\mu_0 + Q(x_0) = 0$; then if we put $\lambda = \mu = 1$, $x = 0$, we get $\lambda_0\tau_0 - 1 = 0$; finally if we put $\lambda = 1$, we get $\lambda_0(lx) + Q(x_0,\sigma x) = 0$ for every x in X'. Since the converse is clear, the condition becomes $\lambda_0 = \tau_0^{-1}$, $\mu_0 = -\tau_0 Q(x_0)$, and

$$Q(x_0,x) = -\tau_0^{-1} l(\sigma^{-1}x)$$

for every x in X'. If we invoke the assumption that Q is nondegenerate, then $Q|X'$ is nondegenerate, hence such an x_0 exists and is unique.

Now the Witt theorem is the following generalization of Lemma 9.1.3. The proof which we shall explain is due to C. Chevalley [7].

Theorem 9.1.1 *Let Q denote a nondegenerate quadratic form on a vector space X over an arbitrary field K and Y any subspace of X. Then every isometry $g_0 : Y \to X$ extends to an element g of $\mathrm{O}(Q)$.*

Proof. The extendability of g_0 is trivial if $Y = 0$ or $Y = X$. Therefore, we shall assume that $Y \neq 0$, X and apply an induction on $\dim_K(Y)$. Let Z denote any subspace of Y of codimension 1 in Y. Then by induction $g_0|Z$ extends to an element g_1 of $\mathrm{O}(Q)$. If $(g_1|Y)^{-1}g_0$ has an extension g_2, then g_1g_2 gives an extension of g_0. Since $(g_1|Y)^{-1}g_0|Z = \mathrm{id}_Z$, the identity map of Z, we may assume from the beginning that $g_0|Z = \mathrm{id}_Z$. We may further assume that $g_0 \neq \mathrm{id}_Y$ for otherwise the extendability of g_0 becomes trivial. We denote by Σ the set of all subspaces Z_1

of X containing Z such that g_0 extends to an isometry $g_1 : Y + Z_1 \to X$ satisfying $g_1|Z_1 = \mathrm{id}_{Z_1}$. The set Σ is not empty because Z is its member. Since $g_0 \neq \mathrm{id}_Y$, Y is not contained in Z_1, hence $Z = Y \cap Z_1$, and hence Z_1 is of codimension 1 in $Y + Z_1$. We shall now assume that Z_1 is maximal in Σ. After replacing Y, Z by $Y + Z_1$, Z_1, we may then assume that Z is the only member of Σ, and we shall examine the consequence of this assumption.

We write $Y = Z + Ka$ necessarily with a in $Y \backslash Z$ and put $b = g_0 a$. Then b is not in Z and $b \neq a$ because $g_0 \neq \mathrm{id}_Y$. Furthermore if we put $Y' = Z + Kb$, then the condition that $g_0 : Y \to Y'$ is an isometry becomes

$$(Q(a) - Q(b))\lambda^2 + Q(a - b, z)\lambda = 0$$

for every λ in K and z in Z. This is equivalent to $Q(a) = Q(b)$ and $a - b$ in $Z^\perp$. If now $H = (a-b)^\perp$, then H is contained in $Y \cup Y'$. Otherwise H contains c which is not in $Y \cup Y'$. Then we can easily verify that the prescription $g_1 : \lambda a + \mu c + z \mapsto \lambda b + \mu c + z$ for every λ, μ in K and z in Z defines an isometry g_1 from $Y + Kc$ to $Y' + Kc$ with the property that $g_1|Y = g_0$ and $g_1|Z_1 = \mathrm{id}_{Z_1}$ for $Z_1 = Z + Kc$, hence $Z_1 \neq Z$ becomes a member of Σ. This contradicts the assumption. Therefore, H is contained in $Y \cup Y'$, hence H becomes the union of $H \cap Y$ and $H \cap Y'$. This implies by Lemma 9.1.1 that H is contained either in Y or in Y'. Since the codimension of H in X is at most 1 for any Q, this implies that either $H = Y$ or $H = Y'$, hence either $Q(a, a - b) = 0$ or $Q(b, a - b) = 0$. Since $Q(a) = Q(b)$, we then get both $Q(a, a - b) = 0$ and $Q(b, a - b) = 0$, hence $H = Y = Y'$. If we put $a_1 = a - b$, then $a_1 \neq 0$ and $Q(a_1) = 0$. Therefore by Lemma 9.1.2, we will have $X = \langle a_1, b_1 \rangle \oplus X'$ for some b_1 satisfying $Q(a_1, b_1) = 1$ and $Q(b_1) = 0$ with X' necessarily contained in Y. Then g_0 becomes an isometry from $Y = Ka_1 + X'$ to itself. Since Q is nondegenerate by assumption, we see by Lemma 9.1.3 that g_0 uniquely extends to an element of $\mathrm{O}(Q)$.

Theorem 9.1.2 *If Q is a reduced quadratic form on a vector space X over an arbitrary field K, then X contains $2p$ elements $a_1, \ldots, a_p$, $b_1, \ldots, b_p$ satisfying $Q(a_i) = Q(b_i) = 0$, $Q(a_i, b_i) = 1$ for $1 \leq i \leq p$ such that it becomes an orthogonal direct sum*

$$X = \langle a_1, b_1 \rangle \oplus \cdots \oplus \langle a_p, b_p \rangle \oplus X_0$$

with $Q|X_0$ anisotropic. Furthermore, if Q is nondegenerate, then up to an isometry the anisotropic kernel X_0 does not depend on the choice of such a Witt decomposition of X.

Proof. If Q is reduced but not anisotropic, then by Lemma 9.1.2 we will have $X = \langle a, b \rangle \oplus X'$, in which $Q(a) = Q(b) = 0$, $Q(a, b) = 1$ and $Q|X'$ is reduced. If $Q|X'$ is not anisotropic, we can apply Lemma 9.1.2 to $Q|X'$. In that way we get a decomposition of X as stated. If

$$X = \langle a'_1, b'_1 \rangle \oplus \cdots \oplus \langle a'_q, b'_q \rangle \oplus X'_0$$

is a similar decomposition of X, we may assume by symmetry that $p \leq q$. Then the prescription $g_0 a_i = a'_i$, $g_0 b_i = b'_i$ for $1 \leq i \leq p$ defines an isometry g_0 from

$H = \langle a_1, b_1\rangle \oplus \cdots \oplus \langle a_p, b_p\rangle$ to $H' = \langle a'_1, b'_1\rangle \oplus \cdots \oplus \langle a'_p, b'_p\rangle$. If now Q is nondegenerate, then g_0 extends by Theorem 9.1.1 to an element g of $\mathrm{O}(Q)$, and

$$gX_0 = g(H^\perp) = (gH)^\perp = \langle a'_{p+1}, b'_{p+1}\rangle \oplus \cdots \oplus \langle a'_q, b'_q\rangle \oplus X'_0.$$

Since $Q|X_0$ is anisotropic, so is $Q|gX_0$. Therefore $q = p$ and $gX_0 = X'_0$.

We call the unique p in Theorem 9.1.2 the *Witt index* of Q. We observe that if we put $W = \langle a_1, \ldots, a_p\rangle$, then $Q|W = 0$. Such a subspace of X is called *totally isotropic*. We shall show that W is maximal, i.e., it is not contained in a strictly larger totally isotropic subspace. Any element x of X can be written uniquely as

$$x = \sum_{1\le i\le p} (\lambda_i a_i + \mu_i b_i) + x_0$$

with λ_i, μ_i in K for all i and x_0 in X_0. We observe that $W + Kx$ is totally isotropic if and only if $\mu_i = 0$ for all i and $Q(x_0) = 0$, hence $x_0 = 0$ because $Q|X_0$ is anisotropic, and hence x is in W. Furthermore, if W_1, W_2 are any two maximal totally isotropic subspaces of X and $\dim_K(W_1) \le \dim_K(W_2)$, then any K-linear injection from W_1 to W_2 is an isometry, hence it extends to an element g of $\mathrm{O}(Q)$ by Theorem 9.1.1. Then $g^{-1}W_2$ is totally isotropic and contains W_1, hence $W_1 = g^{-1}W_2$ by the maximality of W_1. Therefore $\mathrm{O}(Q)$ acts transitively on the set of all maximal totally isotropic subspaces of X.

If $\{w_1, \ldots, w_p\}$ is a K-basis for any totally isotropic subspace W of X, then we can find another totally isotropic subspace W' of X with a K-basis $\{w'_1, \ldots, w'_p\}$ satisfying $Q(w_i, w'_j) = \delta_{ij}$ for $1 \le i,\ j \le p$. This can be proved directly or simply by embedding W in a maximal totally isotropic subspace of X in any Witt decomposition of X. We call $H = W + W'$ a *hyperbolic subspace* of X. We observe that $Q|H$ is nondegenerate.

Remark. In the proof of Theorem 9.1.1 the nondegeneracy assumption on Q is used only at the last stage where we have applied Lemma 9.1.3. Furthermore in the proof of Lemma 9.1.3 the nondegeneracy assumption of Q is used only for the existence of "x_0" there. The fact is that if we just assume Q to be reduced, such an x_0 may not exist. In fact, Lemma 9.1.3 and Theorem 9.1.1 break down as the following example shows. Let K denote any field with $\mathrm{char}(K) = 2$, X a three-dimensional vector space over K with a basis $\{a, b, c\}$, and

$$Q(\alpha a + \beta b + \gamma c) = \alpha\beta + \gamma^2$$

for every α, β, γ in K. Then we see that Q is a reduced quadratic form on X. Put $Y = Kb + Kc$ and define an isometry $g : Y \to Y$ as $g(\beta b + \gamma c) = (\beta + \gamma)b + \gamma c$. Then there is no g^* in $\mathrm{O}(Q)$ which extends g. In fact, if such a g^* exists, then $g^*a = \alpha_0 a + \beta_0 b + \gamma_0 c$ for some $\alpha_0, \beta_0, \gamma_0$ in K. Since $g^*X = X$, we have $\alpha_0 \ne 0$ while $\alpha_0 = Q(g^*a, g^*c) = Q(a, c) = 0$. This is a contradiction.

9.2 Quadratic forms over finite fields

We shall denote by X a finite dimensional vector space over a field K and by Q a reduced quadratic form on X. We shall assume that K is a finite field and make

some computation to prepare for section 9.3. As a side result, we shall show that the anisotropic kernel X_0 in Theorem 9.1.2 is unique up to an isometry. Actually, although we have not included its proof in this book, the above uniqueness holds for any K. At any rate, we shall start with some general observations without assuming that K is finite.

In the case where $\mathrm{char}(K) \neq 2$, there is a classical diagonalization of an arbitrary quadratic form Q on X stating that X has a K-basis $\{w_1, \dots, w_n\}$, hence $\dim_K(X) = n$, such that

$$Q\Big(\sum_{1\leq i\leq n} x_i w_i\Big) = \sum_{1\leq i\leq n} Q(w_i)x_i^2$$

for every $x_1, \dots, x_n$ in K. If $Q = 0$ and $\{w_1, \dots, w_n\}$ is any K-basis for X, then it trivially has the required property. If $Q \neq 0$, then $Q(w_1) \neq 0$ for some w_1 in X. We observe that $Q|Kw_1$ is then nondegenerate, hence $X = Kw_1 \oplus (Kw_1)^\perp$. Therefore we have only to apply an induction on the dimension to $Q|(Kw_1)^\perp$ to find the remaining $w_2, \dots, w_n$.

Suppose that K is arbitrary for a moment, take a K-basis $\{w_1, \dots, w_n\}$ for X, and define a symmetric matrix h with $h_{ij} = Q(w_i, w_j)$ as its (i, j)-entry for $1 \leq i,\ j \leq n$. Then Q is nondegenerate if and only if $\det(h) \neq 0$. In that case

$$d(Q) = (-1)^{n(n-1)/2} \det(h)$$

is called the *discriminant* of Q. If we use another K-basis for X, then h will be replaced by $gh^t g$ for some g in $\mathrm{GL}_n(K)$, hence $d(Q)(K^\times)^2$ is a well-defined element of $K^\times/(K^\times)^2$. Furthermore, if X, X' equipped with nondegenerate quadratic forms Q, Q' are isometric, then $d(Q)(K^\times)^2 = d(Q')(K^\times)^2$ and if $X = H \oplus H^\perp$ for any hyperbolic subspace H, then

$$d(Q)(K^\times)^2 = d(Q\big|H^\perp)(K^\times)^2.$$

If now K is a finite field with $\mathrm{char}(K) \neq 2$, i.e., if $K = \mathbb{F}_q$ for an odd q, then $K^\times/(K^\times)^2$ is isomorphic to $\{\pm 1\}$. If we denote by χ the character of $K^\times$ which gives rise to this isomorphism, then $\chi(d(Q))$ depends only on the isometry class of Q and, in fact, on that of its anisotropic kernel.

We recall that if $K = \mathbb{F}_q$, where q is arbitrary, then K has $L = \mathbb{F}_{q^e}$ as its unique, hence normal, extension of degree e for every $e > 0$ in $\mathbb{N}$ and that the Galois group of L over K is the cyclic group generated by $x \mapsto x^q$. We shall denote the norm homomorphism $L^\times \to K^\times$ by $N = N_{L/K}$ and show that N is surjective. Since $N(x)$ is the product of $x, x^q, x^{q^2}, \dots$, we have

$$N(x) = x^E, \qquad E = (q^e - 1)/(q - 1),$$

hence $\mathrm{card}(\mathrm{Ker}(N)) \leq E$. Since $\mathrm{card}(\mathrm{Im}(N)) \leq \mathrm{card}(K^\times) = q - 1$ and $\mathrm{card}(L^\times) = q^e - 1$, we have equalities at both places. In particular, N is surjective. We shall restrict our attention to the case where $e = 2$. We observe that if we put $N(0) = 0$, then $Q = N$ gives a nondegenerate quadratic form on the vector space L over K.

In fact, if $\{1, \xi\}$ is a K-basis for L, i.e., if ξ is an element of $L \backslash K$, and if we express any x in L as $x = x_1 + x_2\xi$ with x_1, x_2 in K, then

$$Q(x) = N(x_1 + x_2\xi) = x_1^2 + ax_1x_2 + bx_2^2,$$

in which $a = \xi + \xi^q$, $b = \xi^{1+q}$, and $Q(x, y) = 2x_1y_1 + a(x_1y_2 + x_2y_1) + 2bx_2y_2$ for a similar element $y = y_1 + y_2\xi$ of L. Therefore, if $Q(x, y) = 0$ for every y in L, then $ax_1 + 2bx_2 = 2x_1 + ax_2 = 0$. Since the determinant of the coefficient-matrix is $a^2 - 4b = (\xi - \xi^q)^2 \neq 0$, we get $x = 0$. In the following, $L = \mathbb{F}_{q^2}$ will always be equipped with the quadratic form N.

Lemma 9.2.1 *Let X denote a two-dimensional vector space over $K = \mathbb{F}_q$ and Q any anisotropic quadratic form on X. Then X is isometric to $L = \mathbb{F}_{q^2}$, hence Q is nondegenerate.*

Proof. If $\{w_1, w_2\}$ is any K-basis for X, hence $Q(w_1) \neq 0$, and

$$Q(x_1w_1 + x_2w_2) = Q(w_1)(x_1^2 + ax_1x_2 + bx_2^2)$$

for x_1, x_2 in K, then a zero ξ of $t^2 - at + b$ is not in K. Otherwise, $x = \xi w_1 - w_2$ is in X, $Q(x) = 0$, and yet $x \neq 0$, which is a contradiction. Therefore, $L = K(\xi) = K + K\xi$. We observe that $N(x_1 + x_2\xi) = x_1^2 + ax_1x_2 + bx_2^2$. As we have remarked, we can write $Q(w_1) = N(\alpha)$ with some α in $L^\times$. If we put

$$\theta(x_1w_1 + x_2w_2) = \alpha(x_1 + x_2\xi),$$

since the multiplication by α is a K-linear bijection from L to itself, we see that θ gives a K-linear bijection from X to L satisfying $N(\theta(x_1w_1 + x_2w_2)) = Q(x_1w_1 + x_2w_2)$ for every x_1, x_2 in K. We have already remarked that N is nondegenerate. Therefore Q is also nondegenerate.

Lemma 9.2.2 *If there exists an anisotropic quadratic Q on a vector space X over $K = \mathbb{F}_q$, then necessarily* $\dim_K(X) \leq 2$.

Proof. Suppose that $\dim_K(X) > 2$ and take any two-dimensional subspace Y of X. Then $Q|Y$ is anisotropic, hence nondegenerate by Lemma 9.2.1, and hence $X = Y \oplus Y^\perp$. Since $Y^\perp \neq 0$, it contains $y \neq 0$, and then $Q(y) \neq 0$. Since $Q|Y$ is isometric to $L = \mathbb{F}_{q^2}$ and N is surjective, we can find x in Y satisfying $Q(x) = -Q(y)$. Then $Q(x + y) = 0$ and $x + y \neq 0$, which is a contradiction.

We are ready to prove the following theorem, in which $Q^{-1}(i)$ for every i in K denotes the set of all x in X satisfying $Q(x) = i$:

Theorem 9.2.1 *Let Q denote a reduced quadratic form on a vector space X over $K = \mathbb{F}_q$, i.e., a quadratic form Q on X satisfying $X^\perp \cap Q^{-1}(0) = 0$. If* $\dim_K(X) = 2m$, *the anisotropic kernel of Q is either 0 or $L = \mathbb{F}_{q^2}$, and if we respectively put $\chi(Q) = \pm 1$, then*

$$\mathrm{card}(Q^{-1}(i)) = \begin{cases} q^{2m-1} + \chi(Q)\ (q^m - q^{m-1}) & i = 0 \\ q^{2m-1} - \chi(Q)\ q^{m-1} & i \neq 0. \end{cases}$$

Furthermore, if q is odd, then $\chi(Q) = \chi(d(Q))$. If $\dim_K(X) = 2m+1$, the anisotropic kernel of Q is one-dimensional, hence of the form Kw. If q is odd, there are also two cases separated by $\chi(2d(Q)) = \chi(Q(w))$, and

$$\mathrm{card}(Q^{-1}(i)) = \begin{cases} q^{2m} & i = 0 \\ q^{2m} + \chi(2d(Q)i)q^m & i \neq 0, \end{cases}$$

but if q is even, there is only one case and $\mathrm{card}(Q^{-1}(i)) = q^{2m}$ for every i.

Proof. If $\dim_K(X) = 2m$, then by Lemmas 9.2.1, 9.2.2 the anisotropic kernel has the two possibilities stated in the theorem. If we can prove the formula for $\mathrm{card}(Q^{-1}(0))$, then it will show that the two cases are independent of the decomposition of X in Theorem 9.1.2. Furthermore, if $L = K(\xi)$ and $\xi^2 - a\xi + b = 0$ as before, then with respect to the K-basis $\{1, \xi\}$ for L we have $d(N) = a^2 - 4b$, which is $(\xi - \xi^q)^2$. Therefore if q is odd, then $d(N)$ is not in $(K^\times)^2$, hence $\chi(d(N)) = -1$, and hence $\chi(Q) = \chi(d(Q))$. On the other hand, if $\dim_K(X) = 2m+1$, then by Lemma 9.2.2 the anisotropic kernel is of the form Kw for some w in X and $Q(w)(K^\times)^2$ clearly determines its isometry class. Since $\chi(2d(Q)) = \chi(Q(w))$ if q is odd, what remains to be proved is only the formula for $\mathrm{card}(Q^{-1}(i))$.

First of all, in the notation of Theorem 9.1.2 we have

$$Q\Big(\sum_{1 \le i \le p} (x'_i a_i + x''_i b_i) + x_0\Big) = {}^t x' x'' + Q(x_0)$$

for every $x' = {}^t(x'_1 \dots x'_p)$, $x'' = {}^t(x''_1 \dots x''_p)$ in K^p and x_0 in X_0. If now $Q(x) = {}^t x' x''$ for x', x'' in K^m and i is in $K^\times$, then $Q(x) = i$ implies $x' \neq 0$. The number of such x' is $q^m - 1$ and for each $x' \neq 0$ the number of x'' satisfying ${}^t x' x'' - i = 0$ is q^{m-1}, hence

$$\mathrm{card}(Q^{-1}(i)) = (q^m - 1)q^{m-1} = q^{2m-1} - q^{m-1}.$$

If $i = 0$, we have only to add the number of $x' = 0$ and x'' free in K^m, hence

$$\mathrm{card}(Q^{-1}(0)) = q^{2m-1} + q^m - q^{m-1}.$$

If $Q(x) = {}^t x' x'' + N(\xi)$ for x', x'' in K^{m-1} and ξ in L, then $\mathrm{card}(Q^{-1}(0))$ is the sum of the numbers of solutions of $N(\xi) = -{}^t x' x'' = 0$ and $= i$ in $K^\times$. Since $\mathrm{card}(N^{-1}(0)) = 1$ and $\mathrm{card}(N^{-1}(i)) = q + 1$ for i in $K^\times$, we therefore get

$$\begin{aligned} \mathrm{card}(Q^{-1}(0)) &= (q^{2m-3} + q^{m-1} - q^{m-2}) + (q-1)(q+1)(q^{2m-3} - q^{m-2}) \\ &= q^{2m-1} - q^m + q^{m-1}. \end{aligned}$$

As for $\mathrm{card}(Q^{-1}(i))$ for i in $K^\times$, if $N(\alpha) = i$, then $Q^{-1}(1)$ is mapped bijectively to $Q^{-1}(i)$ under $(x', x'', \xi) \mapsto (ix', x'', \alpha\xi)$. Therefore, $\mathrm{card}(Q^{-1}(i))$ is independent of i, hence $(q-1)\mathrm{card}(Q^{-1}(i)) + \mathrm{card}(Q^{-1}(0)) = q^{2m}$, and hence

$$\mathrm{card}(Q^{-1}(i)) = q^{2m-1} + q^{m-1}.$$

In the above argument we have tacitly assumed that $m > 1$, but the formulas are valid also for $m = 1$.

If $Q(x) = {}^t x' x'' + a x_0^2$ for x', x'' in K^m, x_0 in K, and a is in $K^\times$, we add the numbers of solutions in x', x'' of ${}^t x' x'' = -a x_0^2$ for all x_0 in K. In that way we get

$$\mathrm{card}(Q^{-1}(0)) = q(q^{2m-1} - q^{m-1}) + q^m = q^{2m}.$$

As for $\mathrm{card}(Q^{-1}(i))$ for i in $K^\times$, we shall first assume that q is odd. We introduce a quadratic form $Q_1(x, x_1) = {}^t x' x'' + a x_0^2 - i x_1^2$, in which x_1 is a new variable, and compute $\mathrm{card}(Q_1^{-1}(0))$ directly and also as the sum of the numbers of solutions in x of $Q_1(x, x_1) = 0$ for all x_1 in K. Since $\chi(d(Q_1)) = \chi(ai)$, we then get

$$\mathrm{card}(Q_1^{-1}(0)) = q^{2m+1} + \chi(ai)(q^{m+1} - q^m) = q^{2m} + (q-1)\mathrm{card}(Q^{-1}(i)).$$

This implies

$$\mathrm{card}(Q^{-1}(i)) = q^{2m} + \chi(ai) q^m,$$

in which $\chi(ai) = \chi(2d(Q)i)$. We shall next assume that q is even. Then the square map gives an automorphism of K. Therefore, if we write $a = b^2$, $i = j^2$ with b in $K^\times$, j in K, then $-a x_0^2 + i = (b x_0 + j)^2$. Since $x_0 \mapsto b x_0 + j$ gives a bijection from K to itself, if we put $Q_0(x) = {}^t x' x'' + x_0^2$, then $\mathrm{card}(Q^{-1}(i)) = \mathrm{card}(Q_0^{-1}(0))$. Therefore, we get $\mathrm{card}(Q^{-1}(i)) = q^{2m}$ by the above result or from $q \cdot \mathrm{card}(Q^{-1}(i)) = q^{2m+1}$ for all i in K.

9.3 Classical groups over finite fields

We shall define classical groups over an arbitrary field K and compute their orders in the case where K is a finite field, i.e., $K = \mathbb{F}_q$. This topic goes back to L. E. Dickson [12]. We shall use the fact that if a finite group G acts transitively on a set S and if H is the fixer in G of any point ξ of S, then the bijection $G/H \to S$ defined by $g \mapsto g\xi$ implies $\mathrm{card}(G) = \mathrm{card}(S)\mathrm{card}(H)$. We shall also use the notation

$$[i] = 1 - q^{-i}, \qquad [i]_+ = 1 + q^{-i}$$

for every i in $\mathbb{N}$.

We observe that $G = \mathrm{GL}_n(K)$ acts transitively on $S = K^n \backslash \{0\}$ by matrix-multiplication. If we express any element g of $\mathrm{GL}_n(K)$ by its 1×1, $1 \times (n-1)$, $(n-1) \times 1$, $(n-1) \times (n-1)$ entry matrices g_{11}, g_{12}, g_{21}, g_{22}, then the fixer H of $e_1 = {}^t(1\ 0 \ldots 0)$ in G is defined by $g_{11} = 1$, $g_{21} = 0$ necessarily with g_{22} in $\mathrm{GL}_{n-1}(K)$. Therefore, if $K = \mathbb{F}_q$, since $\mathrm{card}(S) = q^n[n]$, we get

$$\mathrm{card}(\mathrm{GL}_n(K)) = q^n[n] \cdot q^{n-1}\mathrm{card}(\mathrm{GL}_{n-1}(K)).$$

We have tacitly assumed that $n > 1$, but if $n = 1$, then $\mathrm{GL}_1(K) = K^\times$, hence $\mathrm{card}(\mathrm{GL}_1(K)) = q[1]$. Therefore, by an induction on n we get

$$\mathrm{card}(\mathrm{GL}_n(K)) = q^{n^2} \cdot \prod_{1 \le i \le n} [i].$$

Furthermore, $g \mapsto \det(g)$ gives a homomorphism from $\mathrm{GL}_n(K)$ to $K^\times$ and the kernel is denoted by $\mathrm{SL}_n(K)$. If $d = \mathrm{diag}\{\tau, 1, \dots, 1\}$, i.e., a diagonal matrix with $\tau, 1, \dots, 1$ as its diagonal entries, then $\det(d) = \tau$ for every τ in $K^\times$. Therefore, the above homomorphism is surjective, hence $\mathrm{card}(\mathrm{SL}_n(K)) = \mathrm{card}(\mathrm{GL}_n(K))/q[1]$, and hence

$$\mathrm{card}(\mathrm{SL}_n(K)) = q^{n^2-1} \cdot \prod_{1<i\le n} [i].$$

We next take a reduced quadratic form Q on a vector space X over K and define the orthogonal group $\mathrm{O}(Q)$ of Q as in section 9.1. We observe that if $g : X \to X$ is any K-linear transformation satisfying $Q(gx) = Q(x)$ for every x in X, then g is necessarily an injection, hence a bijection. In fact, if $gx = 0$ for some x in X, then $Q(x, y) = Q(gx, gy) = 0$ for every y in X and $Q(x) = Q(gx) = 0$, hence x is in $X^\perp \cap Q^{-1}(0)$, and hence $x = 0$ because Q is reduced. Therefore $\mathrm{O}(Q)$ consists of all such g.

After this remark, we shall consider the special case where $X = K^{2m}$ and

$$Q(x) = \sum_{1\le i\le m} x_{2i-1}x_{2i} = x_1x_2 + x_3x_4 + \dots,$$

hence Q is nondegenerate. We shall write $\mathrm{O}_{2m}(K)$ instead of $\mathrm{O}(Q)$. If we take $g = (w_1\ w_2\ \dots\ w_{2m})$ from $M_{2m}(K)$, then the condition for g to be in $G = \mathrm{O}_{2m}(K)$, i.e., $Q(gx) = Q(x)$ for every x in $X = K^{2m}$, becomes $Q(w_i) = 0$ for every i, $Q(w_{2i-1}, w_{2i}) = 1$ for $1 \le i \le m$, and $Q(w_i, w_j) = 0$ for all other $i < j$. If we denote by S the set of all (x, y) in $X \times X$ satisfying $Q(x) = Q(y) = 0,\ Q(x, y) = 1$, then by Theorems 9.1.1, 9.1.2 we see that G acts transitively on S and the fixer H in G of (e_1, e_2) in S consists of all g above with $w_1 = e_1,\ w_2 = e_2$. In fact, if we denote the 2×2, $2 \times (2m-2)$, $(2m-2) \times 2$, $(2m-2) \times (2m-2)$ entry matrices of g by g_{11}, g_{12}, g_{21}, g_{22}, then g is in H if and only if $g_{11} = 1_2$, $g_{12} = 0$, $g_{21} = 0$, and g_{22} is in $\mathrm{O}_{2m-2}(K)$. Furthermore, x for (x, y) in S is free in $Q^{-1}(0)\backslash\{0\}$ and (e_1, y) is in S if and only if $y_2 = 1$, $y_1 + y_3y_4 + \dots + y_{2m-1}y_{2m} = 0$. Therefore, if $K = \mathbb{F}_q$, then by using Theorem 9.2.1 we get

$$\mathrm{card}(S) = q^{2m-2}(\mathrm{card}(Q^{-1}(0)) - 1) = q^{4m-3}[m][m-1]_+,$$

hence

$$\mathrm{card}(\mathrm{O}_{2m}(K)) = q^{4m-3}[m][m-1]_+ \cdot \mathrm{card}(\mathrm{O}_{2m-2}(K))$$

for $m > 1$ and $\mathrm{card}(\mathrm{O}_2(K)) = 2q[1]$ for $m = 1$. This implies

$$\mathrm{card}(\mathrm{O}_{2m}(K)) = 2q^{m(2m-1)}[m] \cdot \prod_{1\le i<m} [2i].$$

Still in the case where $X = K^{2m}$ with K arbitrary for a moment, if there exists a separable quadratic extension L of K generated by a zero ξ of $t^2 - at + b$ for a, b in K, we put

$$Q(x) = \sum_{1\le i<m} x_{2i-1}x_{2i} + (x_{2m-1}^2 + ax_{2m-1}x_{2m} + bx_{2m}^2)$$

and write $\mathrm{O}'_{2m}(K)$ instead of $\mathrm{O}(Q)$. If we take $g = (w_1\ w_2\ \dots\ w_{2m})$ from $M_{2m}(K)$, then the condition for g to be in $G = \mathrm{O}'_{2m}(K)$ becomes $Q(w_i) = 0$ except for $Q(w_{2m-1}) = 1$, $Q(w_{2m}) = b$, $Q(w_{2i-1}, w_{2i}) = 1$ except for $Q(w_{2m-1}, w_{2m}) = a$, and $Q(w_i, w_j) = 0$ for all other $i < j$. If $K = \mathbb{F}_q$, hence $L = \mathbb{F}_{q^2}$, and if $m > 1$, then exactly in the same way as in the previous case but by using the formula in Theorem 9.2.1 for $\mathrm{card}(Q^{-1}(0))$ for the above Q this time we get

$$\mathrm{card}(\mathrm{O}'_{2m}(K)) = \mathrm{card}(S)\ \mathrm{card}(\mathrm{O}'_{2m-2}(K)), \qquad \mathrm{card}(S) = q^{4m-3}[m]_+[m-1].$$

In the case where $m = 1$, if we put $w_1 = {}^t(\alpha, \gamma)$, $w_2 = {}^t(\beta, \delta)$, and $N = N_{L/K}$, then the above condition becomes $N(\alpha+\gamma\xi) = 1$, $N(\beta+\delta\xi) = b$, and $N(\alpha+\gamma\xi, \beta+\delta\xi) = a$. Therefore, $\eta = (\beta+\delta\xi)(\alpha+\gamma\xi)^{-1}$ is also a zero of t^2-at+b, hence $\eta = \xi$ or $\eta = \xi^q$. The subgroup of $\mathrm{O}'_2(K)$ defined by $\eta = \xi$ is isomorphic to $\mathrm{Ker}(N)$ as $g \mapsto \alpha + \gamma\xi$ and $\mathrm{O}'_2(K)$ has a coset by that subgroup represented by g with $\alpha = 1$, $\beta = a$, $\gamma = 0$, $\delta = -1$. In particular, $\mathrm{card}(\mathrm{O}'_2(K)) = 2q[1]_+$. Therefore, we get

$$\mathrm{card}(\mathrm{O}'_{2m}(K)) = 2q^{m(2m-1)}[m]_+ \cdot \prod_{1\le i<m} [2i].$$

In the case where $X = K^{2m+1}$, since the anisotropic kernel is one-dimensional over a finite field, we may assume that

$$Q(x) = \sum_{1\le i\le m} x_{2i-1}x_{2i} + ax_0^2$$

for some a in $K^\times$. Since $\mathrm{O}(Q)$ does not change even if we multiply any element of $K^\times$ to Q, we may further assume that $a = 1$. We shall write $\mathrm{O}_{2m+1}(K)$ instead of $\mathrm{O}(Q)$. Then if $K = \mathbb{F}_q$, by the same argument as before, we get

$$\mathrm{card}(\mathrm{O}_{2m+1}(K)) = \mathrm{card}(S)\mathrm{card}(\mathrm{O}_{2m-1}(K)), \qquad \mathrm{card}(S) = q^{4m-1}[2m]$$

with $\mathrm{card}(\mathrm{O}_1(K)) = 1$ or 2 according as q is even or odd. This implies

$$\mathrm{card}(\mathrm{O}_{2m+1}(K)) = 2q^{m(2m+1)} \cdot \prod_{1\le i\le m} [2i]$$

with the factor 2 above replaced by 1 if q is even.

There is one more type of classical group. A K-valued K-bilinear function A on $X \times X$ satisfying $A(x, x) = 0$ for every x in X is called an *alternating form* on X. We in fact have

$$A(x, y) + A(y, x) = A(x + y, x + y) - A(x, x) - A(y, y) = 0$$

for every x, y in X. If Y is a subspace of X, then clearly $A|(Y \times Y)$ is an alternating form on Y. If S is any subset of X, we define $S^\perp$ as the subspace of X of all x satisfying $A(x, y) = 0$ for every y in S. The alternating form A is called *nondegenerate* if $X^\perp = 0$. If we denote by J_1 the 2×2 matrix with $0, 1, -1, 0$ as its entries and by J_m the $2m \times 2m$ matrix with J_1 on the diagonal and with 0 as all

other 2×2 entry matrices, then $A(x,y) = {}^t x J_m y$ defines a nondegenerate alternating form on $X = K^{2m}$. We shall show that if A is any nondegenerate alternating form on a vector space X over K, then X has a K-basis $\{w_1, w_2, \dots, w_{2m}\}$, hence $\dim_K(X) = 2m$, satisfying $A(w_{2i-1}, w_{2i}) = 1$ for $1 \le i \le m$ and $A(w_i, w_j) = 0$ for all other $i < j$. That will imply

$$A\Big(\sum_{1\le i\le 2m} x_i w_i, \sum_{1\le i\le 2m} y_i w_i\Big) = {}^t x J_m y$$

for every x, y in K^{2m}. We take w_1 arbitrarily from $X\backslash\{0\}$. The nondegeneracy of A implies that the K-linear map from X to K defined by $y \mapsto A(w_1, y)$ is surjective, hence $A(w_1, w_2) = 1$ for some w_2 in X. If we put $X' = \langle w_1, w_2\rangle^\perp$, then X becomes the orthogonal direct sum of $\langle w_1, w_2\rangle$ and X'. In fact, every x in X can be written uniquely as

$$x = A(x, w_2)w_1 - A(x, w_1)w_2 + x'$$

with x' in X'. We observe that if $X' \ne 0$, then $A' = A|(X' \times X')$ is nondegenerate, hence we can apply the same argument to A'. We have only to repeat this process. We introduce, for our later use, the subspace $\mathrm{Alt}_n(K)$ of $M_n(K)$ consisting of all a such that $A(x,y) = {}^t x a y$ becomes an alternating form on K^n. If we denote the (i,j)-entry of a by a_{ij}, then this means $a_{ii} = 0$ for $1 \le i \le n$ and $a_{ij} + a_{ji} = 0$ for $1 \le i < j \le n$. Similarly we denote by $\mathrm{Sym}_n(K)$ the subspace of $M_n(K)$ consisting of all a such that ${}^t a = a$, i.e., $a_{ij} = a_{ji}$ for all i, j.

We now take a nondegenerate alternating form A on X and define the *symplectic group* $\mathrm{Sp}(A)$ of A as the group of all invertible K-linear maps g from X to itself satisfying $A(gx, gy) = A(x,y)$ for every x, y in K. We remark, similarly to the case of a reduced quadratic form, that the invertibility of g is a consequence of $A(gx, gy) = A(x,y)$ for every x, y in X. At any rate if $A(x,y) = {}^t x J_m y$ for $X = K^{2m}$, we shall write $\mathrm{Sp}_{2m}(K)$ instead of $\mathrm{Sp}(A)$; it consists of all g in $M_{2n}(K)$ satisfying ${}^t g J_m g = J_m$. By what we have shown $\mathrm{Sp}(A)$ is isomorphic to $\mathrm{Sp}_{2m}(K)$ if $\dim_K(X) = 2m$. Furthermore, if we denote by S the set of all (x,y) in $K^{2m} \times K^{2m}$ satisfying $A(x,y) = {}^t x J_m y = 1$, then the above observation shows that (x,y) can be considered as the first two columns of an element of $\mathrm{Sp}_{2m}(K)$, hence $G = \mathrm{Sp}_{2m}(K)$ acts transitively on S. Furthermore, the fixer H in G of (e_1, e_2) in S is isomorphic to $\mathrm{Sp}_{2m-2}(K)$. Since x for (x,y) in S is arbitrary in $K^{2m}\backslash\{0\}$ and (e_1, y) is in S if and only if $y_2 = 1$, if $K = \mathbb{F}_q$, then we get

$$\mathrm{card}(\mathrm{Sp}_{2m}(K)) = \mathrm{card}(S)\mathrm{card}(\mathrm{Sp}_{2m-2}(K)), \qquad \mathrm{card}(S) = q^{4m-1}[2m],$$

hence

$$\mathrm{card}(\mathrm{Sp}_{2m}(K)) = q^{m(2m+1)} \cdot \prod_{1\le i\le m} [2i].$$

The above computation shows that if q is even in $K = \mathbb{F}_q$, then $\mathrm{Sp}_{2m}(K)$ and $\mathrm{O}_{2m+1}(K)$ have the same order, hence there exists a bijection from $\mathrm{Sp}_{2m}(K)$ to $\mathrm{O}_{2m+1}(K)$. Actually, they are isomorphic for any perfect field K with $\mathrm{char}(K) = 2$. The proof of this remarkable fact is simple and it is as follows. We change our notation and put

$$Q(x) = x_0^2 + {}^t x' x''$$

for $x' = {}^t(x_1 \ \dots \ x_m)$, $x'' = {}^t(x_{m+1} \ \dots \ x_{2m})$. Then $\mathrm{O}_{2m+1}(K)$ is isomorphic to $\mathrm{O}(Q)$. If for similarly defined y', y'' we put

$$A(x,y) = {}^t x'y'' - {}^t x''y',$$

then $\mathrm{Sp}_{2m}(K)$ is isomorphic to $\mathrm{Sp}(A)$. If we denote the four $m \times m$ entry matrices of any g in $M_{2m}(K)$ by $a,\ b,\ c,\ d$, then g is in $\mathrm{Sp}(A)$ if and only if

$${}^t ac = {}^t ca, \qquad {}^t bd = {}^t db, \qquad {}^t ad - {}^t cb = 1_m.$$

The field K is arbitrary so far. If now K is a perfect field with $\mathrm{char}(K) = 2$, we define two row vectors $u = (u_1 \ \dots \ u_m)$, $v = (v_1 \ \dots \ v_m)$ by the condition that u_i^2, v_i^2 are respectively the i-th diagonal entries of ${}^t ac$, ${}^t bd$ for $1 \le i \le m$. Then we can easily verify that the correspondence

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \ \mapsto \ \begin{pmatrix} 1 & u & v \\ 0 & a & b \\ 0 & c & d \end{pmatrix}$$

gives an isomorphism from $\mathrm{Sp}(A)$ to $\mathrm{O}(Q)$.

Finally, there is a twisted form of $\mathrm{GL}_n(K)$ for $K = \mathbb{F}_q$, i.e. the *unitary group* $U_n(L)$ where $L = \mathbb{F}_{q^2}$. If we denote the automorphism $x \mapsto x^q$ of L over K applied to all entries of g by $g \mapsto g'$, then $U_n(L)$ consists of all g in $M_n(L)$ satisfying ${}^t gg' = 1_n$. We can compute the order of $U_n(L)$ similarly as in the other cases and we get

$$\mathrm{card}(U_n(L)) = q^{n^2} \cdot \prod_{1 \le i \le n} (1 - (-q)^{-i}).$$

We shall not use this fact in our later examples.

9.4 Composition and Jordan algebras

We shall explain some K-algebras. The explanation will be self-contained except for the fact that we do not prove classification theorems. This does not create any gap because our purpose is simply to give a good perspective to the list of $f(x)$ for which we shall compute $Z(s)$.

We recall that a K-algebra A for any field K is a vector space over K in which a K-bilinear multiplication $(a,b) \to ab$ is defined; we shall not assume that $(ab)c = a(bc)$. A K-algebra $A \neq 0$ is called *simple* if A and 0 are the only two-sided ideals of A. We shall assume that $\dim_K(A)$ is finite. We say that C is a *composition algebra* over K if firstly, C is a K-algebra with the unit element $1 \neq 0$, i.e., $C \neq 0$; secondly, C is equipped with a reduced quadratic form n; and thirdly,

$$n(ab) = n(a)n(b) \tag{1}$$

for every a, b in C. We call C a *quaternion* (resp. an *octonion*) *algebra* over K if $\dim_K(C) = 4$ (resp. $\dim_K(C) = 8$). We observe that (1) implies $n(1) = n(1)^2$,

hence $n(1) = 1$ for otherwise $n(1) = 0$. But then $n(a) = n(a1) = n(a)n(1) = 0$, hence $n(a, b) = 0$ for all a, b in C, and hence $C = C^{\perp} \cap n^{-1}(0) = 0$, a contradiction. We polarize (1) in b, i.e., we replace b by $b_1 + b_2$, then by b_1, b_2 and subtract the second from the first. In that way we get

$$n(ab_1, ab_2) = n(a)n(b_1, b_2).$$

If we apply a polarization to the above in a, we get

$$n(a_1b_1, a_2b_2) + n(a_2b_1, a_1b_2) = n(a_1, a_2)n(b_1, b_2)$$

for all a_1, a_2, b_1, b_2 in C. If we put

$$t(a) = n(a, 1), \qquad a' = -a + t(a)1,$$

then $1' = 1$ and $n(a') = n(a)$, hence by polarization $n(a', b') = n(a, b)$. Furthermore, by replacing a_1, a_2, b_1, b_2 respectively by $a, 1, b, c$ and also by $a, c, b, 1$ we get

$$n(ab, c) = n(b, a'c) = n(a, cb'). \tag{2}$$

We rewrite the first polarized form of (1) as $n(ab, ac) = n(a)n(b, c)$. Since $n(ab, ac) = n(a'(ab), c)$ by (2), if we put $d = a'(ab) - n(a)b$, then $n(d, c) = 0$ for all c in C. By using (1), (2), and $n(a') = n(a)$ we also have $n(d) = 0$. Hence d is in $C^{\perp} \cap n^{-1}(0) = 0$, i.e.,

$$a'(ab) = n(a)b. \tag{3}$$

If we put $b = c = 1$ in (2), we get $t(a') = t(a)$, hence $(a')' = a$. If we put $b = 1$ in (3), we get

$$a^2 - t(a)a + n(a)1 = 0,$$

hence by polarization $ab + ba - t(a)b - t(b)a + n(a, b)1 = 0$. On the other hand by (2) we get $n(a, b) = t(ab') = -t(ab) + t(a)t(b)$. By putting these together we get $b'a' - (ab)' = 0$. Therefore, the K-linear map $a \mapsto a'$ is an *involution* of C in the sense that $(ab)' = b'a'$ and $(a')' = a$ for every a, b in C. For our later use, we also remark that

$$t((ab)c) = t(a(bc)),$$

hence we can simply write it as $t(abc)$. In fact, we have

$$t((ab)c) = n(ab, c') = n(b'a', c) = n(a', bc) = t(a(bc));$$

we have used (2), $n(a', b') = n(a, b)$, and (2) again. We similarly have

$$t(ab) = t(ba).$$

In fact, $t(ab) = n(a, 1b') = n(a, b'1) = t(ba)$. Therefore, we get

$$t(abc) = t(bca) = t(cab).$$

We now take a composition algebra C_0 equipped with a nondegenerate quadratic form n_0, put $C = C_0 + C_0$, a direct sum, $n(a_1, a_2) = n_0(a_1) + n_0(a_2)$, and define a multiplication in C as

$$(a_1, a_2)(b_1, b_2) = (a_1 b_1 - b_2' a_2, b_2 a_1 + a_2 b_1'). \tag{4}$$

Then by using (2) in C_0, we get

$$n(ab) - n(a)n(b) = n_0\big((b_2 a_1)b_1 - b_2(a_1 b_1), a_2\big),$$

in which $a = (a_1, a_2),\ b = (b_1, b_2)$. Therefore, C becomes a composition algebra if and only if C_0 is associative. We shall show in the case where C_0 is associative that C itself is associative if and only if C_0 is commutative. Since the if-part is straightforward, we shall prove the only-if part. If we take $a = (a_1, 0),\ b = (b_1, 0),\ c = (1, 1)$, where a_1, b_1 are arbitrary in C_0, then

$$(ab)c - a(bc) = (a_1 b_1, a_1 b_1) - (a_1 b_1, b_1 a_1),$$

hence $(ab)c = a(bc)$ implies $a_1 b_1 = b_1 a_1$.

We have explained the above partly to give some idea about C but mainly to simplify the subsequent verifications. Examples of C are as follows:

(C1) $C = K, \quad n(a) = a^2$.

(C2) $C = K + K, \quad (a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2), \quad n(a_1, a_2) = a_1 a_2$.

(C3) $C = M_2(K)$, with the matrix-multiplication, $n(a) = \det(a)$.

(C4) $C = C_0 + C_0$, as in (4) for $C_0 = C$ in (C3).

The fact that we have a composition algebra in (C1), (C2), (C3) is clear. Therefore, by the above general observation we also have a composition algebra in (C4). Furthermore, (C3) is not commutative, hence (C4) is not associative, and hence the process $C_0 \to C$ applied to (C4) will not produce a composition algebra. We also remark that the involution in each case can easily be made explicit and it is as follows:

$$a' = a, \qquad (a_1, a_2)' = (a_2, a_1), \qquad a' = J_1 {}^t a J_1^{-1}, \qquad (a_1, a_2)' = (a_1', -a_2),$$

in which J_1 is as in section 9.3, i.e., the 2×2 matrix with $0,\ 1,\ -1,\ 0$ as its entries. The fact is that all composition algebras over K can be determined and if K is algebraically closed, then C is isomorphic to one of the above. We refer to N. Jacobson [32] for the details (in the case where $\mathrm{char}(K) \neq 2$).

We shall introduce another class of algebras. We say that A is a *Jordan algebra* over K if A is a commutative K-algebra and

$$(ab)a^2 = a(ba^2)$$

for every a, b in A. If we denote by $\theta(a)$ the multiplication by a in A, then the above *Jordan identity* becomes $\theta(a^2)\theta(a) = \theta(a)\theta(a^2)$. At any rate, any subalgebra of a Jordan algebra is clearly a Jordan algebra. In the following, we shall assume that $\mathrm{char}(K) \neq 2$. If for any K-algebra A we define a new multiplication as

$$a \circ b = (1/2)(ab + ba),$$

then we have $a \circ b = b \circ a$ and $a \circ a = a^2$. If A has an involution $a \mapsto a'$ and B is the subspace consisting of symmetric elements $a' = a$, then B becomes a subalgebra of A under the new multiplication. If C is any K-algebra with involution and $M_n(C)$ is the K-algebra of $n \times n$ matrices with entries in C and with the matrix-multiplication, then $a \mapsto {}^t a'$, where $({}^t a')_{ij} = a'_{ji}$ for all i, j, defines an involution of $M_n(C)$. Therefore, the subspace $H_n(C)$ consisting of hermitian matrices ${}^t a' = a$ forms a subalgebra of $M_n(C)$ under the new multiplication. Suppose now that A is associative. Then A with the new multiplication becomes a Jordan algebra. In fact,

$$(a \circ b) \circ a^2 = (1/4)(a^3 b + a^2 b a + a b a^2 + b a^3) = a \circ (b \circ a^2).$$

Therefore, if C is an associative composition algebra over K so that $M_n(C)$ is also associative, then $H_n(C)$ with the new multiplication is a Jordan algebra. We shall explain further examples of Jordan algebras. We keep in mind that since $\mathrm{char}(K) \neq 2$, an element a of C is symmetric, i.e., $a' = a$, if and only if a is in $K = K1$.

We take a quadratic form Q on a vector space X over K, put

$$A = Ke_1 + Ke_2 + X,$$

and define a multiplication in A as

$$(\alpha_1 e_1 + \alpha_2 e_2 + x)(\beta_1 e_1 + \beta_2 e_2 + y) = \gamma_1 e_1 + \gamma_2 e_2 + z,$$

where $\gamma_i = \alpha_i \beta_i + (1/2) Q(x, y)$ for $i = 1, 2$ and $z = (1/2)((\alpha_1 + \alpha_2) y + (\beta_1 + \beta_2) x)$. We shall show that A is a Jordan algebra. Clearly A is a commutative K-algebra. If we put $a = \alpha_1 e_1 + \alpha_2 e_2 + x$ and $e = e_1 + e_2$, then $ea = a$ and further

$$a^2 - (\alpha_1 + \alpha_2) a + (\alpha_1 \alpha_2 - Q(x)) e = 0.$$

Therefore, if we put $\tau = \alpha_1 + \alpha_2,\ \nu = \alpha_1 \alpha_2 - Q(x)$, then

$$(ab) a^2 = \tau (ab) a - \nu a b = \tau a (ba) - \nu a b = a (b a^2).$$

If now C is any composition algebra and $\alpha_1,\ \alpha_2,\ x$ are the $(1,1),\ (2,2),\ (1,2)$ entries of a in $H_2(C)$ then $a \mapsto \alpha_1 e_1 + \alpha_2 e_2 + x$ gives an isomorphism from $H_2(C)$ to $A = Ke_1 + Ke_2 + C$ where $Q(x) = n(x)$. Therefore, $H_2(C)$ is a Jordan algebra. We shall show that $H_3(C)$ is also a Jordan algebra.

We take a, b, c from $H_3(C)$ and keep in mind that $a'_{ij} = a_{ji}$, etc.; we put $a \circ a \circ a = a \circ (a \circ a),\ e = 1_3$. We introduce the following quadratic and cubic forms on A:

$$\begin{aligned} Q(a) &= (1/2)(a_{11}^2 + a_{22}^2 + a_{33}^2) + n(a_{23}) + n(a_{31}) + n(a_{12}), \\ \det(a) &= a_{11} a_{22} a_{33} + t(a_{23} a_{31} a_{12}) - a_{11} n(a_{23}) - a_{22} n(a_{31}) - a_{33} n(a_{12}). \end{aligned}$$

Since $t(a_{ij} a_{jk} a_{ki})$ is invariant under even permutations of a_{ij}, a_{jk}, a_{ki} and is equal to $t((a_{ij} a_{jk} a_{ki})') = t(a_{ik} a_{kj} a_{ji})$, we see that $t(a_{ij} a_{jk} a_{ki}) = t(a_{23} a_{31} a_{12})$ for all distinct i, j, k. Since

$$Q(a, b) = \sum_i a_{ii} b_{ii} + \sum_{i<j} n(a_{ij}, b_{ij}),$$

we see that Q is nondegenerate. Furthermore,

$$(a \circ b)_{ii} = a_{ii}b_{ii} + (1/2)\{n(a_{ij}, b_{ij}) + n(a_{ik}, b_{ik})\},$$
$$(a \circ b)_{ij} = (1/2)\{(a_{ii} + a_{jj})b_{ij} + (b_{ii} + b_{jj})a_{ij} + a_{ik}b_{kj} + b_{ik}a_{kj}\},$$

hence

$$Q(a \circ b, c) = Q(a, b \circ c).$$

We shall use this fact very often. If we replace b above by a and $a \circ a$, then we get

$$(a \circ a)_{ii} = a_{ii}^2 + n(a_{ij}) + n(a_{ik}), \qquad (a \circ a)_{ij} = (a_{ii} + a_{jj})a_{ij} + a_{ik}a_{kj};$$
$$(a \circ a \circ a)_{ii} = a_{ii}^3 + (2a_{ii} + a_{jj})n(a_{ij}) + (2a_{ii} + a_{kk})n(a_{ik}) + t(a_{23}a_{31}a_{12}),$$
$$(a \circ a \circ a)_{ij} = (a_{ii}^2 + a_{ii}a_{jj} + a_{jj}^2 + n(a_{23}) + n(a_{31}) + n(a_{12}))a_{ij} + Q(a, e)a_{ik}a_{kj}.$$

By using these we can easily verify that a satisfies the following basic cubic equation

$$a \circ a \circ a - Q(a, e)a \circ a + Q_1(a)a - \det(a)e = 0,$$

in which

$$Q_1(a) = (1/2)Q(a, e)^2 - Q(a).$$

If we take a variable t and define the first polar $\det_1(a, b)$ of $\det(a)$ as

$$\det(a + tb) = \det(a) + \det_1(a, b)t + \dots,$$

then by using the definition we get

$$\det_1(a, b) = Q(a^{\#}, b), \qquad a^{\#} = a \circ a - Q(a, e)a + Q_1(a)e.$$

Similarly, by taking the first polar of the above cubic equation for a we get

$$(a \circ a) \circ b + 2a \circ (a \circ b) - Q(b, e)a \circ a - 2Q(a, e)a \circ b$$
$$+ Q_1(a, b)a + Q_1(a)b - \det_1(a, b)e = 0,$$

in which $Q_1(a, b) = Q(a, e)Q(b, e) - Q(a, b)$. If we denote the LHS of the above equation by $L(a, b)$, then we get $a \circ L(a, b) - L(a, a \circ b) = 0$ because both terms are 0. By using the cubic equation for a and the above expression for $Q_1(a, b)$, we can rewrite this equation as

$$a \circ (b \circ (a \circ a)) - (a \circ b) \circ (a \circ a) = \det_1(a, b)a - \det_1(a, a \circ b)e$$
$$+ Q_1(a, a \circ b)a - Q_1(a)Q(b, e)a + \det(a)Q(b, e)e.$$

If we replace $\det_1(a, b)$ by $Q(a^{\#}, b)$ with $a^{\#}$ as above and use the fact that $a \circ a^{\#} = \det(a)e$, then we get

$$\text{RHS} = (Q_1(a, a \circ b) - Q(a, e)Q(a \circ b, e) + Q(a, a \circ b))a = 0.$$

We have thus shown that $H_3(C)$ is a Jordan algebra for any composition algebra C. If we assume that $\mathrm{char}(K) \neq 3$, in addition to $\mathrm{char}(K) \neq 2$, then $Q|Ke$ is nondegenerate, hence $A = Ke \oplus (Ke)^{\perp}$. The proof can be slightly shortened by using this fact. At any rate, the fact is that if K is algebraically closed and $\mathrm{char}(K) \neq 2$, then every simple Jordan algebra over K is isomorphic to $H_n(C)$ for some $n \geq 1$ for the C in (C1), (C2), (C3), $Ke_1 + Ke_2 + X$ with a nondegenerate quadratic form Q on X, or $H_3(C)$ for the C in (C4). We again refer the details to Jacobson [32]. We might mention, for a comparison, that if A is a simple associative algebra over any algebraically closed field K, then by a special case of Wedderburn's theorem A is isomorphic to $M_n(K)$ for some $n \geq 1$.

9.5 Norm forms and Freudenthal quartics

If C is any K-algebra and a is an element of $M_n(C)$ with a_{ij} as its (i,j)-entry, then we put $e = 1_n$ and

$$\mathrm{tr}(a) = a_{11} + a_{22} + \ldots + a_{nn}.$$

We take a Jordan algebra $A = H_n(C)$ and define a^k inductively on $k > 0$ in $\mathbb{N}$ as $a^k = a \circ a^{k-1}$ with the understanding that $a^0 = e$. We take as C one of the (C1), (C2), (C3), (C4) in section 9.4 and show that a satisfies an equation of the form

$$a^n - \mathrm{tr}(a)a^{n-1} + \ldots + (-1)^n \det(a)e = 0,$$

in which $\det(a)$ is a homogeneous polynomial of degree n in the entries of a. Since the above equation is not unique as stated, we shall make $\det(a)$ explicit in each case and call it the *norm form* of A. Since we are familiar with quadratic forms, we shall be interested in the case where $n > 2$.

If a is any element of $M_n(K)$, where K is an arbitrary field, we denote by $\det(a)$ the usual determinant of a. If $\phi(t)$ is the characteristic function of a, i.e., if

$$\phi(t) = \det(te - a) = t^n - \mathrm{tr}(a)t^{n-1} + \ldots + (-1)^n \det(a),$$

then by Cayley's theorem we will have $\phi(a) = 0$. We might recall its proof: If we put $(te - a)^{\#} = \phi(t)(te - a)^{-1}$ and write

$$\phi(t) = \sum_{0 \leq i \leq n} \alpha_i t^i, \qquad (te - a)^{\#} = \sum_{0 \leq i \leq n} b_i t^i$$

with α_i in K and b_i in $M_n(K)$, then $\alpha_i e = b_{i-1} - ab_i$ for $0 \leq i \leq n$, in which $b_{-1} = b_n = 0$. This implies

$$\phi(a) = \sum_{0 \leq i \leq n} \alpha_i a^i = \sum_{0 \leq i \leq n} (a^i b_{i-1} - a^{i+1} b_i) = 0.$$

We shall now assume that $\mathrm{char}(K) \neq 2$. If C is as in (C1), hence $C = K$, then $H_n(C) = \mathrm{Sym}_n(K)$, the subspace of $M_n(K)$ of symmetric matrices. Therefore, we can take the determinant of a as $\det(a)$. If C is as in (C2), hence $C = K + K$,

then $H_n(C)$ consists of $a = (x, {}^t x)$ for all x in $M_n(K)$. Furthermore, we see that a satisfies the same equation in $H_n(C)$ as x in $M_n(K)$. Therefore, we can take the determinant of x as $\det(a)$. If C is as in (C3), hence $C = M_2(K)$, then $H_n(C)$ consists of all a in $M_{2n}(K)$ satisfying $J_n {}^t a J_n^{-1} = a$, i.e., such that $x = aJ_n$ is in $\mathrm{Alt}_{2n}(K)$, in which J_n and $\mathrm{Alt}_{2n}(K)$ are as in section 9.3. If x is in $\mathrm{Alt}_{2n}(K)$, i.e. an alternating matrix in $M_{2n}(K)$, we define its *Pfaffian* $\mathrm{Pf}(x)$ as

$$\mathrm{Pf}(x) = \sum_{\sigma}{}' \varepsilon(\sigma) x_{\sigma(1),\sigma(2)} \cdots x_{\sigma(2n-1),\sigma(2n)},$$

in which $\varepsilon(\sigma) = \pm 1$ according as the permutation σ of $\{1,\ 2,\ \ldots\ ,\ 2n\}$ is even or odd and $\sum'$ indicates the restriction $\sigma(1) < \sigma(2), \ldots, \sigma(2n-1) < \sigma(2n)$, $\sigma(1) < \sigma(3) < \ldots < \sigma(2n-1)$; the number of terms is $(2n)!/2^n n!$. We observe that if we put

$$\psi(t) = \mathrm{Pf}(tJ_n - x) = t^n - \tau t^{n-1} + \ldots + (-1)^n \mathrm{Pf}(x),$$

then we have

$$\tau = x_{12} + x_{34} + \ldots + x_{2n-1,2n} = \mathrm{tr}(a),$$

in which $\mathrm{tr}(a)$ is defined in $H_n(C)$. Furthermore, a similar argument as in the proof of Cayley's theorem shows that $\psi(a) = 0$. Therefore, we can take $\mathrm{Pf}(x) = \mathrm{Pf}(aJ_n)$ as $\det(a)$. If "det" means the usual determinant, then we have found that the norm form in each case has the following meaning: $\det(x)$ for x in $\mathrm{Sym}_n(K)$, $\det(x)$ for x in $M_n(K)$, the Pfaffian $\mathrm{Pf}(x)$ for x in $\mathrm{Alt}_{2n}(K)$.

Finally, in the case where C is as in (C4), we have only to consider $H_n(C)$ for $n \leq 3$. If $n = 2$, then

$$\det(a) = a_{11}a_{22} - n(a_{12}),$$

which is a hyperbolic form in 10 variables. If $n = 3$, then

$$\det(a) = a_{11}a_{22}a_{33} + t(a_{23}a_{31}a_{12}) - a_{11}n(a_{23}) - a_{22}n(a_{31}) - a_{33}n(a_{12}).$$

We shall obtain a classical expression for this cubic form. If we write an arbitrary element a of $M_3(C)$ as $a = (a_1, a_2)$ with a_1, a_2 in $M_6(K)$, then a is in $H_3(C)$ if and only if a_1 is in $H_3(M_2(K))$ and the entries of a_2 satisfy $(a_2)_{ii} = 0$ for $1 \leq i \leq 3$, $(a_2)_{ij} = -(a_2)_{ji}$ for $1 \leq i < j \leq 3$. Therefore, by what we have shown above $y = a_1 J_3$ is in $\mathrm{Alt}_6(K)$. We shall denote the (i,j)-entry of y by y_{ij}; also we put

$$\begin{pmatrix} (a_2)_{23} & (a_2)_{31} & (a_2)_{12} \end{pmatrix} = \begin{pmatrix} z_{11} & z_{12} & \ldots & z_{16} \\ & & & \\ z_{21} & z_{22} & \ldots & z_{26} \end{pmatrix}$$

and $w_{ij} = z_{1i}z_{2j} - z_{1j}z_{2i}$ for $1 \leq i,\ j \leq 6$. Then in $\det(a)$ those terms which are free from z_{ij} will give $\mathrm{Pf}(y)$. Furthermore, we can easily verify that

$$\det(a) - \mathrm{Pf}(y) = -\sum_{i<j} y_{ij} w_{ij} = -{}^t z_1 y z_2,$$

in which $z_i = {}^t(z_{i1} \ldots z_{i6})$ for $i = 1, 2$.

We shall next introduce Freudenthal quartics. We take $A = H_3(C)$ and put $X = K^2 + A^2$. An element x of X is of the form $(a_0, b_0; a, b)$ for some a_0, b_0 in K and a, b in A. We observe that

$$\dim_K(X) = 6 \cdot \dim_K(C) + 8 = 14,\ 20,\ 32,\ 56$$

for $\dim_K(C) = 1, 2, 4, 8$. In the notation of section 9.4 we define the *Freudenthal quartic* on X after H. Freudenthal [14] as

$$f(x) = (a_0 b_0 - Q(a,b))^2 - 4(a_0 \det(b) + b_0 \det(a) + Q(a^\#, b^\#)).$$

It appeared in his earlier paper in the following form:

$$J(y,z) = \mathrm{Pf}(y) + \mathrm{Pf}(z) - (1/4)\mathrm{tr}((yz)^2) + ((1/4)\mathrm{tr}(yz))^2,$$

in which y, z are in $\mathrm{Alt}_8(K)$. Actually, the above cubic form $\mathrm{Pf}(y) - {}^t z_1 y z_2$ and $J(y,z)$ are in E. Cartan's thesis of 1894 but with some incorrectness about $J(y,z)$, which was corrected as above by Freudenthal. Furthermore, he and T. A. Springer developed the theory of Jordan algebras in connection with exceptional simple groups. At any rate, if $C = M_2(K) + M_2(K)$, then there exists a K-linear map $X \to \mathrm{Alt}_8(K)^2$ under which $f(x)$ becomes $-4J(y,z)$. We might give one such map. We write $a = (a_1, a_2)$, $b = (b_1, b_2)$ as before and define y', z' in $\mathrm{Alt}_6(K)$ with their (i,j)-entries y_{ij}, z_{ij} for $1 \le i, j \le 6$ as $y' = a_1 J_3$, $z' = J_3 b_1$. We next define y, z in $\mathrm{Alt}_8(K)$ with their additional (i,j)-entries y_{ij}, z_{ij} for $i, j = 7,\ 8$ as

$$\begin{pmatrix} y_{17} & y_{27} & \cdots & y_{67} \\ y_{18} & y_{28} & \cdots & y_{68} \end{pmatrix} = J_1\big((b_2)_{23}\ (b_2)_{31}\ (b_2)_{12}\big)J_3, \qquad y_{78} = b_0,$$

$$\begin{pmatrix} z_{17} & z_{27} & \cdots & z_{67} \\ z_{18} & z_{28} & \cdots & z_{68} \end{pmatrix} = \big((a_2)_{23}\ (a_2)_{31}\ (a_2)_{12}\big), \qquad z_{78} = a_0.$$

Then, after some lengthy computation, we can see that $f(x) = -4J(y,z)$. Since we shall not use this fact, the details will not be given.

In order to satisfactorily examine Freudenthal quartics in the four cases, we need to prove a large number of formulas in the theory of Jordan algebras. Instead, we shall explain only one case where such a preparation will not be necessary. In fact, we shall use the method we have used in [22], pp. 1021-1023 which depends only on the usual matrix computation.

We know that the action of $\mathrm{GL}_n(K)$ on K^n extends to $\bigwedge^p K^n$ for all p. In particular, for $p = 3$ we have

$$(g \cdot x)_{ijk} = \sum g_{ii'}\ g_{jj'}\ g_{kk'}\ x_{i'j'k'}$$

for every g in $\mathrm{GL}_n(K)$ with $g_{ii'}$ as its (i,i')-entry and for every $i,\ j,\ k$, in which the summation is for all i', j', k'. We observe that if $x \neq 0$, hence $x_{ijk} \neq 0$ for some $i < j < k$ and if g is the permutation-matrix representing $(1i)(2j)(3k)$, then $(g \cdot x)_{123} = x_{ijk} \neq 0$. We shall assume, from now on, that $n = 6$, hence $\dim_K(\bigwedge^3 K^n) = 20$,

and denote the 3×3 entry matrices of g at $(1,1),\ (1,2),\ (2,1),\ (2,2)$ respectively by $\alpha,\ \beta,\ \gamma,\ \delta$. We observe that if $x_{123} \neq 0$ in x, then there exists a unique g with $\alpha = \delta = 1_3,\ \beta = 0$, such that $(g \cdot x)_{ijk} = 0$ for all $i < j \leq 3 < k$ and the unique γ is given by

$$-x_{123}\gamma = (x_{23i}\ x_{31i}\ x_{12i})_{i=4,5,6};$$

we shall denote the RHS by a. In other words, a is the element of $M_3(K)$ with $(x_{23i}\ x_{31i}\ x_{12i})$ as its $(i-3)$-th row for $i = 4,\ 5,\ 6$. Similarly, if $x_{456} \neq 0$, there exists a unique g with $\alpha = \delta = 1_3,\ \gamma = 0$ such that $(g \cdot x)_{ijk} = 0$ for all $i \leq 3 < j < k$ and the unique β is given by

$$-x_{456}\beta = (x_{i56}\ x_{i64}\ x_{i45})_{i=1,2,3};$$

we shall denote the RHS by b. Finally, for an arbitrary x we put $a_0 = -x_{123}$, $b_0 = -x_{456}$ and use the notation $x = (a_0, b_0; a, b)$.

We now take x with $a_0 \neq 0$, denote by $g = g_0$ the element of $\mathrm{SL}_6(K)$ for which $\alpha = \delta = 1_3,\ \beta = 0,\ \gamma = a_0^{-1}a$ and put $g_0 \cdot x = x' = (a_0', b_0'; 0, b')$. If for any a in $M_3(K)$ we put $a^{\#} = \mathrm{Adj}(a)$ so that $aa^{\#} = \det(a)1_3$, then $a_0' = a_0$ and

$$\begin{aligned} b_0' &= b_0 - \mathrm{tr}(\gamma b) - \mathrm{tr}(a\gamma^{\#}) + \det(\gamma)a_0 \\ &= b_0 - a_0^{-1}\mathrm{tr}(ab) - 2a_0^{-2}\det(a), \\ (b')_{ij} &= b_{ij} + 2a_0^{-1}(a^{\#})_{ij} - a_0^{-1}(a^{\#})_{ij} \end{aligned}$$

for $1 \leq i,\ j \leq 3$, hence $b' = b + a_0^{-1}a^{\#}$. Furthermore, if we put

$$J = a_0' \det(b') - (1/4)(a_0'b_0')^2,$$

then by using the above expressions for a_0', b_0', b' and the general formulas

$$\begin{aligned} \det(a+b) &= \det(a) + \mathrm{tr}(a^{\#}b) + \mathrm{tr}(ab^{\#}) + \det(b), \\ \det(a^{\#}) &= \det(a)^2, \qquad (a^{\#})^{\#} = \det(a)a, \end{aligned}$$

we see that $-4J$ is equal to

$$f(x) = (a_0b_0 - \mathrm{tr}(ab))^2 - 4(a_0\det(b) + b_0\det(a) + \mathrm{tr}(a^{\#}b^{\#})).$$

This is the Freudenthal quartic for $C = K + K$. In order to proceed further we need the following lemma, the verification of which is straightforward.

Lemma 9.5.1 *Let L denote an arbitrary field and g any element of* $\mathrm{GL}_6(L)$ *with* 3×3 *entry matrices $\alpha,\ \beta,\ \gamma,\ \delta$. Then*

$$\begin{aligned} g \cdot (1,0;0,0) &= (\det(\alpha), \det(\gamma);\ -\gamma\alpha^{\#},\ -\alpha\gamma^{\#}), \\ g \cdot (0,1;0,0) &= (\det(\beta), \det(\delta);\ -\delta\beta^{\#},\ -\beta\delta^{\#}). \end{aligned}$$

We observe that if $p,\ q,\ p',\ q'$ are elements of $L^{\times}$ satisfying $pq = p'q'$, then we can find g in $\mathrm{SL}_6(L)$ satisfying $g \cdot (p,q;0,0) = (p',q';0,0)$. In fact, by Lemma 9.5.1 we have only to choose $\alpha,\ \delta$ satisfying $\det(\alpha) = p'/p$, $\det(\delta) = q'/q$ and put

$\beta = \gamma = 0$. We also observe that if q is in $L^\times$, we can find g in $\mathrm{SL}_6(L)$ satisfying $g \cdot (1, q; 0, 0) = (1, -q; 0, 0)$. In fact, by Lemma 9.5.1 we have only to choose β, γ satisfying $\det(\beta) = 1/q$, $\det(\gamma) = -q$ and put $\alpha = \delta = 0$. We shall show that if $J \neq 0$ in $x' = (a_0', b_0'; 0, b')$ above and $\theta = (-4J)^{1/2}$, then we can find g in $\mathrm{SL}_6(L)$ for $L = K(\theta)$ satisfying $g \cdot (1, \theta; 0, 0) = x'$. We shall, for the sake of simplicity, write a_0, etc. instead of a_0', etc. so that $x' = (a_0, b_0; 0, b)$ and

$$-4J = (a_0 b_0)^2 - 4a_0 \det(b) = \theta^2 \neq 0.$$

This implies $a_0 \neq 0$ and either $a_0 b_0 - \theta \neq 0$ or $a_0 b_0 + \theta \neq 0$. We have remarked that $(1, \theta; 0, 0)$ and $(1, -\theta; 0, 0)$ are in the same $\mathrm{SL}_6(L)$-orbit. Therefore, we may assume that

$$q = (1/2) a_0 (1 - \theta^{-1} a_0 b_0) \neq 0$$

and we put $p = \theta/q$. Also by another remark we have only to find g in $\mathrm{SL}_6(L)$ satisfying $g \cdot (p, q; 0, 0) = x'$. We just define g as

$$\alpha = -\theta^{-1} a_0 b, \qquad \beta = 1_3, \qquad \gamma = -a_0^{-1} q 1_3, \qquad \delta = \theta^{-2} a_0 p b^{\#}.$$

Then g has the required property. In fact, if we multiply $\theta^{-1} a_0 b$ to the second column of g and add to the first column, then the new first column will have 0, -1_3 as its entry matrices. Since the new matrix is clearly in $\mathrm{SL}_6(L)$, we see that g is in $\mathrm{SL}_6(L)$. The verification of $g \cdot (p, q; 0, 0) = (a_0, b_0; 0, b)$ by Lemma 9.5.1 is straightforward.

Lemma 9.5.2 *If g, q are respectively elements of $\mathrm{GL}_6(L)$, $L^\times$ for any field L and $g \cdot (1, q; 0, 0) = (1, q'; 0, 0)$, then $q' = \pm \det(g) q$.*

Proof. By Lemma 9.5.1 the condition on g becomes

$$(*) \qquad \det(\alpha) + q \det(\beta) = 1, \qquad \det(\gamma) + q \det(\delta) = q',$$
$$\gamma \alpha^{\#} + q \delta \beta^{\#} = 0, \qquad \alpha \gamma^{\#} + q \beta \delta^{\#} = 0.$$

Suppose first that $\det(\alpha) \neq 0$. Then the last two equations imply

$$\gamma = -q \delta \beta^{\#} (\alpha^{\#})^{-1}, \qquad (\det(\alpha) + q \det(\beta)) \beta \delta^{\#} = 0.$$

By the first equation in $(*)$, the second equation above becomes $\beta \delta^{\#} = 0$, hence the fourth equation in $(*)$ becomes $\alpha \gamma^{\#} = 0$, hence $\gamma^{\#} = 0$, and this implies $\det(\gamma) = 0$. Then the second equation in $(*)$ becomes $q \det(\delta) = q'$, hence $\det(\delta) \neq 0$. Then $\beta \delta^{\#} = 0$ above implies $\beta = 0$, hence $\det(\alpha) = 1$, $\gamma \alpha^{\#} = 0$, hence $\gamma = 0$, respectively by the first and the third equations in $(*)$. Therefore, we get $\det(g) = \det(\delta)$ and $q' = \det(g) q$. Suppose next that $\det(\alpha) = 0$, hence $\det(\beta) = 1/q$ by the first equation in $(*)$. Denote by g_0 any element of $\mathrm{SL}_6(L)$ with entry matrices α_0, β_0, γ_0, δ_0 satisfying $\alpha_0 = \delta_0 = 0$ and $\det(\beta_0) = -1/q, \det(\gamma_0) = q$ so that $g_0 \cdot (1, -q; 0, 0) = (1, q; 0, 0)$. Then the entry matrices of $g g_0$ are $\beta \gamma_0$, $\alpha \beta_0$, $\delta \gamma_0$, $\gamma \beta_0$, in which $\det(\beta \gamma_0) = 1$, and $g g_0 \cdot (1, -q; 0, 0) = (1, q'; 0, 0)$. Therefore, by what we have shown, we get $q' = -\det(g) q$.

We shall formulate an immediate consequence of what we have discussed so far as a proposition; further consequences will be used later to compute $Z(s)$ for $f(x)$.

Proposition 9.5.1 *Let K denote any field with char$(K) \neq 2$, identify $\bigwedge^3 K^6$ with $K^2 + M_3(K)^2$ under the K-linear bijection $x \mapsto (a_0, b_0; a, b)$, in which*

$$a_0 = -x_{123}, \qquad b_0 = -x_{456}, \qquad a = (x_{23i}, x_{31i}, x_{12i}), \qquad b = (x_{i56}, x_{i64}x_{i45})$$

respectively for $i = 4,\ 5,\ 6$ and $i = 1,\ 2,\ 3$, and put

$$f(x) = (a_0 b_0 - \mathrm{tr}(ab))^2 - 4(a_0 \det(b) + b_0 \det(a) + \mathrm{tr}(a^{\#} b^{\#})).$$

Then for every g in $\mathrm{GL}_6(K)$, we have

$$f(g \cdot x) = \det(g)^2 f(x);$$

if $f(x) \neq 0$ and $\theta = f(x)^{1/2}$, then there exists an element g of $\mathrm{SL}_6(K(\theta))$ satisfying $g \cdot x = (1, \theta; 0, 0)$; and if θ is in $L^{\times}$ for any field L, the fixer of $(1, \theta; 0, 0)$ in $\mathrm{SL}_6(L)$ consists of all g with its entry matrices α, β, γ, δ satisfying $\det(\alpha) = \det(\delta) = 1$, $\beta = \gamma = 0$.

Proof. In order to prove the first part, i.e., $f(g \cdot x) = \det(g)^2 f(x)$, we can replace K by its algebraic closure, and we shall use the principle of the irrelevance of algebraic inequalities in Chapter 1.1. We take $t = (g, x)$ regarding the 56 entries of g, x as variables and put

$$R_1(t) = \det(g), \qquad R_2(t) = x_{123}, \qquad R_3(t) = (g \cdot x)_{123}, \qquad R_4(t) = f(x),$$

$$R_5(t) = f(g \cdot x), \qquad F(t) = f(g \cdot x) - \det(g)^2 f(x).$$

Suppose that $R_1(t') \neq 0, \ldots, R_5(t') \neq 0$ for any $t' = (g', x')$ in K^{56}. Then we know that there exist elements g_0, g_1 of $\mathrm{SL}_6(K)$ satisfying $g_0 \cdot x' = (1, \theta_0; 0, 0)$, $g_1 \cdot (g' \cdot x') = (1, \theta_1; 0, 0)$, in which $(\theta_0)^2 = f(x')$, $(\theta_1)^2 = f(g' \cdot x')$. This implies $g_1 g' g_0^{-1} \cdot (1, \theta_0; 0, 0) = (1, \theta_1; 0, 0)$, in which $\theta_0 \theta_1 \det(g_1 g' g_0^{-1}) \neq 0$. Then by Lemma 9.5.2 we get

$$f(g' \cdot x') = (\theta_1)^2 = (\det(g_1 g' g_0^{-1})\theta_0)^2 = \det(g')^2 f(x'),$$

i.e., $F(t') = 0$. Therefore, by the above principle $F(t) = 0$, hence $F(t') = 0$ for all t' in K^{56}.

We shall now go back to the original notation. Suppose that $f(x) \neq 0$ and $\theta = f(x)^{1/2}$. Then for some permutation matrix g_0 we will have $(g_0 \cdot x)_{123} \neq 0$. Since $f(g_0 \cdot x) = \det(g_0)^2 f(x) = f(x)$, the second part follows from what we have shown earlier. As for the third part, the proof of Lemma 9.5.2 shows that if g is in the fixer of $(1, \theta; 0, 0)$ in $\mathrm{GL}_6(L)$ and if $\det(\alpha) \neq 0$, then $\det(\alpha) = \det(\delta) = 1$ and $\beta = \gamma = 0$ while if $\det(\alpha) = 0$, then $\det(g) = -1$. Therefore, if g is in $\mathrm{SL}_6(L)$, then we only have the first possibility. Furthermore, every such g is in the fixer of $(1, \theta; 0, 0)$.

9.6 Gauss' identity and its corollaries

C. F. Gauss used a remarkable identity to convert a theta series into an infinite product; he used a special case of that identity in his first sign-determination of the Gaussian sum. We shall recall his identity with his proof and prove its corollaries for our later use.

In the original notation of Gauss [15] we put

$$T = 1 + (a^n - 1)/(a-1) \cdot t + (a^n - 1)(a^n - a)/(a-1)(a^2-1) \cdot t^2 + \dots ,$$

in which a, t are variables. Since T depends on n, we put $\Theta(n) = T$. Then $\Theta(0) = 1$, $\Theta(1) = 1 + t$, $\Theta(2) = 1 + (a+1)t + at^2 = (1+t)(1+at)$. Furthermore, $\Theta(n+1) = (1 + a^n t)\Theta(n)$, hence

$$T = (1+t)(1+at)\cdots(1+a^{n-1}t).$$

This is the *Gauss identity*.

We now take m from $\mathbb{Z}$, n from $\mathbb{N}$, and put

$$F_{m,n}(a,t) = \prod_{1 \le i \le n} (1 - a^{m+i}t) \;/\; (1 - a^i)$$

with the usual understanding that $F_{m,0}(a,t) = 1$; we extend the definition by $F_{m,n}(a,t) = 0$ for $n < 0$. If we put

$$F_{m,n}(a) = F_{m,n}(a,1),$$

then for $m,\ n \ge 0$ we have

$$F_{m,n}(a) = \prod_{1 \le i \le m+n} (1 - a^i) \;\Big/\; \Big(\prod_{1 \le i \le m} (1-a^i) \cdot \prod_{1 \le i \le n} (1 - a^i) \Big)$$

hence $F_{m,n}(a) = F_{n,m}(a)$, and $F_{i,j}(a)F_{i+j,k}(a) = F_{i,j+k}(a)F_{j,k}(a)$. We also observe that

$$(*) \qquad F_{m,n}(a,t) = F_{m,n-1}(a,t) + a^n F_{m-1,n}(a,t)$$

and further $F_{m,n}(a,t) = F_{m-k,n}(a,a^k t)$ for all m, n, k in $\mathbb{Z}$. In this notation the Gauss identity can be written as

$$(G0) \qquad \sum_{i+j=n} F_{i,j}(a) a^{i(i-1)/2} t^i = \prod_{1 \le i \le n} (1 + a^{i-1}t)$$

for every $n \ge 0$. We might also mention that $(*)$ for $t = 1$ is tacitly used in Gauss' proof, in fact as follows: The coefficient of t^i in $(1 + a^n t)\Theta(n)$ is

$$F_{i,n-i}(a)a^{i(i-1)/2} + F_{i-1,n-i+1}(a)a^{(i-1)(i-2)/2+n}$$

for $0 \le i \le n+1$. Since $(i-1)(i-2)/2 + n = i(i-1)/2 + (n-i+1)$, by using $(*)$ for $t = 1$ we see that it is equal to the coefficient of t^i in $\Theta(n+1)$. Therefore, $\Theta(n+1) = (1 + a^n t)\Theta(n)$, and the rest is by an induction on n.

We shall show that

$$(G1) \qquad \sum_{0\le k\le n}\Big\{\prod_{1\le i\le n-k}(1-a^{i+k})(1-a^{i+k}t)\ /\ (1-a^i)\Big\}a^{k^2}t^k = 1.$$

By $(G0)$ we have

$$\prod_{1\le i\le n-k}(1-a^{i+k}t) = \sum_{i+j=n-k} F_{i,j}(a)\ a^{i(i-1)/2}\ (-a^{k+1}t)^i.$$

Since the other product is $F_{k,n-k}(a)$, the LHS of $(G1)$ becomes

$$\sum_{i+j+k=n}(-1)^i F_{k,n-k}(a)\ F_{i,j}(a)\ a^{i(i+1)/2+(i+k)k}t^{i+k}.$$

If we put $l=i+k$, hence $j=n-l$, by using $F_{k,n-k}(a)\ F_{i,j}(a) = F_{k,i}(a)\ F_{i+k,j}(a)$, the above expression can be rewritten as

$$\sum_{0\le l\le n}\ \{\ \sum_{k+i=l} F_{k,i}(a)\ a^{k(k-1)/2}(-1)^k\big\}\cdot(-1)^l F_{l,n-l}(a)\ a^{l(l+1)/2}t^l.$$

According to $(G0)$, we have

$$\sum_{k+i=l} F_{k,i}(a)\ a^{k(k-1)/2}(-1)^k = \prod_{1\le i\le l}(1-a^{i-1}),$$

which represents 1 or 0 according as $l=0$ or $l>0$. This implies $(G1)$.

We shall next prove

$$(G2) \qquad \sum_{0\le k\le n} F_{m-k,k}(a)\ F_{k,n-k}(a,t)\ a^{k^2}t^k = F_{m,n}(a,t).$$

If we put $D_{m,n}(a,t)$ = RHS - LHS, then $D_{m,n}(a,t)=0$ for $n\le 0$. Therefore, we shall assume that $n>0$ and prove $D_{m,n}(a,t)=0$ by an induction on n. If we apply $(*)$ to $F_{m,n}(a,t)$ and $F_{k,n-k}(a,t)$, then we get

$$\begin{aligned} D_{m,n}(a,t) = &\Big\{F_{m,n-1}(a,t) - \sum_{0\le k\le n} F_{m-k,k}(a)\ F_{k,n-k-1}(a,t)\ a^{k^2}t^k\Big\} \\ &+ a^n\Big\{F_{m-1,n}(a,t) - \sum_{0\le k\le n} F_{m-k,k}(a)\ F_{k-1,n-k}(a,t)\ a^{k^2}(a^{-1}t)^k\Big\}. \end{aligned}$$

We observe that in the first $\{\cdot\}$ the term for $k=n$ is 0, hence $\{\cdot\}$ is equal to $D_{m,n-1}(a,t)$, which is 0 by induction. On the other hand, if we replace $F_{m-1,n}(a,t)$ and $F_{k-1,n-k}(a,t)$ in the second $\{\cdot\}$ respectively by $F_{m,n}(a,a^{-1}t)$ and $F_{k,n-k}(a,a^{-1}t)$, then it becomes $D_{m,n}(a,a^{-1}t)$. Therefore, we get $D_{m,n}(a,t) = a^n D_{m,n}(a,a^{-1}t)$. Since a, t are variables and $D_{m,n}(a,t)$ is a polynomial in t, this implies

$$D_{m,n}(a,t) = A_{m,n}(a)t^n$$

for some $A_{m,n}(a)$ which is independent of t. If we can show that $A_{m,n}(a) = 0$, then we will have $D_{m,n}(a,t) = 0$. Since $A_{m,n}(a)$ is the coefficient of t^n in $D_{m,n}(a,t)$, by going back to its definition we get

$$a^{mn} - (-1)^n \prod_{1\le i\le n} (1-a^i)\cdot a^{-n(n+1)/2} A_{m,n}(a)$$
$$= \sum_{0\le k\le n} (-1)^k F_{m-k,k}(a)\cdot \prod_{1\le i\le k} (1-a^{n-k+i})\cdot a^{k(k-1)/2}.$$

Therefore, we have only to show that the above RHS is equal to a^{mn}. By definition we have

$$F_{m-k,k}(a) \prod_{1\le i\le k} (1-a^{n-k+i}) = F_{n-k,k}(a) \prod_{1\le i\le k} (1-a^{m-k+i})$$

and by $(G0)$ we can write

$$\prod_{1\le i\le k} (1-a^{m-k+i}) = \sum_{i+j=k} F_{i,j}(a)\ a^{i(i-1)/2}(-a^{m-k+1})^i.$$

Therefore, if we put $l = n-k$, then the expression which is expected to be a^{mn} becomes

$$\sum_{i+j+l=n} F_{l,n-l}(a)\ F_{i,j}(a)\ a^{mi+j(j-1)/2}(-1)^j.$$

Since $F_{l,n-l}(a)\ F_{i,j}(a) = F_{i,n-i}(a)\ F_{j,l}(a)$, it can be rewritten as

$$\sum_{0\le i\le n} F_{i,n-i}(a)\ a^{mi}\Big\{ \sum_{j+l=n-i} F_{j,l}(a)\ a^{j(j-1)/2}(-1)^j\Big\}.$$

As in the proof of $(G1)$, we see by $(G0)$ that $\{\cdot\}$ above represents 1 or 0 according as $n-i=0$ or $n-i>0$. Therefore, the above expression is indeed equal to a^{mn}.

Finally, we shall show that

$$(G3)\qquad \sum_{0\le k\le n} F_{m-k,k}(a)\ F_{k,n-k}(a,t)\ a^{k^2-k}t^k = F_{m-1,n}(a,t) + tF_{m,n-1}(a,t).$$

If we apply $(*)$ to $F_{m-k,k}(a)$, the above LHS becomes

$$\sum_{0\le k\le n} F_{m-k,k-1}(a)\ F_{k,n-k}(a,t)\ a^{k^2-k}t^k$$
$$+ \sum_{0\le k\le n} F_{m-k-1,k}(a)\ F_{k,n-k}(a,t)\ a^{k^2}t^k.$$

By $(G2)$ the second sum is equal to $F_{m-1,n}(a,t)$. We observe that in the first sum the term for $k=0$ is 0. If we replace k by $k+1$, the sum becomes

$$t\cdot \sum_{0\le k<n} F_{m-k-1,k}(a)\ F_{k+1,n-k-1}(a,t)\ a^{k^2}(at)^k,$$

in which $F_{k+1,n-k-1}(a,t) = F_{k,n-k-1}(a,at)$. Therefore, again by $(G2)$, it is equal to $t\cdot F_{m-1,n-1}(a,at) = t\cdot F_{m,n-1}(a,t)$.

https://doi.org/10.1090/amsip/014/10

Chapter 10

Computation of $Z(s)$

10.1 $Z(\omega)$ in some simple cases

We recall that

$$Z(\omega) = \int_{X^\circ} \omega(f(x))\ dx,$$

in which $X^\circ = O_K^n$, $dx = \mu_n$ is the Haar measure on $X = K^n$ normalized as $\mu_n(X^\circ) = 1$, and $f(x)$ is in $K[x_1, \dots, x_n] \backslash K$. As for ω, it is in $\Omega_0(K^\times)$, i.e., $t = \omega(\pi)$ satisfies $0 < |t| < 1$. We have denoted $Z(\omega_s)$ by $Z(s)$. This is a p-adic analogue of

$$\int_{\mathbb{R}^n} |f(x)|^s \exp(-\pi^t x x)\ dx.$$

There is a remarkable difference between them about the explicit computability for a given $f(x)$. In the real case $Z(s)$ is hardly computable; while in the p-adic case it is a rational function of t and has been computed for a large number of $f(x)$. The significance of an ever-increasing list of explicitly computed $Z(s)$ is that it allows us to formulate conjectures and proceed to their proofs. At any rate, in this chapter we shall explain some $Z(s)$ in the above-mentioned list. We shall start with the simplest cases after the following general remarks.

Suppose that $O_K^\times$ acts on X as $(u, x) \mapsto u \cdot x$ keeping μ_n and X° invariant; suppose further that $f(u \cdot x) = u^m f(x)$ for some $m > 0$ in $\mathbb{N}$. Then by replacing x by $u \cdot x$ in the integral defining $Z(\omega)$ we get

$$Z(\omega) = \chi(u)^m\ Z(\omega)$$

for every u in $O_K^\times$, in which $\chi = \omega | O_K^\times$. Therefore, $Z(\omega) = 0$ unless $\chi^m = 1$. We remark that $X^\circ \backslash \{0\}$ is the disjoint union of $\pi^e U_n$ for all e in $\mathbb{N}$, where $U_n = X^\circ \backslash \pi X^\circ$, hence $U_1 = O_K^\times$ and $\mu_n(U_n) = [n]$ in the notation of Chapter 9.3. We put

$$[i, j] = 1 - q^{-i} t^j, \qquad [i, j]_+ = 1 + q^i t^j$$

so that $[i] = [i, 0]$, $[i]_+ = [i, 0]_+$ for every i, j in $\mathbb{N}$.

Suppose now that $f(x) = \det(x)$ for x in $X = M_n(K)$, hence $\dim_K(X) = n^2$. If we define $u \cdot x$ as the multiplication by u to the first column x_1 of x, then we will have $\det(u \cdot x) = u \det(x)$, hence $Z(\omega) = 0$ unless $\chi = 1$. If we denote $Z(s)$ by $Z_n(s)$, then by the same method as in Chapter 6.3, we can show that

$$Z_n(s) = \prod_{1 \le k \le n} [k]/[k, 1].$$

In fact, as a special case of Lemma 8.2.1, we get $Z_1(s) = [1]/[1,1]$. If $n > 1$, we write $x = (x_1 x')$ and apply the second remark above to the domain of integration by dx_1. In that way, we get

$$Z_n(s) = \sum_{i\geq 0} (q^{-n}t)^i \int_{U_n} dx_1 \Big\{ \int_{(X')^\circ} |\det(x_1 x')|_K^s \; dx' \Big\},$$

in which $X' = M_{n,n-1}(K)$. We observe that every x_1 in U_n can be written as $x_1 = ge_1$ for some g in $\mathrm{SL}_n(O_K)$. If we replace x' by gx', then $\{\cdot\}$ above becomes $Z_{n-1}(s)$, hence

$$Z_n(s) = Z_{n-1}(s) \cdot [n]/[n,1].$$

If we apply the induction assumption to $Z_{n-1}(s)$, we get the above expression for $Z_n(s)$.

Suppose next that x is in $X = \mathrm{Alt}_{2n}(K)$, hence $\dim_K(X) = n(2n-1)$. We then take the Pfaffian $\mathrm{Pf}(x)$ of x as $f(x)$. We recall that $\mathrm{Pf}(x)$ is defined in Chapter 9.5 as

$$\mathrm{Pf}(x) = \sum{}' \epsilon(\sigma) x_{\sigma(1),\sigma(2)} \cdots x_{\sigma(2n-1),\sigma(2n)},$$

in which σ is a permutation of $\{1, 2, \ldots, 2n\}$ restricted as at that place. It follows from the definition that $\mathrm{Pf}(gx^t g) = \det(g)\mathrm{Pf}(x)$ for every g in $\mathrm{GL}_{2n}(K)$. Therefore, if g is a diagonal matrix in $\mathrm{GL}_{2n}(O_K)$ with $u, 1, \ldots, 1$ as its diagonal entries and if we put $u \cdot x = gx^t g$, then $\mathrm{Pf}(u \cdot x) = u\ \mathrm{Pf}(x)$, hence $Z(\omega) = 0$ unless $\chi = 1$. If we denote $Z(s)$ by $Z_n(s)$, then similarly as above we can show that

$$Z_n(s) = \prod_{1\leq k\leq n} [2k-1]/[2k-1,1].$$

In fact, since $\mathrm{Pf}(x) = x_{12}$ for $n = 1$, we get $Z_1(s) = [1]/[1,1]$. In the case where $n > 1$, the first row of x in X° is of the form $\pi^i(0\ {}^t x_1)$ for some i in $\mathbb{N}$ and x_1 in U_{2n-1}, hence $x_1 = g'e_1$ for some g' in $\mathrm{SL}_{2n-1}(O_K)$. If we denote by g the element of $\mathrm{SL}_{2n}(O_K)$ with $1,\ 0,\ 0,\ g'$ as its entry matrices and if x'' in $X'' = \mathrm{Alt}_{2n-2}(K)$ is the right-bottom entry matrix of $g^{-1}x\ {}^t g^{-1}$, then x'' is in $(X'')^\circ$ and $\mathrm{Pf}(x) = \pi^i \mathrm{Pf}(x'')$. Since $d(\pi^i x_1) = q^{-(2n-1)i}\ dx_1$, therefore, we get

$$\begin{aligned} Z_n(s) &= \sum_{i\geq 0} (q^{-(2n-1)}t)^i \int_{U_{2n-1}} dx_1 \Big\{ \int_{(X'')^\circ} |\mathrm{Pf}(x'')|_K^s \; dx'' \Big\} \\ &= Z_{n-1}(s) \cdot [2n-1]/[2n-1,1]. \end{aligned}$$

By induction this implies the above expression for $Z_n(s)$.

As the third simple case we take column vectors x', x'' in K^m and put

$$x = {}^t({}^t x', {}^t x''), \qquad f(x) = {}^t x' x''$$

so that $X = K^{2m}$. In order to compute $Z(\omega)$ we can use Theorem 8.4.1 and an explicit form of $F(i)$ in Chapter 8.3 for the above $f(x)$. We can also do it directly

as follows. If we define $u \cdot x$ as the multiplication by u to x', then $f(u \cdot x) = uf(x)$, hence $Z(\omega) = 0$ unless $\chi = 1$. Furthermore,

$$Z(s) = \sum_{i \geq 0} (q^{-m}t)^i \int_{U_m} dx' \Big\{ \int_{O_K^m} |{}^t x' x''|_K^s \, dx'' \Big\}.$$

If in the above $\{\cdot\}$ we write $x' = ge_1$ for some g in $\mathrm{GL}_m(O_K)$ and replace x'' by ${}^t g^{-1} x''$, then it becomes $[1]/[1,1]$, hence

$$Z(s) = [1][m]/[1,1][m,1].$$

Before we proceed further, we shall compute $Z(s)$ in a similar case where

$$f(x) = {}^t x' x'' + \pi^e x_0$$

for any e in $\mathbb{N}$ so that $X = K^{2m+1}$. If we denote $Z(s)$ by $\varphi(e)$ in this case, then clearly $\varphi(0) = [1]/[1,1]$. If $e > 0$, then we write

$$\varphi(e) = \int_{O_K^m} dx' \Big\{ \int_{O_K^{m+1}} |{}^t x' x'' + \pi^e x_0|_K^s \, dx'' dx_0 \Big\},$$

and split O_K^m above into U_m and πO_K^m. Then, by the repeatedly used argument, we get

$$\varphi(e) = [m] \cdot [1]/[1,1] + q^{-m} t \cdot \varphi(e-1).$$

This is a recursion formula by which we can express $\varphi(e)$ in terms of $\varphi(0)$. In that way we get

$$\int_{X^\circ} |{}^t x' x'' + \pi^e x_0|_K^s \, dx = [1]/[1,1][m,1] \cdot \Big\{ [m] + [0,1] q^{-m} (q^{-m}t)^e \Big\}$$

for every e in $\mathbb{N}$. We might remark that $Z(s)$ in the third case becomes the limit of the above expression as $e \to \infty$.

As the fourth simple case we take x from $X = M_{2m,2n}(K)$ where $m \geq n$ and

$$f(x) = \mathrm{Pf}({}^t x J_m x),$$

in which J_m is as in Chapter 9.3 the element of $\mathrm{Alt}_{2m}(\mathbb{Z})$ with 1 as its $(2i-1, 2i)$-entry for $1 \leq i \leq m$ and 0 as its (i,j)-entry for all other $i < j$. If we define $u \cdot x$ as the multiplication by u to the first column of x, then $f(u \cdot x) = uf(x)$, hence $Z(\omega) = 0$ unless $\chi = 1$. If we denote $Z(s)$ by $Z_{m,n}(s)$, then we have

$$Z_{m,n}(s) = \prod_{1 \leq k \leq n} [2(m-k+1)][2k-1]/[2(m-k+1),1][2k-1,1].$$

The proof is by now a familiar argument. We write the first column of x as $\pi^i x_1$ for some i in $\mathbb{N}$ and x_1 in U_{2m}. If we denote by $\mathrm{Sp}_{2m}(O_K)$ the intersection of $\mathrm{Sp}_{2m}(K)$ and $\mathrm{GL}_{2m}(O_K)$, then it consists of all $g = (w_1 \; w_2 \; \ldots \; w_{2m})$ in $M_{2n}(O_K)$ satisfying ${}^t w_{2i-1} J_m w_{2i} = 1$ for $1 \leq i \leq m$ and ${}^t w_i J_m w_j = 0$ for all other $i < j$. Therefore by

the same argument as in Chapter 9.3 we see that every x_1 in U_{2m} can be written as $x_1 = ge_1$ for some g in $\mathrm{Sp}_{2m}(O_K)$. If we put $X' = M_{2m,2n-1}(K)$, then similarly as before we get

$$Z_{m,n}(s) = \sum_{i\geq 0}(q^{-2m}t)^i \int_{U_{2m}} dx_1 \Big\{ \int_{(X')^\circ} |f(x_1\ x')|_K^s\ dx' \Big\}$$
$$= [2m]/[2m,1] \cdot \int_{(X')^\circ} |f(e_1\ x')|_K^s\ dx'.$$

We shall denote the above integral over $(X')^\circ$ by I. We put $Y = M_{2n-1,2m-1}(K)$ and ${}^t x' = (y_1\ y_2\ y')$ with column vectors $y_1,\ y_2$ so that $y = (y_1\ y')$ is in Y°. Then we will have

$$I = \sum_{i\geq 0} q^{-(2n-1)i} \int_{U_{2n-1}} dy_2 \Big\{ \int_{Y^\circ} |f(e_1{}^t(y_1\ \pi^i y_2\ y'))|_K^s\ dy \Big\}.$$

If in the above $\{\cdot\}$ we write $y_2 = g^* e_1^*$ for some g^* in $\mathrm{GL}_{2n-1}(O_K)$, where e_1^* is the e_1 in K^{2n-1}, and replace y by $g^* y$, then $f(e_1{}^t(y_1\ \pi^i y_2\ y'))$ will be replaced by $\det(g^*) f(e_1{}^t(y_1\ \pi^i e_1^*\ y'))$. Therefore, we get

$$I = [2n-1] \cdot \sum_{i\geq 0} q^{-(2n-1)i} \int_{Y^\circ} |f(e_1{}^t(y_1\ \pi^i e_1^*\ y'))|_K^s\ dy.$$

We shall denote the above integral over Y° by I_i. The point is that if we put $X'' = M_{2m-2,2n-2}(K)$, $x = (e_1{}^t(y_1\ \pi^i e_1^*\ y'))$, and denote by x'' in $(X'')^\circ$ the right-bottom entry matrix of x, then we have

$$f(x) = \mathrm{Pf}({}^t x J_m x) = \pi^i \cdot \mathrm{Pf}({}^t x'' J_{m-1} x'').$$

Therefore, we get $I_i = t^i \cdot Z_{m-1,n-1}(s)$, hence

$$Z_{m,n}(s) = [2m][2n-1]/[2m,1][2n-1,1] \cdot Z_{m-1,n-1}(s)$$

with the understanding that $Z_{m-1,n-1}(s) = 1$ for $n = 1$. This implies the above-stated expression for $Z_{m,n}(s)$. We shall see later in this chapter that if we replace J_m above by an element h of $\mathrm{Sym}_{2m}(\mathbb{Z})$ with 1 as its $(2i-1,2i)$-entry for $1 \leq i \leq m$ and 0 as its (i,j)-entry for all other $i < j$, and accordingly $\mathrm{Pf}({}^t x J_m x)$ by $\det({}^t x h x)$, then the corresponding $Z_{m,n}(s)$ will have an entirely different expression.

Finally, as the fifth simple case we take $x = (y, (z_1\ z_2))$, where y is in $Y = \mathrm{Alt}_6(K)$ and $(z_1\ z_2)$ is in $M_{6,2}(K)$ hence $\dim_K(X) = 27$, and

$$f(x) = \mathrm{Pf}(y) - {}^t z_1 y z_2.$$

If g is a diagonal matrix in $\mathrm{GL}_6(O_K)$ with $u, 1, \ldots, 1$ as its diagonal entries and if we put $u \cdot x = (gy{}^t g, {}^t g^{-1}(uz_1\ z_2))$, then $f(u \cdot x) = uf(x)$, hence $Z(\omega) = 0$ unless $\chi = 1$. We shall show that

$$Z(s) = [1][5][9]/[1,1][5,1][9,1].$$

We shall use capital letters for the spaces of variables expressed by small letters such as X, x and Y, y above. We write $Z(s)$ as an integral with respect to $dy\ dz_1$ followed by an integration by dz_2. If we split $(Z_2)^\circ\backslash\{0\}$ into $\pi^i U_6$ for all i in $\mathbb{N}$, write z_2 in U_6 as $z_2 = ge_1$ for some g in $\mathrm{SL}_6(O_K)$ and replace $y,\ z_1$ respectively by ${}^t g^{-1} y g^{-1},\ gz_1$, then we get

$$Z(s) = [6] \cdot \sum_{i \geq 0} q^{-6i} \int_{Y^\circ \times W^\circ} |\mathrm{Pf}(y) + \pi^i\, {}^t y_1 w|_K^s\ dydw,$$

in which $W = K^5$ and $(0\ {}^t y_1)$ is the first row of y. If y' is obtained from y by crossing out its first row and column, hence $Y' = \mathrm{Alt}_5(K)$, then we write the above integral as an integral with respect to $dy'dw$ followed by an integration by dy_1. We split $(Y_1)^\circ\backslash\{0\}$ into $\pi^j U_5$ for all j in $\mathbb{N}$, write y_1 in U_5 as $y_1 = g'e_1'$ for some g' in $\mathrm{SL}_5(O_K)$, where e_1' is the e_1 in K^5, and replace $y',\ w$ respectively by $g'y'{}^t g',\ {}^t(g')^{-1}w$. If y'' is obtained from the new y' by crossing out its first row and column, hence $Y'' = \mathrm{Alt}_4(K)$, then we get

$$Z(s) = [5][6]/[5,1] \cdot \sum_{i \geq 0} q^{-6i} \int_{(Y'')^\circ \times O_K} |\mathrm{Pf}(y'') + \pi^i x_0|_K^s\ dy'' dx_0.$$

We observe that $\mathrm{Pf}(y'')$ is of the form $x_1x_4 + x_2x_5 + x_3x_6$. Therefore, the above integral is $\varphi(i)$ before for $m = 3$ and, by using that expression for $\varphi(i)$, we get the expression for $Z(s)$ as stated above.

We might mention that in the above computation K is an arbitrary p-adic field and that there is no restriction on q. Cases 1, 2, 3 are classical. The computation of $Z(s)$ in Case 5, i.e., for the norm form of the Jordan algebra $H_3(C)$ for an octonion K-algebra C, was first made by J. G. M. Mars [39] in an equivalent form assuming that q is relatively prime to 6. More precisely he computed Weil's function $F^*(i^*)$ in that case. Case 4 and one more simple case are in [27]. We might further mention that one of the reasons why the above cases are called "simple" is that the zeros of Bernstein's polynomials of $f(x)$ are all integers. We copy the following list from T. Kimura [34]:

$$b_f(s) = \prod_{1 \leq k \leq n} (s+k), \qquad \prod_{1 \leq k \leq n} (s+2k-1), \qquad (s+1)(s+m),$$
$$\prod_{1 \leq k \leq n} (s+2(m-k+1))(s+2k-1), \qquad (s+1)(s+5)(s+9).$$

If we write $b_f(s) = \prod(s+\lambda)$, then the above results can be stated simultaneously as $Z(s) = \prod[\lambda]/[\lambda, 1]$.

10.2 A p-adic stationary phase formula

We shall formulate a general and useful method to compute $Z(s)$. We recall that

$$Z(s) = \int_{X^\circ} |f(x)|_K^s\ dx, \qquad \mathrm{Re}(s) > 0,$$

in which $f(x)$ is in $K[x_1,\dots,x_n]\backslash K$ and the Haar measure dx on $X = K^n$ is normalized so that the total measure of $X^\circ = O_K^n$ becomes 1. After multiplying a suitable power of π to $f(x)$, we may assume that the coefficients of $f(x)$ are in O_K but not all in πO_K, hence $\bar{f}(x) = f(x) \bmod \pi$ is in $\mathbb{F}_q[x_1,\dots,x_n]\backslash\{0\}$. We put $t = q^{-s}$ and use the notation $[i,j]$, etc. as in section 10.1.

Theorem 10.2.1 *We take a subset $\bar{E}$ of $\mathbb{F}_q^n$ and denote by $\bar{S}$ its subset consisting of all $\bar{a}$ in $\bar{E}$ such that $\bar{f}(\bar{a}) = (\partial\bar{f}/\partial x_i)(\bar{a}) = 0$ for $1 \le i \le n$; we further denote by E, S the preimages of $\bar{E}, \bar{S}$ under $X^\circ \to X^\circ/\pi X^\circ$ and by N the number of zeros of $\bar{f}(x)$ in $\bar{E}$. Then we have*

$$\int_E |f(x)|_K^s\, dx = q^{-n}(\mathrm{card}(\bar{E}) - N) + q^{-n}(N - \mathrm{card}(\bar{S}))\ [1]t/[1,1] + \int_S |f(x)|_K^s\, dx.$$

Proof. If we write $\bar{a} = a \bmod \pi$ for every a in X°, then we have

$$\int_E |f(x)|_K^s\, dx = q^{-n} \cdot \sum_{\bar{a}\in\bar{E}\backslash\bar{S}} \int_{X^\circ} |f(a+\pi x)|_K^s\, dx + \int_S |f(x)|_K^s\, dx.$$

If $\bar{f}(\bar{a}) \ne 0$, then $f(a+\pi x) \equiv f(a) \not\equiv 0 \bmod \pi$ for all x in X°, hence the contribution of all such $\bar{a}$ in $\bar{E}$ is $q^{-n}(\mathrm{card}(\bar{E}) - N)$. If $\bar{f}(\bar{a}) = 0$ and $(\partial\bar{f}/\partial x_i)(\bar{a}) \ne 0$ for some i, then we use Lemma 7.4.3. If we put

$$g_i(x) = \pi^{-1}(f(a+\pi x) - f(a)), \qquad g_j(x) = x_j \quad (j \ne i),$$

then $g_1(x),\dots,g_n(x)$ are SRP's in $x_1,\dots,x_n$ and

$$\partial(g_1,\dots,g_n)/\partial(x_1,\dots,x_n)(0) = (\partial f/\partial x_i)(a) \not\equiv 0 \bmod \pi,$$

hence $(y_1,\dots,y_n) = (g_1(x),\dots,g_n(x))$ gives a measure-preserving map from X° to X°. Therefore, we get

$$\int_{X^\circ} |f(a+\pi x)|_K^s\, dx = \int_{O_K} |\pi(y_i + \pi^{-1}f(a))|_K^s\, dy_i = t \cdot [1]/[1,1],$$

hence the contribution of all such $\bar{a}$ in $\bar{E}$ is $q^{-n}(N - \mathrm{card}(\bar{S})) \cdot [1]t/[1,1]$.

We have called the above theorem a *p-adic stationary phase formula*, abbreviated as SPF, in [30]. The significance of SPF is its wide applicability. Before we give a more appropriate example or examples, we shall prove the following general statement by using SPF:

Proposition 10.2.1 *If $f(x)$ is a homogeneous polynomial of degree d in $O_K[x_1,\dots,x_n]$ such that $\bar{f}(\bar{a}) = (\partial\bar{f}/\partial x_i)(\bar{a}) = 0$ for $1 \le i \le n$ implies $\bar{a} = 0$ and further if N denotes the number of zeros of $\bar{f}(x)$ in $\mathbb{F}_q^n$, then*

$$Z(s) = ([1][n]t + (1 - q^{-n}N)[0,1])/[1,1][n,d].$$

Proof. If in SPF we take $\bar{E} = \mathbb{F}_q^n$, then $S = \pi X^\circ$ by assumption. Furthermore, since $f(x)$ is homogeneous of degree d, we have $f(\pi x) = \pi^d f(x)$. Therefore, we get

$$Z(s) = q^{-n}(q^{-n} - N) + q^{-n}(N-1)[1]t/[1,1] + q^{-n}t^d \cdot Z(s).$$

This can be rewritten as stated in the proposition.

Corollary 10.2.1 *If $Q(x)$ is a quadratic form in $O_K[x_1, \ldots, x_n]$ such that $\bar{Q}(x)$ is reduced, then*

$$Z(s) = \begin{cases} [1][n,1]/[1,1][n,2] & n \text{ odd} \\ [1](1 - \chi(\bar{Q})q^{-n/2})/[1,1](1 - \chi(\bar{Q})q^{-n/2}t) & n \text{ even,} \end{cases}$$

in which $\chi(\bar{Q}) = \pm 1$ according as $\bar{Q}$ is hyperbolic or not.

In fact, if $d = 2$, then the condition on $f(x) = Q(x)$ in Proposition 10.2.1 is that $\bar{Q}$ on $= F_q^n$ is reduced. Therefore by Theorem 9.2.1 we have

$$N = \begin{cases} q^{n-1} & n \text{ odd} \\ q^{n-1} + \chi(\bar{Q})[1]q^{n/2} & n \text{ even.} \end{cases}$$

This implies the formula in the corollary.

We shall compute $Z(s)$ for a variant of $f(x)$ in Proposition 10.2.1. Namely, instead of that $f(x)$, we take $f(x) + \pi^i y$ for any i in $\mathbb{N}$ and compute

$$\varphi(i) = \int_{X^\circ \times O_K} |f(x) + \pi^i y|_K^s \, dxdy.$$

We clearly have $\varphi(0) = [1]/[1,1]$. In the case where $i > 0$, if we apply SPF to $\varphi(i)$, we get

$$\varphi(i) = [n,d]Z(s) + \begin{cases} q^{-n}t^i \cdot \varphi(0) & 0 < i \le d \\ q^{-n}t^d \cdot \varphi(i-d) & i \ge d, \end{cases}$$

in which $Z(s)$ is for $f(x)$. If we write $i = dk + i_0$, where $0 \le i_0 < d$, then by an induction on j we get

$$\varphi(i) = [nj, dj]Z(s) + (q^{-n}t^d)^j \cdot \varphi(d(k-j) + i_0)$$

for $0 \le j \le k$, hence

$$\varphi(i) = \begin{cases} [n(k+1), d(k+1)]Z(s) + (q^{-n}t^d)^k \cdot q^{-n}t^{i_0} \cdot [1]/[1,1] & i_0 > 0 \\ [nk, dk]Z(s) + (q^{-n}t^d)^k \cdot [1]/[1,1] & i_0 = 0. \end{cases}$$

In particular, if we replace $f(x)$ by a quadratic form $Q(x)$, then we will have

$$\varphi(i) = \begin{cases} [n(i+1)/2, i+1]Z(s) + (q^{-n/2}t)^{i-1} \cdot q^{-n}t \cdot [1]/[1,1] & i \text{ odd} \\ [ni/2, i]Z(s) + (q^{-n/2}t)^i \cdot [1]/[1,1] & i \text{ even.} \end{cases}$$

We observe that if we formally equate the above RHS's, we get

$$Z(s) = [1][n/2]/[1,1][n/2,1].$$

In other words if $\bar{Q}$ is hyperbolic and only in that case, the above two expressions become equal, and

$$\int_{X^\circ \times O_K} |Q(x) + \pi^e y|_K^s \, dxdy = [1]/[1,1][n/2,1] \cdot \{[n/2] + [0,1]q^{-n/2}(q^{-n/2}t)^e\}$$

for every e in $\mathbb{N}$. We have computed this integral already in section 10.1.

Before we proceed further, we remark that quadratic forms $Q(x)$ in $O_K[x_1, \dots, x_n]$ with reduced $\bar{Q}$ have entirely similar properties as those in $\mathbb{F}_q[x_1, \dots, x_n]$. We shall show, as an example, that if $\bar{Q}$ is hyperbolic, hence $n = 2m$, then we can find $w_1, w_2, \dots, w_n$ in $X^\circ = O_K^n$ satisfying

$$\sum_{1 \le i \le n} O_K w_i = X^0, \qquad Q\Big(\sum_{1 \le i \le n} x_i w_i\Big) = \sum_{1 \le i \le m} x_{2i-1} x_{2i}$$

for every $x_1, \dots, x_n$ in O_K. We first observe that if $\bar{Q}$ is just reduced and $\bar{Q}(\bar{a}_0) = 0$ for some a_0 in X° with $\bar{a}_0 \neq 0$, then we can find a in X° satisfying $Q(a) = 0$, $a \equiv a_0 \mod \pi$. In fact $\pi^{-1}(Q(a_0 + \pi x) - Q(a_0))$ is an SRP in $x_1, \dots, x_n$ with a unit of O_K as the coefficient of x_i for some i, hence it is equal to any element of O_K, say $-\pi^{-1}Q(a_0)$, for some $x = a_1$ in X°. Then $Q(a) = 0$ for $a = a_0 + \pi a_1 \equiv a_0 \mod \pi$. If now $Q(a) = 0$ for some a in X° with $\bar{a} \neq 0$, since $\bar{b} \mapsto \bar{Q}(\bar{a}, \bar{b})$ gives an $\mathbb{F}_q$-linear surjection from $\mathbb{F}_q^n$ to $\mathbb{F}_q$, the O_K-homomorphism $b \mapsto Q(a, b)$ from X° to O_K is also surjective, hence $Q(a, b_0) = 1$ for some b_0 in X°. If we put $b = -Q(b_0)a + b_0$, we will have $Q(a, b) = 1$, $Q(b) = 0$. If we denote the intersection of X° and $\langle a, b\rangle^\perp$ by L, then $x - Q(x, b)a - Q(x, a)b$ is in L for every x in X°, hence

$$X^\circ = (O_K a + O_K b) \oplus L.$$

Therefore, we have only to put $w_1 = a$, $w_2 = b$ and continue this process. We might also mention that if q is odd, then the square map gives a surjection from $1 + \pi O_K$ to itself by Lemma 8.4.1. This implies the isomorphism $O_K^\times/(O_K^\times)^2 \to \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$. If we denote by χ the character of $O_K^\times$ which gives rise to the isomorphism $O_K^\times/(O_K^\times)^2 \to \{\pm 1\}$, then $\chi(\bar{Q}) = \chi(d(Q))$ in Corollary 10.2.1 for the discriminant $d(Q)$ of Q relative to any O_K-basis for X°.

We shall now discuss the case which exemplifies the way SPF can be applied. We shall show that $Z(s)$ is computable for

$$f(x) = \sum_{1 \le i \le n} c_i x_i^{d_i},$$

in which $d_1, \dots, d_n$ are integers larger than 1 at most one of which is divisible by the prime factor of q. This condition is clearly satisfied if they form a strictly increasing sequence of prime numbers with no restriction on q. As for $c_1, \dots, c_n$,

we may assume that they are in O_K but not all in πO_K. If we denote by J the set of all i for which $\bar{c}_i \neq 0$ so that

$$\bar{f}(x) = \sum_{i \in J} \bar{c}_i x_i^{d_i} \neq 0$$

and by N_J the number of zeros of $\bar{f}(x)$ in $\bar{E} = \mathbb{F}_q^n$, then N_J has been expressed in terms of Jacobi sums by A. Weil [57]. Furthermore, $\bar{S}$ is defined by $x_i = 0$ for all i in J. Therefore, by SPF we get

$$Z(s) = \int_{X^\circ} |f(x)|_K^s \, dx = R_J + q^{-\mathrm{card}(J)} t^e \cdot \int_{X^\circ} |f_1(x)|_K^s \, dx,$$

in which

$$R_J = (1 - q^{-n} N_J) + (q^{-n} N_J - q^{-\mathrm{card}(J)})[1]t/[1,1].$$

As for e and $f_1(x)$, we replace x_i in $f(x)$ by πx_i for all i in J and write the new $f(x)$ as $\pi^e f_1(x)$ with $f_1(x)$ satisfying the same condition as $f(x)$. We can then apply the same argument to $f_1(x)$. By repeating this process, we get a sequence $f_0(x) = f(x),\ f_1(x),\ f_2(x),\ \ldots$. If we write

$$f_j(x) = \sum_{1 \leq i \leq n} c_{ji} x_i^{d_i},$$

then c_{ji} differs from c_i only by a power of π, hence we can write

$$Z_j(s) = \int_{X^\circ} |f_j(x)|_K^s \, dx = (\mathrm{ord}(c_{j1}), \ldots, \mathrm{ord}(c_{jn}))$$

for all j in $\mathbb{N}$. The point is that, in view of $\mathrm{ord}(c_{ji}) \leq \max(\mathrm{ord}(c_i), d_i)$ for all i, j, the sequence $Z_0(s) = Z(s),\ Z_1(s),\ Z_2(s),\ \ldots$ becomes periodic, i.e. $Z_j(s) = Z_{j'}(s)$ for some $j < j'$. Then $[\alpha, \beta] Z_j(s)$ for some $\alpha, \beta > 0$ in $\mathbb{N}$ becomes known, hence all $Z_k(s)$, in particular $Z(s)$, will be known. In the following, we take $c_1 = c_2 = \ldots = c_n = 1,\ \{d_1, d_2, \ldots, d_n\} = \{2, 3\},\ \{2, 3, 5\}$ and make the corresponding $Z(s)$ explicit.

If $f(x) = x_1^2 + x_2^3$, then $N_J = q$ not only for $J = \{1\}, \{2\}$ but also for $J = \{1, 2\}$ because the plane curve $f^{-1}\{0\}$ is parametrized as $x_1 = u^3,\ x_2 = -u^2$. Therefore, we get $R_J = [1][j, 1]/[1, 1]$ for $j = \mathrm{card}(J)$. If we denote R_J by R_j for $j = \mathrm{card}(J)$, then we get the following sequence:

$$(0,0) = R_2 + q^{-2} t^2 (0,1), \qquad (0,1) = R_1 + q^{-1} t (1,0),$$

$$(1,0) = R_1 + q^{-1} t (0,2), \qquad (0,2) = R_1 + q^{-1} t^2 (0,0).$$

This implies

$$\begin{aligned} Z(s) &= \int_{X^\circ} |x_1^2 + x_2^3|_K^s \, dx \\ &= [1]/[1,1][5,6] \cdot (1 - q^{-2} t(1-t) - q^{-5} t^5). \end{aligned}$$

If $f(x) = x_1^2 + x_2^3 + x_3^5$, then $N_J = q^2$ for all J. This is clear for $\mathrm{card}(J) = 1$ and also for $J = \{1, 2\}$ by what we have shown. If $x_1^2 + x_3^5 = 0$, $x_3 \neq 0$, and $x_1 = ux_3$, then $u^2 + x_3^3 = 0$, hence $N_J = q^2$ for $J = \{1, 3\}$. If $x_2^3 + x_3^5 = 0$, $x_3 \neq 0$, and $x_2 = ux_3$, then $u^3 + x_3^2 = 0$, hence $N_J = q^2$ for $J = \{2, 3\}$. Finally, if $x_1^2 + x_2^3 + x_3^5 = 0$, $x_3 \neq 0$, and $x_1 = u_1 x_3^3$, $x_2 = u_2 x_3^2$, then $(u_1^2 + u_2^3)x_3 + 1 = 0$, hence

$$N_J = q(\text{from } x_3 = 0) + (q^2 - q)(\text{from } x_3 \neq 0) = q^2$$

also for $J = \{1, 2, 3\}$. Therefore, we get $R_J = [1][j, 1]/[1, 1]$ for $j = \mathrm{card}(J)$. If we denote R_J by R_j for $j = \mathrm{card}(J)$, then we get the following sequence:

$$(0,0,0) = R_3 + q^{-3}t^2(0,1,3), \quad (0,1,3) = R_1 + q^{-1}t(1,0,2),$$

$$(1,0,2) = R_1 + q^{-1}t(0,2,1), \quad (0,2,1) = R_1 + q^{-1}t(1,1,0),$$

$$(1,1,0) = R_1 + q^{-1}t(0,0,4), \quad (0,0,4) = R_2 + q^{-2}t^2(0,1,2),$$

$$(0,1,2) = R_1 + q^{-1}t(1,0,1), \quad (1,0,1) = R_1 + q^{-1}t(0,2,0),$$

$$(0,2,0) = R_2 + q^{-2}t^2(0,0,3), \quad (0,0,3) = R_2 + q^{-2}t^2(0,1,1),$$

$$(0,1,1) = R_1 + q^{-1}t(1,0,0), \quad (1,0,0) = R_2 + q^{-2}t(0,2,4),$$

$$(0,2,4) = R_1 + q^{-1}t^2(0,0,2), \quad (0,0,2) = R_2 + q^{-2}t^2(0,1,0),$$

$$(0,1,0) = R_2 + q^{-2}t(1,0,4), \quad (1,0,4) = R_1 + q^{-1}t(0,2,3),$$

$$(0,2,3) = R_1 + q^{-1}t^2(0,0,1), \quad (0,0,1) = R_2 + q^{-2}t(1,2,0),$$

$$(1,2,0) = R_1 + q^{-1}t(0,1,4), \quad (0,1,4) = R_1 + q^{-1}t(1,0,3),$$

$$(1,0,3) = R_1 + q^{-1}t(0,2,2), \quad (0,2,2) = R_1 + q^{-1}t^2(0,0,0).$$

If we put $u = q^{-1}t$, then we can write

$$Z(s) = \int_{X^\circ} |x_1^2 + x_2^3 + x_3^5|_K^s dx = [1]/[1,1][31,30] \cdot$$
$$1 - q^{-3}t(1-t)(1 + u^6 + u^{10} + u^{12} + u^{16} + u^{18} + u^{22}) - q^{-31}t^{29}.$$

In the above two examples the fact that the successive applications of SPF will terminate by periodicity is known beforehand. In the general case that is an open problem. We recall that Hironaka's theorem guarantees the finiteness of successive monoidal transformations to achieve a desingularization if they are chosen correctly. We also recall that in the two variable case the process is unique as we have mentioned in Chapter 3.3. In that case the desingularization of $f^{-1}(0)$ is so explicit that it can be used to get precise information about the local zeta fucntion of $f(x)$. There are several remarkable papers on this subject. We just mention [24], [26] and above all the papers by D. Meuser [41] and L. Strauss [54].

10.3 A key lemma

We shall formulate a powerful method to compute $Z(s)$ for a relative invariant $f(x)$ of a subgroup G of $\mathrm{GL}_n(K)$. Namely, $f(x)$ is an element of $K[x_1, \ldots, x_n]\backslash K$ satisfying $f(gx) = \nu(g)f(x)$ with $\nu(g)$ in $K^\times$ for every g in G. This implies $\nu(gg') = \nu(g)\nu(g')$ for every g, g' in G. As before we shall assume that the coefficients of $f(x)$ are in O_K but not all in πO_K. We define $G(O_K)$ as the intersection of G and $\mathrm{GL}_n(O_K)$ and denote by $G(\mathbb{F}_q)$ the image of $G(O_K)$ under the homomorphism $\mathrm{GL}_n(O_K) \to \mathrm{GL}_n(\mathbb{F}_q)$. We shall keep on using the notation $X^\circ = O_K^n$, instead of $X(O_K)$, for $X = K^n$. If we denote the images of g, a in $G(O_K)$, X° under $G(O_K) \to G(\mathbb{F}_q)$, $X^\circ \to \mathbb{F}_q^n$ respectively by $\bar{g}$, $\bar{a}$, then we will have

$$\overline{ga} = \bar{g}\bar{a}.$$

Theorem 10.3.1 *If we choose a subset R of X° such that $\mathbb{F}_q^n$ becomes a disjoint union of $G(\mathbb{F}_q)\bar{\xi}$ for all ξ in R, then for $Re(s) > 0$ we have*

$$\int_{X^\circ} |f(x)|_K^s \, dx = \sum_{\xi \in R} \mathrm{card}(G(\mathbb{F}_q)\bar{\xi}) \cdot \int_{\xi + \pi X^\circ} |f(x)|_K^s \, dx.$$

Proof. We first observe that $\nu(g)$ for every g in $G(O_K)$ is in $O_K^\times$. In fact, if g is in $G(O_K)$, hence in $M_n(O_K)$, since $f(x)$ is in $O_K[x_1, \ldots, x_n]$, we see that $f(gx)$ is also in $O_K[x_1, \ldots, x_n]$. Therefore, if $c_i x^i$ is any term of $f(x)$, then $f(gx) = \nu(g)f(x)$ implies that $\nu(g)c_i$ is in O_K for every i. Since c_i is in $O_K^\times$ for at least one i, we see that $\nu(g)$ itself is in O_K. Since $\nu(g)\nu(g^{-1}) = 1$ and g^{-1} is in $G(O_K)$, hence $\nu(g^{-1})$ is in O_K, we see that $\nu(g)$ is in $O_K^\times$.

Secondly, if a, b are in X°, g is in $G(O_K)$, and $\bar{b} = \bar{g}\bar{a}$, then the integrals of $|f(x)|_K^s$ over $a + \pi X^\circ$ and $b + \pi X^\circ$ are equal. In fact, since $\bar{g}\bar{a} = \overline{ga}$ and $G(O_K)$ keeps X° invariant, we have $b + \pi X^\circ = ga + \pi X^\circ = g(a + \pi X^\circ)$. Furthermore since the action of $G(O_K)$ on X° is measure preserving, we get

$$\int_{b+\pi X^\circ} |f(x)|_K^s \, dx = \int_{g(a+\pi X^\circ)} |f(x)|_K^s \, dx = \int_{a+\pi X^\circ} |f(x)|_K^s \, dx.$$

We have tacitly used the fact that $|f(gx)|_K = |\nu(g)|_K |f(x)|_K = |f(x)|_K$.

We have called the above theorem a *key lemma* in [28]. Actually, in a slightly different form it appeared in our paper of 1977 and in the above form with several applications in [25]. We might mention that it would look more natural to use a $G(O_K)$-orbital decomposition of X°. However, that approach did not work except for some very simple cases. The usefulness of the key lemma comes from the facts that firstly the $G(\mathbb{F}_q)$-orbital decomposition of $\mathbb{F}_q^n$ is not too difficult to obtain and secondly in the partial integral of $|f(x)|_K^s$ over $\xi + \pi X^\circ$ we can replace $f(x)$ by a simpler polynomial in a smaller number of variables. This second process has been formalized as a supplement to the key lemma in [28].

At any rate, we remark that if $\bar{f}(\bar{\xi}) \neq 0$, then the partial integral over $\xi + \pi X^\circ$ is clearly q^{-n}. On the other hand, if $f(x)$ is homogeneous of degree d, then the

partial integral over πX° is $q^{-n}t^d \cdot Z(s)$. Therefore, in that case, if we denote by R' the subset of R defined by $\bar{f}(\bar{\xi}) = 0$ and $\bar{\xi} \neq 0$, then we will have

$$[n,d]Z(s) = \mathrm{card}(\bar{f}^{-1}(\mathbb{F}_q^\times))q^{-n} + \sum_{\xi \in R'} \mathrm{card}(G(\mathbb{F}_q)\bar{\xi}) \cdot \int_{\xi+\pi X^\circ} |f(x)|_K^s \, dx.$$

Furthermore, if $\bar{f}(\bar{\xi}) = 0$ and $(\partial \bar{f}/\partial x_i)(\bar{\xi}) \neq 0$ for some i, then the proof of Theorem 10.2.1 shows that

$$\int_{\xi+\pi X^\circ} |f(x)|_K^s \, dx = [1]q^{-n}t/[1,1].$$

We also remark that if $\tilde{G}$ is a subgroup of $\mathrm{GL}_m(K)$ for some m, ρ is a homomorphism from $\tilde{G}(O_K)$ to $G(O_K)$, and $\bar{\rho}$ is a homomorphism from $\tilde{G}(\mathbb{F}_q)$ to $G(\mathbb{F}_q)$ which is compatible with the taking of mod π, i.e.,

$$\bar{\rho}(g \bmod \pi) = \rho(g) \bmod \pi$$

for every g in $\tilde{G}(O_K)$, then we can use the decomposition of $\mathbb{F}_q^n$ into $\tilde{G}(\mathbb{F}_q)$-orbits instead of $G(\mathbb{F}_q)$-orbits. We can also use the obvious fact that if $\tilde{G}(\mathbb{F}_q)_{\bar{\xi}}$ denotes the fixer of $\bar{\xi}$ in $\tilde{G}(\mathbb{F}_q)$ defined by $\bar{\rho}(\bar{g})\bar{\xi} = \bar{\xi}$, then

$$\mathrm{card}(\bar{\rho}(\tilde{G}(\mathbb{F}_q))\bar{\xi}) = \mathrm{card}(\tilde{G}(\mathbb{F}_q))/\mathrm{card}(\tilde{G}(\mathbb{F}_q)_{\bar{\xi}}).$$

We shall give an application of the key lemma which will illustrate how it works. We start with some preparations. We take an arbitrary field F and we let $\mathrm{GL}_n(F)$ act on $\mathrm{Sym}_n(F)$ as $(g,x) \mapsto g \cdot x = gx^t g$. We keep in mind that $\mathrm{rank}(g \cdot x) = \mathrm{rank}(x)$ for every g in $\mathrm{GL}_n(F)$ and x in $\mathrm{Sym}_n(F)$. We write $n = p + k$, where $1 \leq p \leq n$, and denote by g_1, g_{12}, g_{21}, g_2 the $p \times p$, $p \times k$, $k \times p$, $k \times k$ entry matrices of g; if $p = n$, hence $k = 0$, it is understood that $g = g_1$. Also if x_1, x_2 are respectively in $M_p(F)$, $M_k(F)$, we denote by $x_1 \oplus x_2$ the element of $M_n(F)$ with x_1, 0, 0, x_2 as its entry matrices. Suppose now that x_0, x_0' are in $\mathrm{Sym}_p(F)$ and $\det(x_0 x_0') \neq 0$. Then we have

$$g \cdot (x_0 \oplus 0) = x_0' \oplus 0$$

if and only if g_1 is in $\mathrm{GL}_p(F)$ satisfying $g_1 \cdot x_0 = x_0'$, g_2 is in $\mathrm{GL}_k(F)$, g_{12} is free in $M_{p,k}(F)$, and $g_{21} = 0$. We shall show that the $\mathrm{GL}_n(F)$-orbit of any x in $\mathrm{Sym}_n(F)$ contains an element of the form $x_1 \oplus x_2$, in which x_1 is a diagonal matrix with $\det(x_1) \neq 0$ while all diagonal entries of x_2 are 0. Firstly, if g is the permutation matrix representing $(1p)$, then the $(1,1)$-entry of $g \cdot x$ is the (p,p)-entry of x. Secondly, if x_1, x_{12}, ${}^t x_{12}$, x_2 are the $p \times p$, $p \times k$, $k \times p$, $k \times k$ entry matrices of x with $\det(x_1) \neq 0$ and if g is the element of $\mathrm{SL}_n(F)$ such that ${}^t g$ has 1_p, $-x_1^{-1}x_{12}$, 0, 1_k as its entry matrices, then

$$g \cdot x = x_1 \oplus (x_2 - {}^t x_{12} x_1^{-1} x_{12}).$$

We have only to use these facts repeatedly to verify the above statement.

Lemma 10.3.1 *We write $n = p + k$, where $1 \leq p \leq n$, and put*

$$\Sigma_p = \{x \in \mathrm{Sym}_n(F);\ \mathrm{rank}(x) = p\}.$$

Then every $\mathrm{GL}_n(F)$-orbit in Σ_p contains an element of the form $\xi = x_0 \oplus 0$ with x_0 in $\mathrm{Sym}_p(F)$, hence $\det(x_0) \neq 0$. In the special case, where $F = \mathbb{F}_q$ the number of $\mathrm{GL}_n(F)$-orbits in Σ_p is 2 except for the case where p is odd and q is even; in that case the number is 1. Furthermore, if we put

$$c_k = q^{-n(n+1)/2} \cdot \mathrm{card}(\Sigma_p),$$

then in all cases we have

$$c_k = q^{-k(k+1)/2} \cdot \prod_{1 \leq i \leq p} [i+k] \Big/ \prod_{1 \leq 2i \leq p} [2i].$$

Proof. Suppose first that $\mathrm{char}(F) \neq 2$. If for every x in $\mathrm{Sym}_n(F)$ we put $Q_x(u) = {}^t uxu$, where u is in F^n, then the correspondence $x \mapsto Q_x$ gives a bijection from $\mathrm{Sym}_n(F)$ to the set of all quadratic forms on F^n. Furthermore, if we let $\mathrm{GL}_n(F)$ act on this set as $(g, Q) \mapsto (g \cdot Q)(u) = Q({}^t gu)$, then the above bijection becomes equivariant. Therefore by the classical diagonalization of a quadratic form and by Theorem 9.2.1, we get the lemma except for the expression for c_k. If ξ is a representative of one of the two $\mathrm{GL}_n(F)$-orbits in Σ_p for $F = \mathbb{F}_q$ expressed as in the lemma, then

$$\mathrm{card}(\mathrm{GL}_n(F) \cdot x) = \mathrm{card}(\mathrm{GL}_n(F))/q^{pk}\mathrm{card}(\mathrm{GL}_k(F))\mathrm{card}(\mathrm{O}(Q_{x_0})(F)),$$

in which Q_{x_0} is on F^p. If we use the expressions for $\mathrm{card}(G(F))$ for various G in Chapter 9.3, then we can easily see that

$$c_k = q^{-n(n+1)/2} \cdot \sum_{\xi} \mathrm{card}(\mathrm{GL}_n(F) \cdot \xi)$$

is given by the formula in the lemma.

Suppose next that $\mathrm{char}(F) = 2$ and choose a representative of any $\mathrm{GL}_n(F)$-orbit in Σ_p of the form $x_1 \oplus x_2$, in which x_1 is a diagonal matrix of degree say i with $\det(x_1) \neq 0$ while all diagonal entries of x_2 are 0. Then x_2 is in $\mathrm{Alt}_l(F)$, where $l = n - i$, hence $g_2 \cdot x_2 = J_j \oplus 0$ for some g_2 in $\mathrm{GL}_l(F)$, in which $p = i + 2j$. We have thus shown that every $\mathrm{GL}_n(F)$-orbit in Σ_p contains an element ξ of the form in the lemma with $x_0 = x_1 \oplus J_j$. We shall now take $\mathbb{F}_q$ as F. Since every element of F is a square in F, we may assume that $x_1 = 1_i$. A crucial observation is that there exists an element g of $\mathrm{SL}_3(\mathbb{F}_2)$ satisfying

$$g \cdot (1 \oplus J_1) = 1_3.$$

Actually, there are six elements such as g and one of them has 0 only at $(2, 3)$ and $(3, 2)$, i.e., all other entries are 1. Therefore if p is even, then the $\mathrm{GL}_p(F)$-orbit of x_0 contains either $J_{p/2}$ or $\xi_0 = 1_2 \oplus J_{p/2-1}$ while if p is odd, it contains $\xi_1 = 1 \oplus J_{(p-1)/2}$.

We observe that, in the case where p is even, the $\mathrm{GL}_n(F)$-orbits of ξ with $J_{p/2}$ and ξ_0 as x_0 are different because $Q_\xi = 0$ for one and $Q_\xi \neq 0$ for another. Therefore, the number of $\mathrm{GL}_n(F)$-orbits in Σ_p is 2 if p is even and 1 if p is odd.

We shall determine the fixers in $\mathrm{GL}_n(F)$ of the above representatives. We have only to determine the fixers in $\mathrm{GL}_p(F)$ of ξ_0, ξ_1. We for a moment change the notation and replace p by n and write ξ instead of ξ_0, ξ_1. Also we denote by H the fixer of ξ in $\mathrm{GL}_n(F)$. Suppose first that $n = 2m$, put $J = J_{m-1}$, and denote by a, b, c, d the entry matrices of g, in which a is in $M_2(F)$, etc. Then g is in H, i.e., $g\xi^t g = \xi$ for $\xi = 1_2 \oplus J$, if and only if

$$a^t a + bJ^t b = 1_2, \qquad a^t c + bJ^t d = 0, \qquad c^t c + dJ^t d = J.$$

We observe that $c^t c + dJ^t d = J$ implies that all diagonal entries of $c^t c$ are 0, hence $c = (u\ u)$ for some u in F^{2m-2}. Then $c^t c = 0$, hence $dJ^t d = J$, i.e., d is in $\mathrm{Sp}_{2m-2}(F)$. Similarly, $a^t a + bJ^t b = 1_2$ implies that the entries of a are $1 + a_0,\ a_0,\ a_1,\ 1 + a_1$ for some a_0, a_1 in F, hence $a^t c = {}^t c$. Then $a^t c + bJ^t d = 0$ implies ${}^t b = Jd^{-1}c = (v\ v)$, in which $v = Jd^{-1}u$. This implies $bJ^t b = 0$, hence $a^t a = 1_2$, and hence $a_0 = a_1$ in a. Conversely, if a_0, u, d are respectively in F, F^{2m-2}, $\mathrm{Sp}_{2m-2}(F)$ and a, b, c are defined as above, then g is in H. Furthermore, the correspondence $g \mapsto d$ gives a surjective homomorphism from H to $\mathrm{Sp}_{2m-2}(F)$ such that the kernel is isomorphic to $F^{2m-2} \times F$ with the following multiplication:

$$(u, a_0)(u', a_0') = (u + u',\ a_0 + a_0' + {}^t u J u').$$

In particular,

$$\mathrm{card}(H) = q^{2m-1} \cdot \mathrm{card}(\mathrm{Sp}_{2m-2}(F)) = \mathrm{card}(\mathrm{Sp}_{2m}(F))/q^{2m}[2m].$$

Suppose next that $n = 2m+1$ and $\xi = 1 \oplus J_m$. Then in a similar but much simpler way we see that H consists of $g = 1 \oplus d$ for all d in $\mathrm{Sp}_{2m}(F)$.

If we go back to the original notation, then the order of the fixer of ξ in $\mathrm{GL}_n(F)$ is given by

$$q^{pk}\mathrm{card}(\mathrm{GL}_k(F)) \cdot \begin{cases} \left.\begin{array}{ll} \mathrm{card}(\mathrm{Sp}_p(F)) & x_0 = J_{p/2} \\ \mathrm{card}(\mathrm{Sp}_p(F))/q^p[p] & x_0 = \xi_0 \end{array}\right\} & p \text{ even} \\ \mathrm{card}(\mathrm{Sp}_{p-1}(F)) \quad x_0 = \xi_1 & p \text{ odd} \end{cases}$$

Therefore, we get the same c_k as before also in this case.

We are now ready to apply the key lemma to the computation of $Z(s)$ for $X = \mathrm{Sym}_n(K)$ and $f(x) = \det(x)$, hence $\dim_K(X) = n(n+1)/2$ and $\deg(f) = n$. We write $n = p+k$, where $1 \leq p \leq n$, and denote the entry matrices of x by x_1, x_{12}, ${}^t x_{12}$, x_2 with x_1 in $\mathrm{Sym}_p(K)$, etc. as before. If ξ is an element of $X^\circ = \mathrm{Sym}_n(O_K)$ with $x_1 = \xi_0,\ x_{12} = 0,\ x_2 = 0$ such that $\mathrm{rank}(\xi_0 \mod \pi) = p$, i.e., $\det(\xi_0)$ is in $O_K^\times$, then the partial integral of $|f(x)|_K^s$ over $\xi + \pi X^\circ$ can be written as

$$q^{-n(n+1)/2} \cdot \int_{\mathrm{Sym}_p(O_K) \times M_{p,k}(O_K)} dx_1 dx_{12} \Big\{ \int_{\mathrm{Sym}_k(O_K)} |\det(\xi + \pi x)|_K^s\ dx_2 \Big\}.$$

We shall examine the above $\{\cdot\}$. If we denote by g the element of $\mathrm{GL}_n(K)$ such that ${}^t g$ has 1_p, $-\pi(\xi_0+\pi x_1)^{-1}x_{12}$, 0, 1_k as its entry matrices, then g is in $\mathrm{GL}_n(O_K)$ and

$$g\cdot(\xi+\pi x)=(\xi_0+\pi x_1)\oplus\pi(x_2-\pi^t x_{12}(\xi_0+\pi x_1)^{-1}x_{12}).$$

Therefore, if we denote the original $Z(s)$ by $Z_n(s)$, then $\{\cdot\}$ becomes $t^k Z_k(s)$, hence

$$\int_{\xi+\pi X^\circ}|\det(x)|_K^s\,dx=q^{-n(n+1)/2}t^k Z_k(s).$$

Therefore, by the key lemma and Lemma 10.3.1 we will have

$$[n(n+1)/2,n]Z_n(s)=\sum_{0\le k<n}c_k t^k Z_k(s).$$

This is a recursion formula by which we can determine $Z(s)=Z_n(s)$ starting with $Z_0(s)=1$. The result is as follows:

Proposition 10.3.1 *If $X=\mathrm{Sym}_n(K)$ and $f(x)=\det(x)$, then*

$$Z(s)=1/[1,1]\cdot\prod_{1\le i\le m}[2i-1]/[2i+1,2]\cdot\begin{cases}[2m+1,1] & n=2m\\ [2m+1] & n=2m+1.\end{cases}$$

Proof. In view of the recursion formula, we have only to show that

$$\sum_{0\le k\le n}c_k t^k Z_k(s)/Z_n(s)=1,$$

in which c_k is as in Lemma 10.3.1 with the understanding that $c_n=q^{-n(n+1)/2}$ and $Z_k(s)$ is the $Z(s)$ in the proposition with n replaced by k for $0\le k\le n$. We separate cases according as n is even or odd. Then after an elementary computation, we see that the LHS is equal to

$$\sum_{0\le k\le m}\Big(\prod_{1\le i\le m-k}[2i+2k][2i+2k+1,2]/[2i]\Big)q^{-2k^2}(q^{-1}t^2)^k$$

for $n=2m$ or $n=2m+1$. If in the formal identity $(G1)$ in Chapter 9.6, we replace n, a, t respectively by m, q^{-2}, $q^{-1}t^2$, then we see that the above expression is indeed equal to 1.

Proposition 10.3.1 in the case where q is odd is in [25]; the restriction is removed by the generality of Lemma 10.3.1. At any rate, by T. Kimura [34] we have

$$b_f(s)=\prod_{1\le k\le n}(s+(k+1)/2).$$

10.4 $Z(s)$ for a Freudenthal quartic

We shall compute $Z(s)$ for the Freudenthal quartic $f(x)$ in Proposition 9.5.1. We have identified $X = \bigwedge^3 K^6$ with $K^2 + M_3(K)^2$ as $x = (a_0, b_0; a, b)$, in which

$$a_0 = -x_{123}, \qquad b_0 = -x_{456}, \qquad a = (x_{23i}\ x_{31i}\ x_{12i}), \qquad b = (x_{i56}\ x_{i64}\ x_{i45})$$

respectively for $i = 4$, 5, 6 and $i = 1$, 2, 3; we have $\dim_K(X) = 20$ and

$$f(x) = (a_0 b_0 - \mathrm{tr}(ab))^2 - 4(a_0 \det(b) + b_0 \det(a) + \mathrm{tr}(a^\#, b^\#)),$$

in which $a^\# = \mathrm{Adj}(a) = \det(a)a^{-1}$, etc. We shall first determine the $\mathrm{GL}_6(\mathbb{F}_q)$-orbital decomposition of $X(\mathbb{F}_q) = \bigwedge^3 \mathbb{F}_q^6$. For a moment, we take any field F with $\mathrm{char}(F) \neq 2$. We recall that $f(g \cdot x) = \det(g)^2 f(x)$ for every g in $\mathrm{GL}_6(F)$ and x in X. We express g by its 3×3 entry matrices α, β, γ, δ as before. We can easily verify that if $\beta = \gamma = 0$ in g, then

$$g \cdot (a_0, b_0; a, b) = (\det(\alpha)a_0, \det(\delta)b_0; \delta a \alpha^\#, \alpha b \delta^\#)$$

for every α, δ in $\mathrm{GL}_3(F)$.

If ξ is in $X(F') = \bigwedge^3 (F')^6$, where F' is any field which contains F, and $f(\xi) \neq 0$, then for every g in the fixer of ξ in $\mathrm{GL}_6(F')$ we have $\det(g) = \pm 1$. Therefore, the fixer of ξ in $\mathrm{SL}_6(F')$ is the kernel of the homomorphism from the fixer of ξ in $\mathrm{GL}_6(F')$ to $\{\pm 1\}$ under $g \mapsto \det(g)$, hence the corresponding index is at most two. After this remark, we take $\xi_0 = (1, \theta^3; 0, 0)$ with θ^2 in $F^\times$ so that $f(\xi_0) = \theta^6$ is also in $F^\times$. We have shown in Proposition 9.5.1 that the fixer of ξ_0 in $\mathrm{SL}_6(F(\theta))$ consists of all g with α, δ in $\mathrm{SL}_3(F(\theta))$ and $\beta = \gamma = 0$. Furthermore, if g_1 is defined by $\alpha = \delta = 0$, $\beta = \theta^{-1}1_3$, $\gamma = \theta 1_3$, then by Lemma 9.5.1 we see that $g_1 \cdot \xi_0 = \xi_0$ while $\det(g_1) = -1$. Therefore, if we denote by H the fixer of ξ_0 in $\mathrm{GL}_6(F(\theta))$, then H is the union of $\mathrm{SL}_3(F(\theta)) \times \mathrm{SL}_3(F(\theta))$ embedded in $\mathrm{GL}_6(F(\theta))$ as $(\alpha, \delta) \mapsto g$ above and its coset represented by g_1. In particular, if $F = \mathbb{F}_q$ and θ itself is in F, say $\theta = 1$, then

$$\mathrm{card}(\mathrm{GL}_6(F) \cdot \xi_0) = \mathrm{card}(\mathrm{GL}_6(F))/2\mathrm{card}(\mathrm{SL}_3(F))^2 = q^{20} \cdot c_0,$$
$$c_0 = (1/2)[1][2]_+[3]_+[5].$$

On the other hand, if θ is not in F, i.e., if θ^2 is in $F^\times \backslash (F^\times)^2$, then we take $\xi_0' = (-\theta^2, 0; 0, 1_3)$. If g_0 is defined by $\alpha = \theta 1_3$, $\beta = 1_3$, $\gamma = -1_3$, $\delta = \theta^{-1}1_3$, then by Lemma 9.5.1 we see that $\xi_0' = g_0 \cdot (-1/2\theta)\xi_0$. Therefore, the correspondence $g \mapsto g' = g_0 g g_0^{-1}$ gives an isomorphism from H to the fixer H' of ξ_0' in $\mathrm{GL}_6(F(\theta))$. In particular, $g_1' = g_0 g_1 g_0^{-1}$ is in H'. Since g_1' has $\alpha = 1_3$, $\delta = -1_3$, $\beta = \gamma = 0$ as its entry matrices, it is in $\mathrm{GL}_6(F)$ and $\det(g_1') = -1$. We observe that the isomorphism $H \to H'$ restricted to $\mathrm{SL}_3(F(\theta)) \times \mathrm{SL}_3(F(\theta))$ has the following form:

$$g = \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \mapsto g' = (1/2) \begin{pmatrix} \alpha + \delta & -\theta(\alpha - \delta) \\ -\theta^{-1}(\alpha - \delta) & \alpha + \delta \end{pmatrix}$$

We write $\alpha = \alpha_0 + \theta\alpha_1$, $\delta = \delta_0 + \theta\delta_1$ with α_i, δ_i in $M_3(F)$ for $i = 0, 1$ and observe that g' is in $\mathrm{GL}_6(F)$ if and only if $\alpha_0 = \delta_0$, $\alpha_1 = -\delta_1$, i.e., if and only if α, δ are conjugate under the automorphism of $F(\theta)$ over F. This shows that the fixer of ξ_0' in $\mathrm{SL}_6(F)$ is isomorphic to $\mathrm{SL}_3(F(\theta))$. Therefore, if $F = \mathbb{F}_q$, then

$$\mathrm{card}(\mathrm{GL}_6(F) \cdot \xi_0') = \mathrm{card}(\mathrm{GL}_6(F))/2\mathrm{card}(\mathrm{SL}_3(F(\theta)) = q^{20} \cdot c_0',$$
$$c_0' = (1/2)[1][2][3][5].$$

We keep in mind that $c_0 + c_0' = [1][10]$.

We shall next take $\xi_1 = (0, 0; 1_3, 0) = e_{234} + e_{315} + e_{126}$ in which e_{ijk} stands for $e_i \wedge e_j \wedge e_k$ for $1 \leq i,\ j,\ k \leq 6$, and determine its fixer in $\mathrm{GL}_6(F)$. If for any ξ we define the p-th polar of $f(x)$ at ξ by

$$f(\xi + tx) = \sum_{p \geq 0} f_p(\xi, x)t^p = f(\xi) + f_1(\xi, x)t + \dots,$$

where t is a variable, then we get $f_1(\xi_1, x) = 4x_{456}$. Since for every g in $\mathrm{GL}_6(F)$ we have $f_p(g \cdot \xi, g \cdot x) = \det(g)^2 f_p(\xi, x)$, if $g \cdot \xi_1 = \xi_1$ and $g \cdot x = x'$, then $x'_{456} = \det(g)^2 x_{456}$, i.e.,

$$\sum_{1 \leq i,j,k \leq 6} g_{4i}g_{5j}g_{6k}x_{ijk} = \det(g)^2 x_{456}$$

for every x in $X(F)$. We shall for a moment restrict our attention to the submatrix $(\gamma\ \delta)$ of g. If we denote by π_{ijk} the determinant of the 3×3 matrix made up of its i-th, j-th, k-th columns, then we can rewrite the above condition as

$$\sum_{1 \leq i < j < k \leq 6} \pi_{ijk}x_{ijk} = \det(g)^2 x_{456}$$

for every x, hence $\pi_{456} = \det(g)^2 \neq 0$. In particular, the 4-th, 5-th, 6-th columns are linearly independent. Therefore, $\pi_{145} = \pi_{146} = \pi_{156} = 0$ implies that the first column is 0. Similarly, we see that the second and the third columns are 0, hence $\gamma = 0$ in g. On the other hand, if $v = v_1e_1 + v_2e_2 + v_3e_3$ for v_i in F, then $\xi_1 v = (v_1e_4 + v_2e_5 + v_3e_6)e_{123}$. By applying the above g to this we see that $\alpha = \det(\alpha)\delta$, i.e., $\delta\alpha^{\#} = 1_3$. Conversely, if for any α in $\mathrm{GL}_3(F)$ we define δ as above and take $\beta = \gamma = 0$ in g, then g is in the fixer of ξ_1 in $\mathrm{GL}_6(F)$. Furthermore, if $\alpha = \delta = 1_3$ and $\gamma = 0$ in any g in $\mathrm{GL}_6(F)$, then we can easily verify that

$$g \cdot \xi_1 = \xi_1 + \mathrm{tr}(\beta)e_{123}.$$

Therefore, the kernel of the surjective homomorphism from the fixer of ξ_1 in $\mathrm{GL}_6(F)$ to $\mathrm{GL}_3(F)$ defined by $g \mapsto \alpha$ consists of all g with $\alpha = \delta = 1_3$, $\gamma = 0$, and $\mathrm{tr}(\beta) = 0$. If $F = \mathbb{F}_q$, this implies

$$\mathrm{card}(\mathrm{GL}_6(F) \cdot \xi_1) = \mathrm{card}(\mathrm{GL}_6(F))/q^8\mathrm{card}(\mathrm{GL}_3(F)) = q^{20} \cdot c_1,$$
$$c_1 = q^{-1}[4][5][6].$$

We shall next take $\xi_2 = e_{126} + e_{346}$. If $v = \sum v_i e_i$ for v_i in F, then

$$\xi_2 v = -(v_3 e_{1236} + v_4 e_{1246} + v_5 e_{1256} + v_1 e_{1346} + v_2 e_{2346} + v_5 e_{3456}).$$

Therefore, $\xi_2 v = 0$ if and only if $v = v_6 e_6$. This implies that if g is in the fixer of ξ_2 in $\mathrm{GL}_6(F)$, hence $\xi_2(g e_6) = g(\xi_2 e_6) = 0$, we get $g e_6 = \lambda^{-1} e_6$ for some λ in $F^\times$. Furthermore, if g_0 is the element of $\mathrm{GL}_5(F)$ which is obtained from g by crossing out its 6-th row and column, then $g_0 \cdot (e_{12} + e_{34}) = \lambda(e_{12} + e_{34})$, i.e., $g_0(J_2 \oplus 0)^t g_0 = \lambda(J_2 \oplus 0)$. Therefore, g is of the form

$$g = \begin{pmatrix} g_{11} & g_{12} & 0 \\ 0 & g_{22} & 0 \\ g_{31} & g_{32} & \lambda^{-1} \end{pmatrix},$$

in which g_{11} is in $\mathrm{GL}_4(F)$ satisfying $g_{11} J_2 {}^t g_{11} = \lambda J_2$, g_{22}, λ are in $F^\times$, and other entry matrices are free. Conversely, if g is of this form, then g is in $\mathrm{GL}_6(F)$ and $g \cdot \xi_2 = \xi_2$. We further observe that $g \mapsto \lambda$ defines a surjective homomorphism from the fixer of ξ_2 in $\mathrm{GL}_6(F)$ to $F^\times$ because the diagonal matrix with λ, 1, λ, 1, 1, λ^{-1} as its diagonal entries is in the fixer for every λ in $F^\times$. Therefore, if $F = \mathbb{F}_q$, then

$$\begin{aligned} \mathrm{card}(\mathrm{GL}_6(F) \cdot \xi_2) &= \mathrm{card}(\mathrm{GL}_6(F))/q^{11}[1]^2 \mathrm{card}(\mathrm{Sp}_4(F)) = q^{20} \cdot c_2, \\ c_2 &= q^{-5}[3][5][6]/[1]. \end{aligned}$$

Finally, if $\xi_3 = e_{123}$, then Lemma 9.5.1 shows that the fixer of ξ_3 in $\mathrm{GL}_6(F)$ consists of all g with α in $\mathrm{SL}_3(F)$, δ in $\mathrm{GL}_3(F)$, $\gamma = 0$, and β free in $M_3(F)$. If $F = \mathbb{F}_q$, therefore, we get

$$\begin{aligned} \mathrm{card}(\mathrm{GL}_6(F) \cdot \xi_3) &= \mathrm{card}(\mathrm{GL}_6(F))/q^{10}[1]\mathrm{card}(\mathrm{SL}_3(F))^2 = q^{20} \cdot c_3, \\ c_3 &= q^{-10}[2]_+[3]_+[5]. \end{aligned}$$

We shall show, by using $f_p(g \cdot \xi, g \cdot x) = \det(g)^2 f_p(\xi, x)$ for every g, that the $\mathrm{GL}_6(F)$-orbits of $\xi_0, \xi_0', \xi_1, \xi_2, \xi_3$ are different. Firstly, $f(\xi_0)$ is in $(F^\times)^2$ while $f(\xi_0')$ is in $F^\times \backslash (F^\times)^2$. Secondly, $f(\xi_1) = f(\xi_2) = f(\xi_3) = 0$ and $f_1(\xi_1, x) \neq 0$, $f_1(\xi_2, x) = f_1(\xi_3, x) = 0$. Thirdly, we can easily see that $f_2(\xi_2, x)$ and $f_2(\xi_3, x)$ are nondegenerate quadratic forms respectively in five and one variables. Therefore, the five $\mathrm{GL}_6(F)$-orbits are certainly different. Furthermore, in the case where $F = \mathbb{F}_q$ we have

$$c_0 + c_0' + c_1 + c_2 + c_3 = [20] = q^{-20} \cdot \mathrm{card}(X(F) \backslash \{0\}).$$

By putting these together we see that $X(F)\backslash\{0\}$ becomes the disjoint union of the $\mathrm{GL}_6(F)$-orbits of $\xi_0, \xi_0', \xi_1, \xi_2, \xi_3$. Therefore, by the key lemma we get

$$(*) \qquad [20,4]Z(s) = [1][10] + c_1 \cdot [1]t/[1,1] + \sum_{i=2,3} c_i \cdot \int_{X^\circ} |f(\xi_i + \pi x)|_K^s \, dx.$$

We have only to compute the above two partial integrals.

Suppose first that $i = 2$. If we apply the even permutation $\{1,3,4,5,6\} \mapsto \{3,5,6,4,1\}$ to the subscripts of e_i, then $\xi_2 = e_{126}+e_{346}$ becomes $\xi = -e_{123}+e_{156} = (1,0;0,u)$, in which $u = 1 \oplus 0$, and the integral to be computed becomes

$$\int_{X^\circ} |f(\xi+\pi x)|_K^s \, dx = \int_{O_K \times M_3(O_K)} da_0 da \Big\{ \int_{O_K \times M_3(O_K)} |f(\xi+\pi x)|_K^s \, db_0 db \Big\}.$$

In the above $\{\cdot\}$ we have $\xi + \pi x = (a_0', \pi b_0; \pi a, u + \pi b)$, in which $a_0' = 1 + \pi a_0$. Therefore, if we define an element g of $\mathrm{SL}_6(O_K)$ by $\alpha = \delta = 1_3$, $\beta = 0$, and $\gamma = (a_0')^{-1}\pi a$, then, as we have seen in Chapter 9.5, we have

$$g \cdot (\xi + \pi x) = (a_0', \pi b_0'; 0, u + \pi b'),$$

in which $b' = b + (a_0')^{-1}\pi a^{\#}$ and

$$b_0' = b_0 - (a_0')^{-1}\mathrm{tr}(a(u+\pi b)) - 2(a_0')^{-2}\pi^2 \det(a).$$

We observe that $(b_0, b) \mapsto (b_0', b')$ gives a measure-preserving bijection from $O_K \times M_3(O_K)$ to itself. Since $f(a_0', \pi b_0'; 0, u+\pi b') = (\pi a_0' b_0')^2 - 4a_0' \det(u+\pi b')$, therefore we get

$$\int_{X^\circ} |f(\xi+\pi x)|_K^s \, dx = \int_{O_K \times M_3(O_K)} |(\pi b_0)^2 - \det(u+\pi b)|_K^s \, db_0 db.$$

The above integral can be reduced to an integral in Corollary 10.2.1 by the method we have repeatedly used in section 10.1. We write $b = (b_1 \ b')$ with a 3×2 submatrix b' and express the integral as an integral by db' followed by an integration by $db_0 \, db_1$. Since the first column of $u + \pi b$ can be completed to an element of $\mathrm{SL}_3(O_K)$, if b'' denotes the bottom 2×2 submatrix of b', then the integral by db' becomes an integral by db''. In that way we get

$$\begin{aligned} \int_{X^\circ} |f(\xi+\pi x)|_K^s \, dx &= t^2 \cdot \int_{O_K \times M_2(O_K)} |b_0^2 + \det(b'')|_K^s \, db_0 db'' \\ &= t^2 \cdot [1][5,1]/[1,1][5,2]. \end{aligned}$$

Suppose next that $i = 3$ and put $\xi = -\xi_3 = (1,0;0,0)$. Then by the first part of the above argument we get

$$\int_{X^\circ} |f(\xi+\pi x)|_K^s \, dx = \int_{O_K \times M_3(O_K)} |(\pi b_0)^2 + \det(\pi b)|_K^s \, db_0 db.$$

We shall compute this integral in the following lemma:

Lemma 10.4.1 *If we define $P(t)$ as*

$$[1]\big\{1 - (1+q^{-1}-q^{-3})q^{-3}t + (1+q^{-1}-q^{-2}-q^{-3}-q^{-4})q^{-3}t^2 + q^{-12}t^3\big\},$$

then

$$\int_{O_K \times M_3(O_K)} |y_0^2 + \pi \det(y)|_K^s \, dy_0 dy = P(t)/[1,1][5,2][7,2].$$

Proof. We shall denote the integral in question by Z_0 and compute it by a successive application of SPF. In doing so we shall use the following facts: If we let $\mathrm{GL}_3(F) \times \mathrm{GL}_3(F)$ act on $M_3(F)$ as $(g_1, g_2) \cdot y = g_1 y g_2^{-1}$, then $M_3(F)$ splits into four orbits $\Sigma_0, \Sigma_1, \Sigma_2, \Sigma_3$, in which Σ_p consists of all y with $\mathrm{rank}(y) = p$ and it is represented by $1_p \oplus 0$; if $k = 3 - p$, the fixer of $1_p \oplus 0$ consists of all (g_1, g_2) with the entry matrices a_i, b_i, c_i, d_i of g_i satisfying $a_1 = a_2$ in $\mathrm{GL}_p(F)$, d_1, d_2 in $\mathrm{GL}_k(F)$, $c_1 = 0$, $b_2 = 0$, and b_1, c_2 free for $0 \le p \le 3$. Furthermore, all partial derivatives of $\det(y)$ vanish at y if and only if $y^{\#} = 0$, i.e., $\mathrm{rank}(y) \le 1$. If $F = \mathbb{F}_q$, then the above structure of the fixer of $1_p \oplus 0$ implies

$$\begin{aligned} q^{-9}\mathrm{card}(\Sigma_p) &= q^{-k^2}[k+1]^2 \dots [3]^2/[1] \dots [p] \\ &= q^{-9}, \quad q^{-4}[3]^2/[1], \quad q^{-1}[2][3]^2/[1], \quad [1][2][3] \end{aligned}$$

respectively for $p = 0, 1, 2, 3$. Moreover since the map $\det : M_3(F) \to F$ is surjective with $\mathrm{card}(\det^{-1}(c)) = \mathrm{card}(\mathrm{SL}_3(F))$ or $q^9 - \mathrm{card}(\mathrm{GL}_3(F))$ according as $c \ne 0$ or $c = 0$, the number of (y_0, y) satisfying $y_0^2 + \det(y) = 0$ is

$$(q-1) \cdot \mathrm{card}(\mathrm{SL}_3(F)) + (q^9 - \mathrm{card}(\mathrm{GL}_3(F)) = q^9.$$

Also we shall reduce the integral over $M_3(O_K)$ to that over $M_2(O_K)$ similarly as in the previous case.

If now we put $D = O_K \times M_3(O_K)$ and $D' = O_K \times M_2(O_K)$, then we have

$$\begin{aligned} Z_0 &= [1] + q^{-1}tZ_1, \qquad Z_1 = \int_D |\pi y_0^2 + \det(y)|_K^s \, dy_0 dy; \\ Z_1 &= [1][2][3] + [2][3]^2 q^{-1}t/[1,1] + [3]^2 q^{-4}t/[1] \cdot Z_2 + q^{-9}tZ_3, \\ Z_2 &= \int_{D'} |y_0^2 + \pi \det(y')|_K^s \, dy_0 dy', \qquad Z_3 = \int_D |y_0^2 + \pi^2 \det(y)|_K^s \, dy_0 dy; \\ Z_2 &= [1] + q^{-1}tZ_{21}, \qquad Z_{21} = \int_{D'} |\pi y_0^2 + \det(y')|_K^s \, dy_0 dy'; \\ Z_{21} &= [1][2] + [2]^2 q^{-1}t/[1,1] + q^{-4}tZ_2; \\ Z_3 &= [1] + q^{-1}t^2 Z_{31}, \qquad Z_{31} = \int_D |y_0^2 + \det(y)|_K^s \, dy_0 dy; \\ Z_{31} &= [1] + ([1][9] - [3]^2 q^{-4}) q^{-1}t/[1,1] + [3]^2[5,1]q^{-5}t^2/[1,1][5,2] + q^{-10}t^2 Z_0. \end{aligned}$$

At the last stage we have used Corollary 10.2.1 as in the previous case. We have only to put these together.

If we incorporate the computed integrals for $i = 2$, 3 into $(*)$, then after an elementary computation we get the following result:

Proposition 10.4.1 *If q is odd and*

$$f(x) = (a_0 b_0 - \mathrm{tr}(ab))^2 - 4(a_0 \det(b) + b_0 \det(a) + \mathrm{tr}(a^{\#} b^{\#}))$$

for $x = (a_0, b_0; a, b)$ in $X = K^2 + M_3(K)^2$, then

$$\int_{X^\circ} |f(x)|_K^s \, dx = [1][5]C(t)/[1,1][5,2][7,2][10,2],$$

in which $C(t)$ *is*

$$[5]_+ - (1 + q^{-1} + q^{-2} - q^{-6})q^{-5}t + (1 - q^{-4} - q^{-5} - q^{-6})q^{-6}t^2 + [5]_+q^{-12}t^3.$$

We recall that if C is any composition algebra over K and $X = K^2 + H_3(C)^2$, then the corresponding Freudenthal quartic $f(x)$ on X is defined in Chapter 9.5. We have just computed $Z(s)$ in one case. Actually all $Z(s)$ have been computed in [25]. If for any m, n in $\mathbb{N}$ satisfying $m \geq n$ and for variables a, t, we put

$$C_{m,n}(a,t) = (1+a^m) - (1 + a^{m-n} + a^{2m-2n} - a^{2m-n})a^{n+1}t + (1 - a^n - a^m - a^{2m-n})a^{m+1}t^2 + (1 + a^m)a^{2m+2}t^3,$$

then for $C =$ (C1), (C2), (C3), (C4) in Chaper 9.4, we have

$$\int_{X^\circ} |f(x)|_K^s \, dx = [1][3k/2+2]C_{3k/2+2,k+2}(q^{-1},t)/[1,1][k+3,2][2k+3,2][3k+4,2],$$

in which $k = \dim_K(C) \neq 1$, i.e., $k = 2$, 4, 8; if $k = 1$, then it becomes

$$[1][4][7,1]/[1,1][4,2][7,2].$$

The computation has been done uniformly. Instead of $(*)$ we have

$$[6k+8,4]Z(s) = [1][3k+4] + [1][k+2][3k/2+2][2k+2]q^{-1}t/[1,1] + c_2I_2 + c_3I_3,$$

in which

$$c_2 = q^{-(k+3)}[3k/2][3k/2+2][2k+2]/[k/2],$$
$$c_3 = q^{-(3k+4)}[k/2+1]_+[k+1]_+[3k/2+2],$$
$$I_2 = [1][k+3,1]t^2/[1,1][k+3,2],$$
$$I_3 = ([1]t^2/[1,1][k+3,2][2k+3,2])\{1 - (1 + q^{-k/2} - q^{-k-1})q^{-k/2-2}t + (1 + q^{-k/2} - q^{-k/2-1} - q^{-k-1} - q^{-3k/2-1})q^{-k/2-2}t^2 + q^{-3k-6}t^3\}$$

for $k = 2$, 4, 8. This implies the above result. Actually $Z(s)$ has been computed also in some "twisted cases." Furthermore, in the case where $k = 8$ not only $Z(s)$ but also $Z(\omega)$ was computed earlier via Weil's function $F^*(i^*)$. At any rate, by T. Kimura [34] we have

$$b_f(s) = (s+1)(s+(k+3)/2)(s+k+3/2)(s+3k/2+2)$$

for $k = 1$, 2, 4, 8.

We further mention that $Z(s)$ for the norm form has been computed in *all twisted cases*. If C is the unique unramified quadratic extension of K, i.e., the field K_2 in the notation of Chapter 11.6, the result is stated in [25]. Furthermore the norm form of any associative simple K-algebra can be handled in the same way as $\det(x)$ while every octonian K-algebra is isomorphic to the one in (C4). That leaves only the case where C is either a ramified quadratic extension of K or a quaternion K-algebra not isomorphic to $M_2(K)$. In those rather difficult cases the computation has been carried out by M. M. Robinson [46].

10.5 $Z(s)$ for the Gramian $\det({}^t xhx)$

We shall start with some observations on a quadratic map. We take an m-dimensional vector space V over any field F with $\mathrm{char}(F) \neq 2$ and a nondegenerate quadratic form Q on V. We put $X = V^n$, where $m \geq 2n$, and let $G = \mathrm{O}(Q) \times \mathrm{GL}_n(F)$ act on X, $Y = \mathrm{Sym}_n(F)$ as

$$(g, g') \cdot x = gx\,{}^t g', \qquad (g, g') \cdot y = g' \cdot y = g' y\,{}^t g'.$$

We write $x = (x_1 \dots x_n)$ with x_i in V, denote the (i, j)-entry of y by y_{ij}, and define a *quadratic map* $i_X : X \to Y$ as

$$y = i_X(x), \qquad y_{ij} = Q(x_i, x_j)$$

for $1 \leq i,\ j \leq n$. We observe that i_X is G-equivariant. We shall denote by X' the G-invariant subset of X defined by $\mathrm{rank}(x) = n$, i.e., by the condition that the column space $\langle x_1, \dots, x_n \rangle$ of x is n-dimensional. We observe that if $x' = (x'_1 \dots x'_n)$ is also in X' with $i_X(x) = i_X(x')$, then the correspondence $x_i \mapsto x'_i$ for $1 \leq i \leq n$ gives an isometry from $\langle x_1, \dots, x_n \rangle$ to $\langle x'_1, \dots, x'_n \rangle$, which extends to an element of $\mathrm{O}(Q)$ by the Witt theorem. Therefore, if $\{\eta\}$ is a complete set of representatives of $\mathrm{GL}_n(F)$-orbits in Y and if ξ is chosen arbitrary from $X' \cap i_X^{-1}(\eta)$, then the set $\{\xi\}$ forms a complete set of representatives of G-orbits in X'. In the following we shall determine the fixer G_x in G of any x in X'.

If $\mathrm{rank}(i_X(x)) = p$, then for our purpose we may assume that

$$y = i_X(x) = y_0 \oplus 0,$$

in which y_0 is in $\mathrm{Sym}_p(F)$ necessarily with $\det(y_0) \neq 0$. If we write $n = p + k$ and denote by g'_{11}, g'_{12}, g'_{21}, g'_{22} the $p \times p$, $p \times k$, $k \times p$, $k \times k$ entry matrices of g', then the fixer $\mathrm{GL}_n(F)_y$ of y in $\mathrm{GL}_n(F)$ is defined by g'_{11} in $\mathrm{GL}_p(F)$ satisfying $g'_{11} y_0\,{}^t g'_{11} = y_0$, g'_{22} in $\mathrm{GL}_k(F)$, $g'_{21} = 0$, and g'_{12} free in $M_{p,k}(F)$. We shall choose an F-basis for V depending on x. We write

$$\langle x_1, \dots, x_n \rangle = W_0 + W$$

such that $Q|W_0$ is nondegenerate, $Q|W = 0$, and W is contained in $W_0^\perp$. We then have $\dim_K(W_0) = p$ and $\dim_K(W) = k$. We know that we can find a k-dimensional subspace W' of $W_0^\perp$ such that $Q|W' = 0$ and $H = W + W'$ is hyperbolic. In that way we get an orthogonal decomposition

$$V = W_0 \oplus (W + W') \oplus W_1,$$

in which $m_1 = \dim_K(W_1)$ is equal to $m - p - 2k$, hence also to $m - n - k = m - 2n + p$. If we choose F-bases for W_0, W, W', W_1 suitably, then V can be identified with F^m and $Q(v)$ for v in F^m can be written as $(1/2)^t v h_x v$ with

$$h_x = \begin{pmatrix} h_0 & 0 & 0 & 0 \\ 0 & 0 & 1_k & 0 \\ 0 & 1_k & 0 & 0 \\ 0 & 0 & 0 & h_1 \end{pmatrix},$$

in which h_0, h_1 are respectively in $\mathrm{Sym}_p(F)$, $\mathrm{Sym}_{m_1}(F)$ and $\det(h_0)\det(h_1) \neq 0$. Since $y = {}^t x h_x x$, we also have

$$x = \begin{pmatrix} x_0 \\ 0 \end{pmatrix}, \qquad x_0 = \begin{pmatrix} x_{11} & 0 \\ x_{21} & x_{22} \end{pmatrix}, \qquad {}^t x_{11} h_0 x_{11} = y_0$$

with x_{11}, x_{22}, x_{21} respectively in $\mathrm{GL}_p(F)$, $\mathrm{GL}_k(F)$, $M_{k,p}(F)$.

We are ready to determine the fixer G_x. If (g, g') is an element of G_x, hence $gx = x\ {}^t(g')^{-1}$, then since $g'_{21} = 0$ in g' we will have

$$x_0\ {}^t(g')^{-1} x_0^{-1} = \begin{pmatrix} \alpha & 0 \\ \gamma & \delta \end{pmatrix}$$

with $\alpha = x_{11}\ {}^t(g'_{11})^{-1} x_{11}^{-1}$, etc. and

$$g = \begin{pmatrix} \alpha & 0 & g_{13} & g_{14} \\ \gamma & \delta & g_{23} & g_{24} \\ 0 & 0 & g_{33} & g_{34} \\ 0 & 0 & g_{43} & g_{44} \end{pmatrix}$$

with g_{33} in $M_k(F)$, etc. Conversely, if g is of this form and if g' is defined as above in terms of α, γ, δ and x_0, then $gx = x\ {}^t(g')^{-1}$. Furthermore the condition that g' is in $\mathrm{GL}_n(F)_y$ becomes α in $\mathrm{GL}_p(F)$ satisfying ${}^t\alpha h_0 \alpha = h_0$ and δ in $\mathrm{GL}_k(F)$. We shall examine the condition that g is in $\mathrm{O}(Q)$, i.e., ${}^t g h_x g = h_x$. We observe that if g_{14}, g_{24}, g_{34}, g_{43} are all 0, $g_{33} = {}^t\delta^{-1}$, $g_{44} = 1_{m_1}$, and

$$g_{13} = -\alpha h_0^{-1\,t}(\delta^{-1}\gamma), \qquad g_{23} = -(1/2)\gamma h_0^{-1\,t}(\delta^{-1}\gamma),$$

then ${}^t g h_x g = h_x$. Therefore, the homomorphism $G_x \to \mathrm{GL}_n(F)_y$ defined by $(g, g') \mapsto g'$ is surjective. Furthermore, if $\alpha = 1_p$, $\gamma = 0$, $\delta = 1_k$, then the condition on g becomes that g_{13}, g_{14}, g_{34} are all 0, $g_{33} = 1_k$, ${}^t g_{44} h_1 g_{44} = h_1$, and g_{23}, g_{24}, g_{43} satisfy

$$g_{23} + {}^t g_{23} + {}^t g_{43} h_1 g_{43} = 0, \qquad g_{24} + {}^t g_{43} h_1 g_{44} = 0.$$

This gives a description of the kernel K_x of $G_x \to \mathrm{GL}_n(F)_y$. In fact, if we associate quadratic forms Q_0, Q_1 respectively on F^p, F^{m_1} to h_0, h_1 as Q is associated with h_x and further if we put

$$a = (1/2)(g_{23} - {}^t g_{23}), \qquad b = g_{43}, \qquad [b, b'] = -(1/2)({}^t b h_1 b' - {}^t b' h_1 b),$$

then we get a surjective homomorphism $K_x \to \mathrm{O}(Q_1)$ as $g \mapsto g_{44}$ such that its kernel is isomorphic as $g \mapsto (b, a)$ to $M_{m_1,k}(F) \times \mathrm{Alt}_k(F)$ with the following multiplication:

$$(b, a)(b', a') = (b + b', a + a' + [b, b']).$$

We have seen such a group in the proof of Lemma 10.3.1. At any rate G_x has now been determined. We keep in mind that

$$d(Q) = (-1)^{pm_1} d(Q_0) d(Q_1)$$

up to a factor in $(F^\times)^2$.

We now take $\mathbb{F}_q$ as F, write $X'(F)$ instead of X', and choose a complete set of representatives of $G(F)$-orbits in $X'(F)$. In doing so, we shall assume that $d(Q)$ is in $(F^\times)^2$ if m is even so that, by Theorem 9.2.1, the anisotropic kernel of Q becomes 0. Then with respect to a suitable F-basis for V we can identify V with F^m so that we can write $Q(v) = (1/2)^t vhv$, in which

$$h = \begin{pmatrix} 0 & 1_n & 0 \\ 1_n & 0 & 0 \\ 0 & 0 & h' \end{pmatrix}$$

for some h'. We then have $X = M_{m,n}(F)$ and $i_X(x) = {}^t xhx$ for all x in X. We define Σ_p as in Lemma 10.3.1 and choose representatives η_p of $\mathrm{GL}_n(F)$-orbits in Σ_p of the form $\eta_p = y_0 \oplus 0$ with y_0 in $\mathrm{Sym}_p(F)$, hence $\det(y_0) \neq 0$. We keep in mind that the number of η_p is 2 for $p > 0$ and 1 for $p = 0$. If we define an element ξ_p of $M_{m,n}(F)$ as $\xi_p = {}^t(\eta_p \ 1_n \ 0)$, then ξ_p is in $X'(F)$ and $(1/2)i_X(\xi_p) = \eta_p$. Therefore, $\{\xi_p\}$ for all η_p and for $0 \leq p \leq n$ forms a complete set of representatives of $G(F)$-orbits in $X'(F)$.

We shall compute $\mathrm{card}(G(F) \cdot \xi_p)$ for each ξ_p. We have $\mathrm{card}(G(F) \cdot \xi_p) = \mathrm{card}(G)/\mathrm{card}(G_x)$ for $x = \xi_p$, in which $\mathrm{card}(G) = \mathrm{card}(\mathrm{O}(Q))\ \mathrm{card}(\mathrm{GL}_n(F))$ and G_x has been made explicit. Therefore, if we put

$$\gamma = q^{-m(m-1)/2} \cdot \mathrm{card}(\mathrm{O}(Q))$$

and define γ_0, γ_1 similarly for $\mathrm{O}(Q_0)$, $\mathrm{O}(Q_1)$, then we can easily verify that

$$q^{-mn} \cdot \mathrm{card}(G(F) \cdot \xi_p) = q^{-k(k+1)/2} \cdot \prod_{1 \leq i \leq p} [k+i] \cdot \gamma/\gamma_0\gamma_1.$$

Furthermore, since $d(Q_0)d(Q_1) = (-1)^{pm_1} d(Q)$, where $d(Q) = 1$ if m is even, up to a factor in $(F^\times)^2$, by using the formulas in Chapter 9.3 we get

$$\gamma = 2 \cdot \prod_{1 \leq 2i < m} [2i]$$

multiplied by $[m/2]$ if m is even and

$$\sum_{\eta_p} 1/\gamma_0\gamma_1 = 1/\big(2 \prod_{1 \leq 2i \leq p} [2i] \cdot \prod_{1 \leq 2i \leq m_1} [2i]\ \big)$$

multiplied by $[m/2 - k]_+$ if m, p are both even.

We now take a p-adic field with odd $q = \mathrm{card}(O_K/\pi O_K)$, define a quadratic form Q on $V = K^m$ as $Q(v) = (1/2)^t vhv$ for any h in $\mathrm{Sym}_m(O_K)$ with $\det(h)$ in $O_K^\times$, put $X = V^n = M_{m,n}(K)$ for $m \geq 2n$ and define $f(x)$ as the *Gramian* of $i_X(x) = {}^t xhx$, i.e., as

$$f(x) = \det({}^t xhx)$$

for x in X. We shall assume that $d(Q)$ is in $(O_K^\times)^2$ if m is even and compute

$$Z(s) = \int_{X^\circ} |f(x)|_K^s \, dx$$

for $\mathrm{Re}(s) > 0$. If we define an open subset $(X')^\circ$ of X° by $\mathrm{rank}(x \mod \pi) = n$, then the computation of $Z(s)$ will be reduced to that of

$$Z_0(s) = \int_{(X')^\circ} |f(x)|_K^s \, dx.$$

In fact, if we denote by I the set of all $i = (i_1, \ldots, i_n)$ in $\mathbb{Z}^n$, where $1 \le i_1 < \ldots < i_n \le m$, by $\pi_i(x)$ the determinant of the $n \times n$ submatrix of x obtained by crossing out its k-th rows for $k \ne i_1, \ldots, i_n$, and further by $h_{i,j}$ for $j = (j_1, \ldots, j_n)$ also in I the determinant of the $n \times n$ submatrix of h obtained by crossing out its k-th rows for $k \ne i_1, \ldots, i_n$ and l-th columns for $l \ne j_1, \ldots, j_n$, then we can write

$$f(x) = \det({}^t xhx) = \sum_{i,j \in I} h_{i,j} \pi_i(x) \pi_j(x).$$

Therefore, the reduction of $Z(s)$ to $Z_0(s)$ can be done by the following lemma:

Lemma 10.5.1 *We only assume that $m \ge n$ in $X = M_{m,n}(K)$ and that $f(x)$ is any homogeneous polynomial of degree d in $\pi_i(x)$ with coefficients in K. Then*

$$\int_{X^\circ} |f(x)|_K^s \, dx = 1/\prod_{1 \le k \le n} [m-k+1, d] \cdot \int_{(X')^\circ} |f(x)|_K^s \, dx.$$

We shall postpone the proof of this lemma to section 10.6 and quickly finish the computation of $Z(s)$, i.e., that of $Z_0(s)$. We shall use $\eta_p = y_0 \oplus 0$, $\xi_p = {}^t(\eta_p \ 1_n \ 0)$ for the liftings of the previous η_p, ξ_p to $\mathrm{Sym}_n(O_K)$, $(X')^\circ$ so that, e.g., $\det(y_0) \not\equiv 0 \mod \pi$ instead of $\det(y_0) \ne 0$; also we shall normalize h as before with entries in O_K this time. We observe that if we denote by x_{22} the $k \times k$ submatrix of x with its (i,j)-entries for $p < i, j \le n$ as the entries of x_{22}, then we will have

$$f(\xi_p + \pi x) = 2^n \cdot \det \begin{pmatrix} y_0 + \pi y_{11} & \pi y_{12} \\ \pi^t y_{12} & \pi y_{22} \end{pmatrix},$$

in which the entries of y_{11}, y_{12}, y_{22} are SRP's in the entries of x. We further observe that $y_{22} \equiv (1/2)(x_{22} + {}^t x_{22}) \mod \pi$ and the above determinant is equal to

$$\pi^k \det(y_0 + \pi y_{11}) \det(y_{22} - \pi^t y_{12}(y_0 + \pi y_{11})^{-1} y_{12})$$

with $y_0 + \pi y_{11}$ in $\mathrm{GL}_p(O_K)$. Therefore, we get

$$\int_{X^\circ} |f(\xi_p + \pi x)|_K^s \, dx = t^k \cdot \int_{\mathrm{Sym}_k(O_K)} |\det(y_{22})|_K^s \, dy_{22}.$$

If we put

$$c_k = \sum_{\eta_p} q^{-mn} \mathrm{card}(G(F) \cdot \bar{\xi}_p)$$

for $F = \mathbb{F}_q$ and $\bar{\xi}_p = \xi_p \mod \pi$, then by using the key lemma, the above result on c_k and Proposition 10.3.1 we get the following preliminary result:

Proposition 10.5.1 *We assume that $m \geq 2n$ in $X = M_{m,n}(K)$, denote by h an element of $\mathrm{Sym}_m(O_K)$ with $\det(h)$ in $O_K^\times$ such that $(-1)^{m(m-1)/2}\det(h)$ is in $(O_K^\times)^2$ if m is even, and put*

$$Z(s) = \int_{X^\circ} |\det({}^t xhx)|_K^s \, dx.$$

If further we write $n = p + k$ and put $m_1 = m - n - k$, then we have

$$Z(s) = 1/\prod_{1\leq i\leq n} [m-i+1,2]\cdot Z_0(s), \qquad Z_0(s) = \sum_{0\leq k\leq n} c_k t^k \cdot I_k,$$

in which

$$c_k = q^{-k(k+1)/2}\cdot \prod_{1\leq i\leq p}[k+i]\cdot \prod_{1\leq 2i<m}[2i]/\Big(\prod_{1\leq 2i\leq p}[2i]\cdot \prod_{1\leq 2i\leq m_1}[2i]\Big)$$
$$\cdot \begin{cases} [m/2]\begin{Bmatrix} [m/2-k]_+ & p \text{ even} \\ 1 & p \text{ odd}\end{Bmatrix} & m \text{ even} \\ 1 & m \text{ odd}, \end{cases}$$
$$I_k = 1/[1,1]\cdot \prod_{1\leq 2i\leq k}[2i-1]/[2i+1,2]\cdot \begin{cases} [k+1,1] & k \text{ even} \\ [k] & k \text{ odd}\end{cases}$$

for $0 \leq k \leq n$.

10.6 An integration formula

We shall prove an integration formula which implies Lemma 10.5.1. Since the formula has some generality, we shall change our notation and state it independently of that lemma. We take an arbitrary field F and denote by X the subset of $M_{m,n}(F)$, where $m \geq n$, consisting of all x with $\mathrm{rank}(x) = n$. Namely the new X is the old X'. The condition means that x can be completed by an additional $r = m - n$ columns to an element of $\mathrm{GL}_m(F)$. We define I and $\pi_i(x)$ for every i in I as in section 10.5. We order the set I lexicographically and define a map f from X to F^N, where $N = \mathrm{card}(I)$, as

$$f(x) = (\pi_i(x))_{i\in I} = {}^t(\pi_{i_0}(x)\ \dots),$$

in which $i_0 = (1, 2, \dots, n)$. We put $G = \mathrm{GL}_m(F)$, $H = \mathrm{SL}_n(F)$, and denote the $n\times n$, $n\times r$, $r\times n$, $r\times r$ submatrices of any g in G by g_{11}, g_{12}, g_{21}, g_{22}. We define a homomorphism ρ from G to $\mathrm{GL}_N(F)$ so that $f(gx) = \rho(g)f(x)$ for every g in G and x in X. The (i,j)-entry of $\rho(g)$ for $i = (i_1 \dots, i_n)$, $j = (j_1 \dots, j_n)$ is defined by g exactly in the same way as $h_{i,j}$ is defined by h in section 10.5. If we put $Y = f(X)$, then G acts on Y as $g\cdot y = \rho(g)y$ for every g in G and y in Y. We see by definition that the actions of G on X, Y are transitive and equivariant. Furthermore, if we put

$$\xi = {}^t(1_n\ 0), \qquad \eta = f(\xi) = {}^t(1\ 0\ \dots\ 0),$$

then the fixer G_ξ of ξ in G is clearly defined by $g_{11} = 1_n$, $g_{21} = 0$. We shall show that the fixer G_η of η in G is defined by g_{11} in H, $g_{21} = 0$. Since such an element is clearly in G_η, we have only to prove the converse. We shall exclude the simple case where $n = 1$. If g is in G_η, then $f(g\xi) = {}^t(1\ 0\ \dots\ 0)$ and $g\xi = {}^t({}^t g_{11}\ {}^t g_{21})$. Therefore, if we denote the k-th row of $g\xi$ by v_k for all k, then $v_1, \dots, v_n$ are the n rows of g_{11}, and $\det(g_{11}) = 1$. In particular, they are linearly independent, hence $v_k = c_1 v_1 + \dots + c_n v_n$ with $c_1, \dots, c_n$ in F depending on k. If we take $k > n$ and put $i = (1, \dots, j-1, j+1, \dots, n, k)$ for any $1 \le j \le n$, then $\pi_i(g\xi) = (-1)^{n-j} c_j = 0$, hence $c_j = 0$, and hence $g_{21} = 0$.

We shall derive two consequences from the above information on G_ξ, G_η. Firstly for every x in X we have $f^{-1}(f(x)) = xH$. Since xH is clearly contained in $f^{-1}(f(x))$, we shall prove the converse. We can write $x = g\xi$ and any x' in $f^{-1}(f(x))$ as $gg'\xi$ for some g, g' in G. Then $gg' \cdot \eta = g \cdot \eta$, hence $g' \cdot \eta = \eta$. As we have seen, this implies that $(g')_{11}$ is in H, $(g')_{21} = 0$, hence

$$x' = gg'\xi = g\xi(g')_{11} = x(g')_{11}.$$

Secondly, if $F = \mathbb{F}_q$, then by Chapter 9.3 we have

$$\mathrm{card}(X(F)) = \mathrm{card}(G(F))/\mathrm{card}(G_\xi(F)) = q^{mn} \cdot \prod_{1 \le k \le n} [m-k+1]$$

while $\mathrm{card}(Y(F)) = \mathrm{card}(X(F))/\mathrm{card}(\mathrm{SL}_n(F))$.

We now take a p-adic field K as F. Then G, H become locally compact groups and X is a locally compact space because they are either open or closed in locally compact spaces. We shall show that Y is also locally compact. Since the action of G on Y is bicontinuous and transitive, it will be enough to show that Y contains a compact open subset. If we put $V = Y \cap (O_K^\times \times O_K^{N-1})$, then V is an open subset of Y. We shall show that V is compact. If y is in V and x_1 is the top $n \times n$ submatrix of any x in $f^{-1}(y)$, then $\det(x_1) = y_{i_\circ}$ is in $O_K^\times$, hence x_1 is in $\mathrm{GL}_n(K)$, and $y = f(xx_1^{-1})y_{i_\circ}$. If we denote the k-th row of xx_1^{-1} by v_k for all k, then $v_k = c_1 v_1 + \dots + c_n v_n$ with the j-th entry of v_k as c_j for $1 \le j \le n$. Furthermore, if we put $i = (1, \dots, j-1, j+1, \dots, n, k)$, then

$$y_i = \pi_i(xx_1^{-1})y_{i_\circ} = (-1)^{n-j} c_j y_{i_\circ}$$

with $y_{i_\circ}$ in $O_K^\times$ and y_i in O_K, hence c_j is in O_K. Therefore, xx_1^{-1} with 1_n as its top $n \times n$ submatrix is in $M_{m,n}(O_K)$, hence

$$V = f\begin{pmatrix} 1_n \\ M_{r,n}(O_K) \end{pmatrix} O_K^\times.$$

Since $O_K^\times$, O_K are compact and f is continuous, we see that V is compact.

Once we know that X, Y are locally compact, then by Lemma 7.3.1 we can identify X, Y respectively with G/G_ξ, G/G_η under $g \mapsto x = g\xi$, $g \mapsto y = g \cdot \eta$. We shall denote by X° the compact open subset of X consisting of all x in $M_{m,n}(O_K)$ such that $\mathrm{rank}(x \mod \pi) = n$, i.e., with $\pi_i(x)$ in $O_K^\times$ for some i. The condition

means that x can be considered as the left $m \times n$ submatrix of an element of $G(O_K) = \mathrm{GL}_m(O_K)$. If we put $Y^\circ = f(X^\circ)$, then $G(O_K)$ acts transitively and equivariantly on X°, Y°.

We shall introduce relatively invariant measures on the homogeneous spaces X, Y. We shall first determine the modules of G, G_ξ, G_η by using Lemma 7.4.2. We take any p and denote by μ_p the normalized Haar measure on K^p and on its open subsets as before. If we put $G_p = \mathrm{GL}_p(K)$, $H_p = \mathrm{SL}_p(K)$ so that $G = G_m$, $H = H_n$, then their modules are 1. In fact,

$$dg = |\det(g)|_K^{-p}\ \mu_{p^2}(g)$$

gives a Haar measure on G_p and $d(gg_0) = dg$ for every g_0 in G_p, hence $\Delta_{G_p} = 1$. Since the homogeneous space G_p/H_p is a group, in fact the group $G_1 = K^\times$, it has an invariant measure. Therefore, by Proposition 7.2.1, we have $\Delta_{G_p}|H_p = \Delta_{H_p}$, hence $\Delta_{H_p} = 1$. If g is any element of G_ξ, hence $g_{11} = 1_n$, $g_{21} = 0$, then

$$dg = \mu_{nr}(g_{12}) \cdot |\det(g_{22})|_K^{-r}\ \mu_{r^2}(g_{22})$$

gives a Haar measure on G_ξ and $d(gg_0) = |\det(g_0)|_K^n dg$ for every g_0 in G_ξ, hence $\Delta_{G_\xi}(g) = |\det(g)|_K^n$. If g is an element of G_η, hence g_{11} is in H, $g_{21} = 0$, and if for a moment μ_H denotes any Haar measure on H, then

$$dg = \mu_H(g_{11}) \cdot \mu_{nr}(g_{12}) \cdot |\det(g_{22})|_K^{-r} \mu_{r^2}(g_{22})$$

gives a Haar measure on G_η and $d(gg_0) = |\det(g_0)|_K^n dg$ for every g_0 in G_η, hence $\Delta_{G_\eta}(g) = |\det(g)|_K^n$.

The above information about the modules on G, G_ξ, G_η implies, in view of Proposition 7.2.1, that X, Y have measures μ_X, $\mu_Y \neq 0$ satisfying

$$\mu_X(gx) = |\det(g)|_K^n\ \mu_X(x), \qquad \mu_Y(g \cdot y) = |\det(g)|_K^n\ \mu_Y(y)$$

for every g in G. Actually, the restriction of μ_{mn} on $M_{m,n}(K)$ to its open subset X is such a measure μ_X and we simply take $\mu_X = \mu_{mn}|X$. Furthermore, we normalize μ_H as

$$\mu_H(H(O_K)) = q^{-(n^2-1)}\mathrm{card}(H(F)) = \prod_{1<k\leq n} [k],$$

in which $H(O_K) = \mathrm{SL}_n(O_K)$ and $F = \mathbb{F}_q$, and μ_Y as

$$\mu_Y(Y^\circ) = \mu_X(X^\circ)/\mu_H(H(O_K)).$$

We shall show that

$$\mu_X(X^\circ) = \prod_{1\leq k\leq n} [m-k+1].$$

In general, for every $e = (e_1, \ldots, e_n)$ in $\mathbb{N}^n$ we denote by $E(e)$ the union of all $G(O_K)x$ such that the upper $n \times n$ submatrix of x is an upper-triangular matrix in $M_n(O_K)$ with $\pi^{e_1}, \ \ldots\ , \pi^{e_n}$ as its diagonal entries and the lower $r \times n$ submatrix of x is 0. If $x^* = gx$ for some g in $G(O_K)$ has a similar form, then we see that

the upper $n \times n$ submatrix of x^* has the same diagonal entries as x. Therefore, $X_0 = X \cap M_{m,n}(O_K)$ becomes the disjoint union of all compact open subsets $E(e)$. Furthermore, $E(0) = G(O_K)\xi = X^\circ$. We shall show that

$$\mu_X(E(e)) = \prod_{1 \le k \le n} [m-k+1] q^{-(m-k+1)e_k}.$$

We denote the first column of any x in $M_{m,n}(K)$ by x_1. If x is in $E(e)$, then $x_1 = \pi^{e_1} g \varepsilon_1$ for some g in $G(O_K)$ and $\varepsilon_1 = {}^t(1\ 0\ \dots\ 0)$. Furthermore, suppose that $x_1 = \pi^{e_1}\varepsilon_1$ for some x in $M_{m,n}(O_K)$ and denote by x' the $(m-1) \times (n-1)$ submatrix of x obtained by crossing out its first row and column. Then we see that x is in $E(e)$ if and only if x' is in $E(e')$ for $e' = (e_2, \dots, e_n)$ relative to X' defined similarly as X for $m-1$, $n-1$ instead of m, n. Therefore, by an induction on n we get

$$\mu_X(E(e)) = [m] q^{-me_1} \cdot \mu_{X'}(E(e')) = \prod_{1 \le k \le n} [m-k+1] q^{-(m-k+1)e_k}.$$

We are ready to prove the following lemma.

Lemma 10.6.1 *If Φ is in $\mathcal{D}(X)$, i.e., if Φ is a $\mathbb{C}$-valued locally constant function on X with compact support, then*

$$\int_X \Phi(x)\mu_X(x) = \int_Y \Big\{ \int_H \Phi(xh)\mu_H(h) \Big\} \mu_Y(f(x)).$$

Proof. By Proposition 7.2.1 we have

$$\begin{aligned} \int_G \varphi(g) |\det(g)|_K^n \, dg &= \int_X \Big\{ \int_{G_\xi} \varphi(gh)\, dk \Big\} \mu_X(g\xi) \\ &= \int_Y \Big\{ \int_{G_\eta} \varphi(gk')\, dk' \Big\} \mu_Y(g \cdot \eta) \end{aligned}$$

for every φ in $\mathcal{D}(G)$ provided that the Haar measures dg, dk, dk' respectively on G, G_ξ, G_η are suitably normalized. If we put

$$\Phi(x) = \int_{G_\xi} \varphi(gk)\, dk,$$

where $x = g\xi$, then we know, cf. loc. cit., that the correspondence $\varphi \mapsto \Phi$ gives a $\mathbb{C}$-linear surjection from $\mathcal{D}(G)$ to $\mathcal{D}(X)$. Furthermore, if we put $h = (k')_{11}$, then we have $gk'k\xi = xh$. Therefore, by Proposition 7.2.1 we have

$$\int_{G_\eta} \varphi(gk')\, dk' = \int_H \Big\{ \int_{G_\xi} \varphi(gk'k)\, dk \Big\} \mu_H(h) = \int_H \Phi(xh)\mu_H(h).$$

By putting these together we get the formula in the lemma up to a factor in $\mathbb{R}_+^\times$ independent of Φ. We shall show that this factor is 1.

If x_0 is in $xH \cap X^\circ$ for some x in X, then $xH \cap X^\circ = x_0H \cap X^\circ$ and some $n \times n$ submatrix say x_i of x_0 is in $\mathrm{GL}_n(O_K)$. Therefore, if x_0h for some h in H is in X°, then x_ih is in $M_n(O_K)$,hence h is in $M_n(O_K)$, and hence in $\mathrm{SL}_n(O_K) = H(O_K)$. We have thus shown that $xH \cap X^\circ \neq \emptyset$ implies $xH \cap X^\circ = x_0H(O_K)$ for some x_0 in X° and $x_0H \cap X^\circ = x_0H(O_K)$ for every x_0 in X°. Therefore, if in the integration formula we take the characteristic function of X° as Φ, then its RHS becomes $\mu_H(H(O_K))\mu_Y(Y^\circ)$. Since the LHS is $\mu_X(X^\circ)$, the constant factor is 1.

We know that we can replace Φ in the above lemma by any continuous integrable function on X. Therefore, if Φ, φ are continuous functions respectively on X, Y such that $\Phi(x)\varphi(f(x))$ is integrable on X, then the lemma implies

$$\int_X \varphi(f(x))\Phi(x)\mu_X(x) = \int_Y \varphi(y)\Big\{\int_H \Phi(xh)\mu_H(h)\Big\}\mu_Y(y),$$

in which $y = f(x)$. If we take the characteristic function of X° as Φ, then the last part of the proof of Lemma 10.6.1 implies

$$\int_{X^\circ} \varphi(f(x))\mu_X(x) = \mu_H(H(O_K)) \int_{Y^\circ} \varphi(y)\mu_Y(y).$$

Before we proceed further, we make the following remark. The relatively invariant measure μ_Y on Y remains relatively invariant under the normalizer of $\rho(G)$ in $\mathrm{GL}_N(K)$. In particular, if c is in $K^\times$, then $\mu_Y(cy)$ differs from $\mu_Y(y)$ by a factor in $\mathbb{R}_+^\times$ independent of y. By Lemma 7.2.1 this factor gives a continuous homomorphism from $K^\times$ to $\mathbb{R}_+^\times$. Therefore, it is of the form $|c|_K^\sigma$ for some σ in $\mathbb{R}$ independent of c. On the other hand, if we put $g = \pi 1_m$, then $\rho(g)y = \pi^n y$ and $|\det(g)|_K^n = q^{-mn}$, hence $\mu_Y(\pi^n y) = q^{-mn}\mu_Y(y)$. By putting these together we see that $\sigma = m$, hence

$$\mu_Y(cy) = |c|_K^m \mu_Y(y)$$

for every c in $K^\times$.

We now express Y as the disjoint union of $\pi^k Y^\circ$ for all k in $\mathbb{Z}$. Then by using the above remark we can rewrite the integration formula as

$$(*) \qquad \int_X \varphi(f(x))\Phi(x)\mu_X(x) = \sum_{k\in\mathbb{Z}} q^{-mk} \cdot \int_{Y^\circ} \varphi(\pi^k y)\Big\{\int_H \Phi(xh)\mu_H(h)\Big\}\mu_Y(y),$$

in which $f(x) = \pi^k y$. In particular, if we take the characteristic function χ of $X_0 = X \cap M_{m,n}(O_K)$ as Φ, then $(*)$ becomes

$$\int_{X_0} \varphi(f(x))\mu_X(x) = \sum_{k\geq 0} q^{-mk} \cdot \int_{Y^\circ} \varphi(\pi^k y) \left\{\int_H \chi(xh)\mu_H(h)\right\} \mu_Y(y)$$

in which $f(x) = \pi^k y$. The above $\{\cdot\}$ can be made explicit, e.g., as follows: We observe that it is invariant under $x \mapsto gx$ for any g in $G(O_K)$, hence it is independent of y. We take any k from $\mathbb{N}$ and in $(*)$ we replace φ by the constant 1 and Φ by the characteristic function of the subset of X_0 defined by the condition that $f(x)$

is in $\pi^k Y^\circ$. We observe that this subset is the disjoint union of $E(e)$ for all e in $\mathbb{N}^n$ satisfying $|e| = e_1 + \ldots + e_n = k$. Therefore we get

$$\sum_{|e|=k} \mu_X(E(e)) = q^{-mk} \cdot \{\ \cdot\ \} \cdot \mu_Y(Y^\circ).$$

We put all these together and use the fact that $M_{m,n}(O_K)\backslash X_0$ is of measure 0 by $\mu_X(X_0) = 1$. In that way we get the following proposition:

Proposition 10.6.1 *Let φ denote any $\mathbb{C}$-valued continuous function on the image of $M_{m,n}(K)$ under $x \mapsto (\pi_i(x))$ and $U_{m,n}$ the compact open subset of $M_{m,n}(O_K)$ defined by rank$(x \mod \pi) = n$. Then we have*

$$\int_{M_{m,n}(O_K)} \varphi(f(x))\ dx = \sum_{e\in\mathbb{N}^n} \Big(\prod_{1\le k\le n} q^{-(m-k+1)e_k} \Big) \int_{U_{m,n}} \varphi(\pi^{|e|} f(x))\ dx,$$

in which $e = (e_1, \ldots, e_n)$ and $|e| = e_1 + \ldots + e_n$.

Now Lemma 10.5.1 follows from Proposition 10.6.1. We have only to denote $f(x)$ in Proposition 10.6.1 say by $p(x)$, express $f(x)$ in Lemma 10.5.1 by $h(p(x))$ with $h(y)$ homogeneous of degree d, and take $\varphi(y) = |h(y)|_K^s$.

10.7 $Z(s)$ for $\det({}^t xhx)$ in product forms

We shall go back to Proposition 10.5.1 and convert $Z_0(s)$, hence also $Z(s)$, into a product. The product form of $Z_0(s)$ depends on m, n mod 2. We recall that

$$Z_0(s) = \sum_{0\le k\le n} c_k t^k \cdot I_k,$$

in which c_k and I_k are as in that proposition. We shall make some preliminary computation. We replace k above by $2k$ and $2k+1$, and put the two terms for the same new k together. If n is odd, then the summation in the new k will become for $0 \le k \le (n-1)/2$. However, if n is even, the summation will become for $0 \le k \le n/2 - 1$ and an extra term, i.e., $c_n t^n I_n$. It turns out that this extra term is obtained from the combined general term by substituting $n/2$ for k. At any rate, the result can be stated more or less uniformly as follows:

$$Z_0(s) = A/[1,1] \cdot \prod_{1\le i\le n} [i] \cdot Z_1(s),$$

$$Z_1(s) = \sum_{0\le 2k\le n} A_k q^{-k(2k+1)} t^{2k} \cdot \Big\{ \prod_{m-n-2k<2i<m} [2i] / \Big(\prod_{1\le 2i\le n-2k} [2i] \cdot \prod_{1\le i\le k} [2i][2i+1,2] \Big) \Big\},$$

in which

$$A = \begin{cases} [m/2] & n \text{ even} \\ [m/2][m/2,1]_+ & n \text{ odd} \end{cases} \quad m \text{ even}$$
$$\begin{cases} [n+1,1] & n \text{ even} \\ [m-n+1,1] & n \text{ odd} \end{cases} \quad m \text{ odd}$$

while $A_k = 1$ except for the case where m, n are both even, and in that case

$$A_k = [m/2-2k]_+[2k+1,1] + [m-n-2k][n-2k]q^{-2k-1}t.$$

The verifications are similar and straightforward.

We shall convert $Z_1(s)$ into a product. The conversion will be made by using (G2) and (G3) in Chapter 9.6. We recall that

$$(G2) \qquad \sum_{0\le k\le n} F_{m-k,k}(a)F_{k,n-k}(a,t)a^{k^2}t^k = F_{m,n}(a,t),$$

$$(G3) \qquad \sum_{0\le k\le n} F_{m-k,k}(a)F_{k,n-k}(a,t)a^{k^2-k}\ t^k = F_{m-1,n}(a,t) + tF_{m,n-1}(a,t),$$

in which

$$F_{m,n}(a,t) = \prod_{1\le i\le n}(1-a^{m+i}t)/(1-a^i), \qquad F_{m,n}(a) = F_{m,n}(a,1)$$

for m, n in $\mathbb{Z}$ with the understanding that $F_{m,n}(a,t) = 0$ for $n < 0$. In all cases, we replace q^{-2} by a and $q^{-1}t^2$ by t. More precisely, we shall be replacing the variables a, t in (G2) and (G3) by q^{-2}, $q^{-1}t^2$.

If m, n are not both even, hence $A_k = 1$, we replace them respectively by

$$\begin{cases} 2(m+n+1), & 2n+1 & m \text{ even}, & n \text{ odd} \\ 2(m+n)+1, & 2n & m \text{ odd}, & n \text{ even} \\ 2(m+n)+1, & 2n+1 & m \text{ odd}, & n \text{ odd}. \end{cases}$$

Then in all three cases we get

$$\begin{aligned} Z_1(s) &= \prod_{1\le i\le n}(1-a^{m+i})/(1-a^it) \cdot \sum_{0\le k\le n} F_{m-k,k}(a)F_{k,n-k}(a,t)a^{k^2}t^k \\ &= \prod_{1\le i\le n}(1-a^{m+i})(1-a^{m+i}t)/(1-a^i)(1-a^it), \end{aligned}$$

this by (G2). Therefore in the original notation we have

$$Z_1(s) = 1/\prod_{1\le 2i\le n}[2i][2i+1,2] \cdot \begin{cases} \prod_{1\le 2i\le n}[m-2i][m-2i+1,2] m \text{ even},\ n \text{ odd} \\ \prod_{1\le 2i\le n}[m-2i+1][m-2i+2,2] \quad m \text{ odd}. \end{cases}$$

In the case where m, n are both even, we write

$$A_k = B_1 + B_2\ q^{2k},$$

in which B_1, B_2 are free from k, i.e.,

$$B_1 = 1 - (1 + q^{-m/2+n} + q^{-m+2n})q^{-n-1}t, \qquad B_2 = [m/2+1,1]_+ q^{-m/2},$$

and split $Z_1(s)$ as

$$Z_1(s) = B_1 \cdot Z_1'(s) + B_2 \cdot Z_2(s).$$

If we replace m, n respectively by $2(m+n)$, $2n$, then in the same way as in the previous cases we get

$$Z_1'(s) = 1/(1-a^{m+n}) \cdot \prod_{1\le i\le n} (1-a^{m+i})(1-a^{m+i}t)/(1-a^i)(1-a^it).$$

As for $Z_2(s)$, we have

$$\begin{aligned} Z_2(s) = 1/(1-a^{m+n}) &\cdot \prod_{1\le i\le n} (1-a^{m+i})/(1-a^it) \\ &\cdot \sum_{0\le k\le n} F_{m-k,k}(a)F_{k,n-k}(a,t)a^{k^2-k}\ t^k, \end{aligned}$$

and the sum over $0 \le k \le n$ is equal to $F_{m-1,n}(a,t) + tF_{m,n-1}(a,t)$ by (G3). Therefore, if in the original notation we put

$$C = [m+1,2]B_1 + ([m-n+1,2] + [n]q^{-1}t^2)B_2,$$

then we have

$$Z_1(s) = C/[n][n+1,2] \cdot \prod_{1\le i<n/2} [m-2i][m-2i+1,2]/[2i][2i+1,2].$$

Furthermore if we replace B_1, B_2 by their expressions in terms of q^{-1}, t, then we get $C = C_{m/2,n}(q^{-1},t)$ for the $C_{m,n}(a,t)$ in section 10.4, i.e.,

$$\begin{aligned} C_{m,n}(a,t) = (1+a^m) &- (1 + a^{m-n} + a^{2m-2n} - a^{2m-n})a^{n+1}t \\ &+ (1 - a^n - a^m - a^{2m-n})a^{m+1}t^2 + (1+a^m)a^{2m+2}t^3 \end{aligned}$$

for $m \ge n$. We have thus converted $Z_0(s)$ in Proposition 10.5.1 into the following definitive form:

Proposition 10.7.1 *If m is even, then*

$$\begin{aligned} Z_0(s) = [m/2] &\prod_{1\le i\le n} [i] \Big/ \Big([1,1] \cdot \prod_{1\le 2i\le n} [2i][2i+1,2] \Big) \\ &\cdot \prod_{1\le 2i\le n} [m-2i][m-2i+1,2] \begin{cases} C_{m/2,n}(q^{-1},t)/[m-n][m-n+1,2] & n \text{ even} \\ [m/2,1]_+ & n \text{ odd} \end{cases} \end{aligned}$$

and if m is odd, then

$$Z_0(s) = \prod_{1\le i\le n}[i]/\ (\ [1,1]\cdot \prod_{1\le 2i\le n}[2i][2i+1,2]\ )$$
$$\cdot \prod_{1\le 2i\le n}[m-2i+1][m-2i+2,2] \begin{cases} [n+1,1] & n \text{ even} \\ [m-n+1,1] & n \text{ odd.} \end{cases}$$

We have assumed that $(-1)^{m(m-1)/2}\det(h)$ is in $(O_K^\times)^2$ in the case where m is even. The fact is that if it is in $O_K\backslash(O_K^\times)^2$, then we have only to replace all $q^{-m/2}$ in the above formulas by $-q^{-m/2}$. Propositions 10.5.1 and 10.7.1 are in Part I of [29]. We recall that we have seen the cubic polynomial $C_{m,n}(a,t)$ in t for $(m,n)=(5,4)$ in Proposition 10.4.1, i.e., in the $Z(s)$ for a Freudenthal quartic $f(x)$. We have mentioned there with a reference that $C_{m,n}(a,t)$ for $(m,n)=(8,6)$, $(14,10)$ also appear in the $Z(s)$ for other Freudenthal quartics. Although $C_{m,n}(a,t)$ is a strange polynomial, this fact can be expected because Freudenthal quartics are similar. We have now seen that $C_{m,n}(a,t)$ also appears in the $Z(s)$ for the Gramian $\det({}^txhx)$, in fact only in a certain case as stated in Proposition 10.7.1. This is a mystery for us because we fail to see any similarity between Freudenthal quartics and the Gramian. At any rate, $C_{m,n}(a,t)$ has the following formal properties:

$$\begin{aligned} C_{m,n}(a^{-1},t^{-1}) &= a^{-3m-2}t^{-3}C_{m,n}(a,t), \\ C_{m,n}(a,0) &= 1+a^m, \\ C_{m,n}(a,1) &= (1+a^m)(1-a^{n+1})(1-a^{2m-n+1}), \\ C_{m,n}(a,a^{-1}) &= (1+a^{m-1})(1-a^n)(1-a^{2m-n}). \end{aligned}$$

We can easily verify the fact that $C_{m,n}(a,t)$ is the only element of $\mathbb{Q}(a)[t]$ with these properties. Furthermore, we can show that $C_{m,n}(a,t)$ is irreducible in $\mathbb{C}(a)[t]$ for $n>0$ while clearly

$$C_{m,0}(a,t) = (1+a^m)(1-at)(1-a^{2m+1}t^2).$$

We also mention that $b_f(s)$ for $f(x)=\det({}^txhx)$ was computed as an example of their general theory in a joint paper [50] by M. Sato, M. Kashiwara, T. Kimura, and T. Oshima. The result is

$$b_f(s) = \prod_{1\le k\le n}(s+(k+1)/2)(s+(m-k+1)/2).$$

We observe that, in all examples which we have computed or mentioned, the real parts of the poles of $Z(s)$ for $f(x)$ are the zeros of $b_f(s)$ with the order of each pole at most equal to the order of the corresponding zero. As we have emphasized in the Introduction, to convert this experimental fact into a theorem is an open problem. As we have also mentioned in the Introduction, without the information about the orders this has been proved by T. Kimura, F. Sato, and X.-W. Zhu [35] in the case where $f(x)$ is the basic relative invariant of an irreducible regular prehomogeneous

vector space. In their proof Theorem 8.5.1 and a theorem of M. Sato play key roles. Also in the case where the number of variables in $f(x)$ is 2 and in cases of some generality, it has been proved by F. Loeser [37], [38].

Now, in spite of the complexity of the expression of $Z(s)$ for the Gramian $f(x) = \det({}^t xhx)$, it has remarkably simple properties. Firstly, if we denote by $\deg_t(Z(s))$ the degree of $Z(s)$ as a rational function of t, then we have

$$\deg_t(Z(s)) = -2n = -\deg(f).$$

If $f(x)$ is a Freudenthal quartic, then we also have

$$\deg_t(Z(s)) = -4 = -\deg(f).$$

If we examine other examples of $Z(s)$, then we will find that the above property is shared by all $Z(s)$ provided that $f(x)$ is homogeneous and, e.g., non-zero coefficients of $f(x)$ are all units of $O_K^\times$. Secondly, the coefficients of the expressions of $Z(s)$ as a rational function of $a = q^{-1}$ and t for $f(x) = \det({}^t xhx)$ are numerical constants independent of K. Therefore, the process of replacing a, t by a^{-1}, t^{-1}, i.e., q by q^{-1}, makes sense, and we have

$$Z(s)|_{q\mapsto q^{-1}} = t^{2n} Z(s) = t^{\deg(f)} Z(s).$$

If $f(x)$ is a Fredenthal quartic, then we similarly have

$$Z(s)|_{q\mapsto q^{-1}} = t^4 Z(s) = t^{\deg(f)} Z(s).$$

If we examine other examples for which the process "$q \mapsto q^{-1}$" makes sense, we will find that the above property is shared by all $Z(s)$ provided that $f(x)$ satisfies the homogeneity condition, etc. As we have mentioned in the Introduction, we proposed precisely formulated conjectures on the above properties of $Z(s)$ in [25], [29] and now they have been settled, hence the conjectures have become theorems, by J. Denef [9] and J. Denef and D. Meuser [10]. We shall explain the way they proved their theorems in the next and last chapter.

https://doi.org/10.1090/amsip/014/11

Chapter 11

Theorems of Denef and Meuser

11.1 Regular local rings

We have not yet made any explicit use of algebraic varieties. We shall now try to explain some fragments of algebraic geometry to state Hironaka's desingularization theorem in an algebraic form and a theorem on Weil's zeta functions over finite fields so that the readers can fully appreciate the proofs by Denef and Meuser of their theorems which depend heavily on those theorems. We shall go back to Chapter 1.2 and start with some properties of regular local rings.

We take a local ring A, i.e., a noetherian ring $A \neq 0$ in which the set of all nonunits forms a maximal ideal $\mathfrak{m}$. It is the same thing to say that A is a noetherian ring with only one maximal ideal $\mathfrak{m}$. We know by Corollary 1.2.1 that the dimension of $\mathfrak{m}/\mathfrak{m}^2$ as a vector space over $A/\mathfrak{m}$ gives the smallest number of generators of $\mathfrak{m}$ as an A-module. Since that will be sufficient for our purpose, we shall assume that A contains a field K satisfying $A = K + \mathfrak{m}$ and identify K with $A/\mathfrak{m}$. We know by Theorem 1.2.2 that $\mathfrak{m}^0 = A,\ \mathfrak{m},\ \mathfrak{m}^2, \ldots$ form a decreasing sequence of ideals of A with 0 as their intersection. We put $G_r(A) = \mathfrak{m}^r/\mathfrak{m}^{r+1}$ and denote by $G(A)$ the direct sum of $G_0(A) = K,\ G_1(A),\ G_2(A), \ldots$. We observe that every $G_r(A)$ is a vector space over K and $G(A)$ becomes a graded K-algebra. Furthermore, if we put $\dim_K(\mathfrak{m}/\mathfrak{m}^2) = n$ and if we introduce a polynomial ring $K[x] = K[x_1, \ldots, x_n]$, where $x_1, \ldots, x_n$ are variables, then we can define a surjective homomorphism from the graded K-algebra $K[x]$ to $G(A)$ as follows. We write $\mathfrak{m} = Aa_1 + \ldots + Aa_n$ and denote the image of a_i in $G_1(A)$ by y_i for $1 \leq i \leq n$. Then $G_1(A) = Ky_1 + \ldots + Ky_n$, where $y_1, \ldots, y_n$ are linearly independent over K, and

$$G_r(A) = \sum_{|e|=r} Ky_1^{e_1} \ldots y_n^{e_n},$$

in which $e = (e_1, \ldots, e_n)$ is in $\mathbb{N}^n$ and $|e| = e_1 + \ldots + e_n$, for all r. Therefore, if we define a K-linear bijection from $K[x]_1$ to $G_1(A)$ as $x_i \mapsto y_i$ for $1 \leq i \leq n$, then it uniquely extends to a surjective K-algebra homomorphism from $K[x]$ to $G(A)$ mapping $K[x]_r$ to $G_r(A)$ for all r. If we denote the kernel of the above homomorphism by $\mathfrak{a}$, then $\mathfrak{a}$ is a homogeneous ideal of $K[x]$ and $K[x]/\mathfrak{a}$ becomes isomorphic

to $G(A)$ as graded K-algebras. Therefore, if we denote Hilbert's characteristic function of any finitely generated $K[x]$-module M by $\chi(M,t)$ as in Theorem 1.3.3, then we will have

$$\dim_K(A/\mathfrak{m}^{r+1}) = \sum_{i\le r} \dim_K(G_i(A)) = \chi(G(A),r)$$

for all large r. After P. Samuel [47] we call $d = \deg(\chi(G(A),t))$ the *dimension* of A and write $\dim(A) = d$. We observe that

$$\chi(G(A),t) = \chi(K[x],t) - \chi(\mathfrak{a},t) = \binom{t+n}{n} - \chi(\mathfrak{a},t)$$

and that, by the remark after Theorem 1.3.3, we have

$$\deg\left(\chi(\mathfrak{a},t) - \binom{t}{n}\right) < n$$

if $\mathfrak{a} \neq 0$. Therefore, we get $d \le n$ with the equality if and only if $\mathfrak{a} = 0$. We shall summarize the above observations as follows:

Proposition 11.1.1 *Let A denote a local ring with $\mathfrak{m}$ as its maximal ideal such that A contains a field K satisfying $A = K + \mathfrak{m}$ and $G(A)$ the graded K-algebra with $G_r(A) = \mathfrak{m}^r/\mathfrak{m}^{r+1}$ for all r. Then there exists a polynomial $\chi(t)$ satisfying*

$$\dim_K(A/\mathfrak{m}^{r+1}) = \sum_{i\le r} \dim_K(G_i(A)) = \chi(r)$$

for all large r. If we put

$$n = \dim_K(\mathfrak{m}/\mathfrak{m}^2), \qquad d = \deg(\chi(t)) = \dim(A),$$

then $d \le n$. Furthermore, we have $d = n$ if and only if $G(A)$ is isomorphic to a polynomial ring $K[x_1,\dots,x_n]$ as graded K-algebras.

We call A a *regular local ring* if $d = n$. In that case, A is an integral domain. In fact, if a, b are elements of A both different from 0, their images in $G_i(A)$, $G_j(A)$ for some i, j are not 0, hence the image of ab in $G_{i+j}(A)$ is not 0, and hence $ab \neq 0$.

Proposition 11.1.2 *Suppose that A is a regular local ring with $\dim(A) = n$, express its maximal ideal $\mathfrak{m}$ as $\mathfrak{m} = Aa_1 + \ldots + Aa_n$, and put*

$$\mathfrak{p} = Aa_1 + \ldots + Aa_p$$

for $0 \le p \le n$. Then $A/\mathfrak{p}$ is also a regular local ring, hence $\mathfrak{p}$ is a prime ideal of A, and $\dim(A/\mathfrak{p}) = n - p$.

Proof. Since the local ring A is regular, every a in A gives rise to a unique sequence $f_0(x),\ f_1(x),\ f_2(x),\dots$ with $f_i(x)$ in $K[x]_i$ satisfying

$$a \equiv \sum_{i\le r} f_i(a) \mod \mathfrak{m}^{r+1},$$

in which $f_i(a) = f_i(a_1, \dots, a_n)$ for all r. We put $\mathfrak{q} = Aa_{p+1} + \dots + Aa_n$ so that we get $\mathfrak{m} = \mathfrak{p} + \mathfrak{q}$. Since $A/\mathfrak{p}$ has $\mathfrak{m}/\mathfrak{p}$ as its unique maximal ideal, it is a local ring. Therefore, we have only to show that $G_r(A/\mathfrak{p})$ is K-isomorphic to $K[x_{p+1}, \dots, x_n]_r$ under the correspondence $a \mapsto f_r(x)$. We have

$$G_r(A/\mathfrak{p}) = (\mathfrak{m}/\mathfrak{p})^r/(\mathfrak{m}/\mathfrak{p})^{r+1} = \mathfrak{q}^r/(\mathfrak{q}^r \cap (\mathfrak{p} + \mathfrak{q}^{r+1})),$$

in which $\mathfrak{p} + \mathfrak{q}^{r+1} = \mathfrak{p} + \mathfrak{m}^{r+1}$. We observe that an element a of A is in $\mathfrak{q}^r$ if and only if $f_i(x) = 0$ for $i < r$, $f_r(x)$ is in $k[x_{p+1}, \dots x_n]_r$, and $f_i(x)$ for $i > r$ is of degree at least r in $x_{p+1}, \dots, x_n$; that a is in $\mathfrak{p} + \mathfrak{m}^{r+1}$ if and only if $f_i(x)$ is at least of degree 1 in $x_1, \dots, x_p$ for $0 \leq i \leq r$. Therefore, the additional condition for a in $\mathfrak{q}^r$ to be in $\mathfrak{p} + \mathfrak{m}^{r+1}$ is simply $f_r(x) = 0$, hence $G_r(A/\mathfrak{p})$ is K-isomorphic to $K[x_{p+1}, \dots, x_n]_r$ as $a \mapsto f_r(x)$.

Theorem 11.1.1 *Let $K[x] = K[x_1, \dots, x_n]$ denote the ring of polynomials in n variables $x_1, \dots, x_n$ with coefficients in a field K, $a = (a_1, \dots, a_n)$ an element of K^n, and $f_1(x), \dots, f_p(x)$ elements of $K[x]$ satisfying $f_i(a) = 0$ for all i such that rank$(J(a)) = p$ for the $p \times n$ matrix $J(x)$ with $\partial f_i/\partial x_j$ as its (i, j)-entry for $1 \leq i \leq p$, $1 \leq j \leq n$; let further S denote the set of all $g(x)$ in $K[x]$ satisfying $g(a) \neq 0$ and put*

$$A = S^{-1}K[x], \qquad \mathfrak{m} = \sum_{1 \leq i \leq n} A(x_i - a_i), \qquad \mathfrak{p} = \sum_{1 \leq i \leq p} Af_i(x).$$

Then A and $A/\mathfrak{p}$ are regular local rings with $\dim(A) = n$ *and* $\dim(A/\mathfrak{p}) = n - p$.

Proof. We apply the K-automorphism of $K[x]$ defined by $x_i \mapsto y_i = x_i - a_i$ for $1 \leq i \leq n$ and reduce the general case to the case where $a = 0$. Since we can write $A = K[x] + \mathfrak{m}^r$ for all r, we can identify $G(A)$ with $K[x]$. Therefore, A is a regular local ring with $\dim(A) = n$. Furthermore, by assumption there exist $1 \leq j_1 < \dots < j_p \leq n$ such that if $g(x)$ denotes the determinant of the of $p \times p$ submatrix of $J(x)$ obtained by crossing out its j-th columns for all $j \neq j_1, \dots, j_p$, then $g(0) \neq 0$. We observe that every $f(x)$ in $K[x]$ satisfying $f(0) = 0$ and its first polar

$$(\partial f/\partial x_1)(0)x_1 + \dots + (\partial f/\partial x_n)(0)x_n$$

have the same image in $\mathfrak{m}/\mathfrak{m}^2$. Therefore, if we denote x_j for $j \neq j_1, \dots, j_p$ by $t_1, \dots, t_d$, then the images of $f_1(x), \dots, f_p(x)$, $t_1, \dots, t_d$ in $\mathfrak{m}/\mathfrak{m}^2$ form its K-basis, hence

$$\mathfrak{m} = \sum_{1 \leq i \leq p} Af_i(x) + \sum_{1 \leq j \leq d} At_j.$$

It then follows from Proposition 11.1.2 that $\mathfrak{p}$ is a prime ideal of A and $A/\mathfrak{p}$ is a regular local ring with $\dim(A/\mathfrak{p}) = d = n - p$.

We remark that if we put $P = K[x] \cap \mathfrak{p}$, then P is a prime ideal of $K[x]$ satisfying $S^{-1}P = \mathfrak{p}$ and a minimal representation of the ideal of $K[x]$ generated by $f_1(x), \dots, f_p(x)$ is of the form

$$\sum_{1 \leq i \leq p} K[x]f_i(x) = P \cap \Big(\bigcap_{1 < i \leq t} Q_i \Big),$$

in which the primary ideal Q_i of $K[x]$ intersects S for $1 < i \leq t$. This follows from Lemma 1.2.2 and Proposition 1.2.1.

11.2 Geometric language

We shall fix an algebraically closed field Ω, denote by F any subfield of Ω and by m, n nonnegative integers. Then, as a set, the *affine n-space* Aff^n is defined as Ω^n with $\mathrm{Aff}^n = \{0\}$ for $n = 0$. Also as a set, the *projective n-space* Proj^n is defined as the factor space of $\Omega^{n+1}\backslash\{0\}$ by $\Omega^\times$ in the same way as in Chapter 3.1. If a is a point of Proj^n represented by $(a_1, \ldots, a_{n+1})$ in $\Omega^{n+1}\backslash\{0\}$, then $(a_1, \ldots, a_{n+1})$ are called the *homogeneous coordinates* of a; they are determined by a up to a common factor in $\Omega^\times$. If $t_1, \ldots, t_{n+1}$ are variables and $f(t)$ is a homogeneous polynomial in $\Omega[t] = \Omega[t_1, \ldots, t_{n+1}]$, then we denote $f(a_1, \ldots, a_{n+1})$ simply by $f(a)$. This will not cause any problem because we shall be interested only in whether or not $f(a)$ is 0 and in the quotient $f(a)/g(a)$ where $g(t)$ is also homogeneous of the same degree as $f(t)$ with $g(a) \neq 0$. If I is any set of homogeneous polynomials $f_i(t)$ in $\Omega[t]$, then a subset of Proj^n is well defined as the set of all a satisfying $f_i(a) = 0$ for all $f_i(t)$ in I. We call such a set a *closed subset* of Proj^n. If J is a similar subset of $\Omega[t]$ as I such that I and J generate the same ideal of $\Omega[t]$, then I and J define the same closed subset of Proj^n. Therefore, by Hilbert's basis theorem, i.e., by Theorem 1.3.1, we may assume that I is finite. If X is a closed subset of Proj^n defined by I, we take all homogeneous polynomials in $\Omega[t]$ which vanish at every point of X and denote by $I(X)$ the ideal of $\Omega[t]$ generated by them. Then, by Hilbert's Nullstellensatz, i.e., by Theorem 1.3.2, $I(X)$ is the root of the ideal of $\Omega[t]$ generated by I. If $I(X)$ has an ideal basis in $F[t] = F[t_1, \ldots, t_{n+1}]$, then X is called an *F-closed subset* of Proj^n. If $I(X)$ is a prime ideal, then X is called *irreducible*. Every closed subset X of Proj^n can be expressed as a finite union of irreducible closed subsets $X_1, X_2, \ldots$. If no X_i is contained in X_j for $i \neq j$, then the expression is unique, and $X_1, X_2, \ldots$ are called *irreducible components* of X. An outline of the proof is as follows.

Since $I(X)$ is equal to its root $r(I(X))$, by Theorem 1.2.1 its minimal representation $I(X) = P_1 \cap P_2 \cap \ldots$, where $P_1, P_2, \ldots$ are necessarily prime ideals of $\Omega[t]$ with no inclusion relation, is unique. Every λ in $\Omega^\times$ gives rise to an Ω-automorphism of $\Omega[t]$ as $t_i \mapsto \lambda t_i$ for $1 \leq i \leq n+1$, and $I(X)$ is invariant under this action of $\Omega^\times$ on $\Omega[t]$, hence $P_1, P_2, \ldots$ will just be permuted. Since the m-th power map from $\Omega^\times$ to itself is surjective for every $m > 0$, it has no subgroup of finite index larger than 1. Therefore, the permutation group is trivial, hence every P_i is invariant. Then the homogeneous parts of every $f(t)$ in P_i is in P_i, hence P_i is generated by homogeneous polynomials, and hence they define a closed subset X_i. By definition, $X_1, X_2, \ldots$ are the irreducible components of X.

The complement of a closed subset of Proj^n is called *open*. The intersection of a closed subset and an open subset of Proj^n, i.e., the difference of two closed subsets, is called *locally closed*. We observe that $t_i \neq 0$, i.e., the complement of the closed subset of Proj^n defined by t_i, defines an open subset U_i of Proj^n and Proj^n becomes the union of $U_1, \ldots, U_{n+1}$. If a with homogeneous coordinates $(a_1, \ldots, a_{n+1})$ is in

U_i, i.e., $a_i \neq 0$, and if we put

$$\phi_i(a) = (a_1/a_i, \dots, a_{i-1}/a_i, a_{i+1}/a_i, \dots, a_{n+1}/a_i),$$

then ϕ_i gives a bijection from U_i to Aff^n for $1 \leq i \leq n+1$. Therefore, we can say that Proj^n is covered by $n+1$ affine n-spaces.

If X is any nonempty locally closed subset of Proj^n, then we can define closed, open, and locally closed subsets of X by relative topology. For instance, if I is any set of homogeneous polynomials in $\Omega[t]$, then the intersection of X and the closed subset of Proj^n defined by I is a closed subset of X. In the following we shall denote by $g(t)$, $g'(t)$, etc. homogeneous polynomials in $\Omega[t]$ all different from 0. If $g(t)$ is such a polynomial, the open subset of X defined by $g(t) \neq 0$, i.e., as the difference of X and the closed subset of Proj^n defined by $g(t)$, will be denoted by X_g. We observe that $X_g = \emptyset$ if and only if $g(a) = 0$ for every a in X; that $X_g \cap X_{g'} = X_{gg'}$; and that the set of all X_g forms an open base for X. If $X_g \neq \emptyset$ and if $f(t)$ is a homogeneous polynomial in $\Omega[t]$ of the same degree as $g(t)^k$ for some k in $\mathbb{N}$, then the quotient $f(t)/g(t)^k$ gives rise to a well-defined Ω-valued function on X_g. We shall denote by $\mathcal{O}(X_g)$ the Ω-algebra of all such functions on X_g. If now a is any point of X, then we take the direct limit of $\mathcal{O}(X_g)$ for all $g(t)$ such that $g(a) \neq 0$ and denote it by $\mathcal{O}_{X,a}$. We recall that the above direct limit is defined as follows: We say that φ, φ' respectively in $\mathcal{O}(X_g)$, $\mathcal{O}(X_{g'})$, where $g(a)g'(a) \neq 0$ are equivalent if for some multiple $g''(t)$ of $g(t)g'(t)$, also satisfying $g''(a) \neq 0$, the restrictions of φ, φ' to $X_{g''}$ are equal. The set of all equivalence classes forms an Ω-algebra, and that is $\mathcal{O}_{X,a}$. We observe that $\mathcal{O}_{X,a}$ is a local ring, i.e., the set $\mathfrak{m}_a$ of all nonunits of $\mathcal{O}_{X,a}$ forms a maximal ideal; the noetherian property of $\mathcal{O}_{X,a}$ will become clear later. The set of $\mathcal{O}_{X,a}$ for all a in X is denoted by $\mathcal{O}_X$ and the pair $(X, \mathcal{O}_X)$ or simply X is called a *quasi-projective variety*. If X is closed, then it is called a *projective variety*. If X is the difference of F-closed subsets, then X is called a *quasi-projective F-variety*. As a special case, a *projective F-variety* is defined. Suppose that X, Y are quasi-projective varieties not necessarily in the same projective space and f is a map from X to Y. Then f is called a *morphism* if for every a in X, $b = f(a)$, and ψ in $\mathcal{O}_{Y,b}$ the composition $\psi \circ f$ is in $\mathcal{O}_{X,a}$. The product of two morphisms is a morphism. If a morphism is bijective and if the inverse map is also a morphism, then it is called an *isomorphism*. If X is contained in Y, then the inclusion map is a morphism, and X is called a *subvariety* of Y.

We shall show that the product $X = \mathrm{Proj}^m \times \mathrm{Proj}^n$, hence also the product of projective varieties, can be considered as a projective variety. We take any point (a, b) of X and denote the homogeneous coordinates of a, b respectively by $(a_1, \dots, a_{m+1})$, $(b_1, \dots, b_{n+1})$. We order $N+1 = (m+1)(n+1)$ elements $c_{ij} = a_i b_j$ of Ω lexicographically as $(c_{11}, c_{12}, \dots)$ and regard them as homogeneous coordinates of a point c of Proj^N. Then we get a well-defined map from X to Proj^N as $(a, b) \mapsto c$. We shall examine the image of X. We introduce $N+1$ variables t_{ij} and put

$$f_{ij,i'j'}(t) = t_{ij}t_{i'j'} - t_{ij'}t_{i'j}$$

for $1 \leq i,\ i' \leq m+1$, $1 \leq j,\ j' \leq n+1$. We denote by I the set of these quadratic forms in t_{ij} and by Y the closed subset of Proj^N defined by I. If $c_{ij} = a_i b_j$ as above,

then $f_{ij,i'j'}(c) = 0$ for all $f_{ij,i'j'}(t)$ in I. Therefore, c is in Y. Conversely, suppose that c is any point of Y with homogeneous coordinates $(c_{11}, c_{12}, \dots)$ so that $c_{i_0 j_0} \neq 0$ for some i_0, j_0. Denote by a, b the points of Proj^m, Proj^n with $(c_{1,j_0}, \dots, c_{m+1,j_0})$, $(c_{i_0,1}, \dots, c_{i_0,n+1})$ as their respective homogeneous coordinates. Then we see that c is the image of (a, b). We have thus shown that Y is the image of X. We shall show that the surjective map $X \to Y$ is injective, hence bijective. Suppose that (a', b') in X has the same image as (a, b) and that $(a'_1, \dots, a'_{m+1})$, $(b'_1, \dots, b'_{n+1})$ are the homogeneous coordinates of a', b'. Then we will have $a'_i b'_j = \lambda a_i b_j$ for all i, j with some λ in $\Omega^\times$. If $a_{i_0} b_{j_0} \neq 0$, then $a'_{i_0} b'_{j_0} \neq 0$, hence we may assume that $a_{i_0} = b_{j_0} = a'_{i_0} = b'_{j_0} = 1$. This implies $\lambda = 1$, $a'_i = a'_i b'_{j_0} = a_i b_{j_0} = a_i$, and similarly $b'_j = b_j$ for all i, j, hence $(a, b) = (a', b')$. We now define $\mathcal{O}_X$ so that the bijection $X \to Y$ becomes an isomorphism. We might mention that $\mathcal{O}_X$ can be defined directly by using doubly homogeneous polynomials. We also remark that if for any $1 \leq i_0 \leq m+1$ we define an open subset U_{i_0} of Proj^m as before and put $J = \{t_{i_0,j}; 1 \leq j \leq n+1\}$, then the above isomorphism $X \to Y$ gives rise to an isomorphism from the product $U_{i_0} \times \mathrm{Proj}^m$ to the difference of Y and the closed subset of Proj^N defined by J. Therefore, $\mathrm{Aff}^m \times \mathrm{Proj}^n$ can be considered as a quasi-projective variety.

As a rather special case of the above, we regard any closed subset of Aff^n as a quasi-projective variety, and call it an *affine variety*. If X is such a variety, then the set $I(X)$ of all $f(t)$ in $\Omega[t] = \Omega[t_1, \dots, t_n]$ which vanish at every point of X forms an ideal of $\Omega[t]$. We shall show that if $g(t)$ is any element of $\Omega[t]$ different from 0, then the open subset X_g of X consistsing of all a in X for which $g(a) \neq 0$ can be considered as an affine variety. In fact, if s is a variable, then the set Y of all common zeros of elements of $I(X)$ and $h(t, s) = g(t)s - 1$ in $\Omega[t, s]$ is an affine variety in Aff^{n+1}. Furthermore, the correspondence $a \mapsto (a, b)$, where $b = 1/g(a)$, gives a bijection from X_g to Y. If an element of $\mathcal{O}_{Y,(a,b)}$ is represented by a function defined by $f^*(t, s)/g^*(t, s)$ for $f^*(t, s)$, $g^*(t, s)$ in $\Omega[t, s]$ and $g^*(a, b) \neq 0$ and if e is at least equal to the degrees in s of $f^*(t, s)$, $g^*(t, s)$, then

$$f^*(t, 1/g(t))/g^*(t, 1/g(t)) = f'(t)/g'(t),$$

in which $f'(t) = g(t)^e f^*(t, 1/g(t))$, $g'(t) = g(t)^e g^*(t, 1/g(t))$ are in $\Omega[t]$ and $g'(a) \neq 0$. This implies that $X \to Y$ is a morphism. Since the projection $Y \to X$ is a morphism, the bijection $X \to Y$ is an isomorphism.

We shall make some remarks on the local ring $\mathcal{O}_{X,a}$ for any quasi-projective variety X. Firstly, $\mathcal{O}_{X,a}$ will not change even if we replace X by X_g for any homogeneous polynomial $g(t)$ satisfying $g(a) \neq 0$. We observe that X_g for a suitable $g(t)$ becomes an affine variety. In fact, by definition X can be expressed as $X = X_1 \backslash X_2$ for some closed subsets X_1, X_2 of Proj^n and a is not in X_2. Therefore, we can find a homogeneous polynomial $g_0(t)$ in $I(X_2)$ satisfying $g_0(a) \neq 0$. If further a is in U_i, then we can take $g(t) = g_0(t)t_i$. Therefore, after replacing X by X_g, we may assume that X is an affine variety in Aff^n. We change the notation accordingly and write $\Omega[t] = \Omega[t_1, \dots, t_n]$. We shall show that if S denotes the set of all $g(t)$ in $\Omega[t]$ satisfying $g(a) \neq 0$, where $a = (a_1, \dots, a_n)$, then $\mathcal{O}_a = \mathcal{O}_{X,a}$ can be identified with $S^{-1}\Omega[t]/S^{-1}I(X)$. In particular, $\mathcal{O}_a$ is a noetherian ring. We

recall that an element of $\mathcal{O}_a$ is an equivalence class of functions on X_g for all $g(t)$ in S; that two functions on X_g, $X_{g'}$ respectively defined by $f(t)/g(t)^k$, $f'(t)/g'(t)^{k'}$ for $f(t)$, $f'(t)$ in $\Omega[t]$, $g(t)$, $g'(t)$ in S, and k, k' in $\mathbb{N}$ are equivalent if for some multiple $g''(t)$ of $g(t)g'(t)$, also in S, they give rise to the same function on $X_{g''}$. Then $h(t) = f(t)g'(t)^{k'} - f'(t)g(t)^k$ vanishes at every point of $X_{g''}$, hence $g''(t)h(t)$ is in $I(X)$, and hence $f(t)/g(t)^k - f'(t)/g'(t)^{k'}$ in in $S^{-1}I(X)$. Since the converse is clear, we indeed have $\mathcal{O}_a = S^{-1}\Omega[t]/S^{-1}I(X)$.

After these preliminaries, suppose that X is a quasi-projective variety and for every a in X put $\dim_a(X) = \dim(\mathcal{O}_a)$. Then by Proposition 11.1.1 we have

$$\dim_a(X) \leq \dim_\Omega(\mathfrak{m}_a/\mathfrak{m}_a^2).$$

We say, after O. Zariski [63], that a is a *simple point* of X if the equality holds, i.e., if $\mathcal{O}_a$ is a regular local ring. We sometimes denote by X_{smooth} the set of all simple points of X. If $X = X_{\text{smooth}}$, then we call X *nonsingular* or *smooth*. Furthermore if $d = \dim_a(X)$ is independent of a in X, then we say that X is *d-dimensional* or, more precisely, *everywhere d-dimensional*. We observe that Aff^n and Proj^n are both smooth and everywhere n-dimensional.

Finally, suppose that a point a of Proj^n with homogeneous coordinates $(a_1, \ldots, a_{n+1})$ is contained in U_i and U_j, i.e., $a_i a_j \neq 0$. Then we clearly have $F(\phi_i(a)) = F(\phi_j(a))$; we denote this field by $F(a)$. If $F(a) = F$ we say that a is an *F-rational point*. If X is a quasi-projective F-variety in Proj^n, we denote by $X(F)$ the set of all F-rational points of X.

11.3 Hironaka's desingularization theorem (algebraic form)

We shall start with a simple example. We fix an algebraically closed field Ω and denote by F any subfield of Ω as in section 11.2. We take the product $X \times \text{Proj}^{n-1}$, where $X = \text{Aff}^n$, and denote by Y its closed subset defined by $x_i z_j - x_j z_i$ for $1 \leq i, j \leq n$, in which $(x_1, \ldots, x_n)$ are the coordinates on X and $(z_1, \ldots, z_n)$ are the homogeneous coordinates on Proj^{n-1} all considered as variables. If h denotes the restriction to Y of the projection from $X \times \text{Proj}^{n-1}$ to X, then h gives a bijection from $Y \backslash h^{-1}(0)$ to $X \backslash \{0\}$, in which $h^{-1}(0) = \{0\} \times \text{Proj}^{n-1}$. In order to get more precise information about Y and h, we express Proj^{n-1} as the union of the open subset Z_α defined by $z_\alpha \neq 0$ for $1 \leq \alpha \leq n$. Then Y becomes the union of $Y_\alpha = Y \cap (X \times Z_\alpha)$ for all α. Since they are all similar, we take $\alpha = 1$ and put

$$(t_1, \ldots, t_{2n-1}) = (x_1, \ldots, x_n, z_2/z_1, \ldots, z_n/z_1);$$

also we denote the image of t_i in $\Omega[t_1, \ldots, t_{2n-1}]/I(Y_1)$ by y_i for $1 \leq i \leq 2n - 1$. Then Y_1 becomes isomorphic to Aff^n under the map $y = (y_1, \ldots, y_{2n-1}) \mapsto (y_1, y_{n+1}, \ldots, y_{2n-1})$ and

$$h(y) = (y_1, \ldots, y_n) = (y_1, y_1 y_{n+1}, \ldots, y_1 y_{2n-1}).$$

If we use $(y_1, y_{n+1}, \dots, y_{2n-1})$ as the coordinates on Y_1, then the jacobian of $h|Y_1$ becomes

$$\partial(x_1, \dots, x_n)/\partial(y_1, y_{n+1}, \dots, y_{2n-1}) = y_1^{n-1}.$$

Also $(y_1, y_{n+1}, \dots, y_{2n-1}) = (x_1, x_2/x_1, \dots, x_n/x_1)$, hence $h|Y_1$ gives rise to an isomorphism from $Y_1 \backslash y_1^{-1}(0)$ to $X \backslash x_1^{-1}(0)$. At any rate Y is a closed smooth n-dimensional subvariety of $X \times \mathrm{Proj}^{n-1}$.

We now take $f(x)$ from $F[x_1, \dots, x_n] \backslash F$, denote by $f^{-1}(0)$ the set of all a in X satisfying $f(a) = 0$, and examine the effect of $h : Y \to X$ on the hypersurface $f^{-1}(0)$ in X. We shall assume that if $f_0(x)$ is the leading form of $f(x)$, i.e., the homogeneous part of $f(x)$ of the smallest degree, then $N = \deg(f_0) > 0$ and not all partial derivatives of $f_0(x)$ vanish at any point of $f_0^{-1}(0)$ other than 0. We observe that the preimage $(f \circ h)^{-1}(0)$ of $f^{-1}(0)$ in Y under h is the union of its intersection with Y_α for $1 \leq \alpha \leq n$. Since they are all similar, we take $\alpha = 1$ and use the same notation as above. We then have

$$f(h(y)) = f(y_1, y_1 y_{n+1}, \dots, y_1 y_{2n-1}) = y_1^N f_1(y),$$

in which

$$f_1(y) = f_0(1, y_{n+1}, \dots, y_{2n-1}) + y_1 f'(y)$$

with $f'(y)$ in $F[y_1, y_{n+1}, \dots, y_{2n-1}]$. In general, if $f_1(t), \dots, f_p(t)$ in $\Omega[t_1, \dots, t_n]$ satisfy the condition in Theorem 11.1.1 for $K = \Omega$, then we say that the p hypersurfaces $f_1^{-1}(0), \dots, f_p^{-1}(0)$ in Aff^n are *transversal at* a. In that case the theorem implies that a is a simple point of their intersection. We shall show that $f_1^{-1}(0)$ and $y_1^{-1}(0)$ are transversal at every point of their intersection.

If $b = (b_1, b_{n+1}, \dots, b_{2n-1})$ is any point of their intersection, then $b_1 = 0$ and $f_1(b) = f_0(c) = 0$, in which $c = (1, b_{n+1}, \dots, b_{2n-1})$. If $f_1^{-1}(0)$ and $y_1^{-1}(0)$ are not transversal at b, then

$$(\partial f_1/\partial y_{n+i})(b) = (\partial f_0/\partial x_{i+1})(c) = 0$$

for $1 \leq i < n$. If we write down Euler's identity for $f_0(x)$ and evaluate both sides at c, then we also have $(\partial f_0/\partial x_1)(c) = 0$. Since $f_0(c) = 0$ and $c \neq 0$, this contradicts the assumption that $f_0^{-1}(0) \backslash \{0\}$ is smooth.

If we further assume that $f(x)$ is homogeneous, hence $f(x) = f_0(x)$, then $f^{-1}(0) \backslash \{0\}$ is smooth. In that case since $f_1(y) = f(1, y_{n+1}, \dots, y_{2n-1})$, the above argument shows that $f_1^{-1}(0)$ is smooth. Therefore, if we denote by E_1, E_2 the closed subsets of Y such that their intersections with Y_1 are respectively $y_1^{-1}(0)$, $f_1^{-1}(0)$ and their intersections with Y_α are similar, then $(f \circ h)^{-1}(0)$ becomes the union of E_1, E_2 and they are both smooth, $(n-1)$-dimensional, and have normal crossings in the sense that they are transversal at every point of their intersection. Furthermore, the bijection from $Y \backslash h^{-1}(0)$ to $X \backslash \{0\}$ is an isomorphism. We also observe that Y and E_1, E_2 are F-varieties.

We shall now introduce the concept of Hironaka's desingularization of a hypersurface by using some terminology which will be explained in a slightly different language.

Definition 1. *Let $f(x)$ denote any element of $F[x_1, \dots, x_n] \backslash F$, where F is an arbitrary field and $x_1, \dots, x_n$ are variables. Then a Hironaka's desingularization of the hypersurface in $X = \mathrm{Aff}^n$ defined by $f(x)$ is a closed smooth n-dimensional F-subvariety Y of $X \times \mathrm{Proj}^m$ for some m such that the restriction h to Y of the projection $X \times \mathrm{Proj}^m \to X$ has the following properties: Firstly, there exists a finite set $\mathcal{E}$ of closed smooth $(n-1)$-dimensional F-subvarieties E of Y with normal crossings. Secondly, as point-sets $(f \circ h)^{-1}(0)$ is the union of all E in $\mathcal{E}$ and h gives rise to an isomorphism $Y \backslash (f \circ h)^{-1}(0) \to X \backslash f^{-1}(0)$. Thirdly, the divisors of $f \circ h$ and $h^*(dx_1 \wedge \cdots \wedge dx_n)$ on Y are respectively of the forms $\sum N_E E$ and $\sum (n_E - 1)E$, in which N_E, n_E are positive integers and the summations are for all E in $\mathcal{E}$.*

It follows from the definition that $h : Y \to X$ is surjective. We shall give a local description of the Hironaka desingularization. We denote by $z_1, \dots, z_{m+1}$ the homogeneous coordinates on Proj^m and express Proj^m as the union of the open subsets Z_α defined by $z_\alpha \neq 0$ for $1 \leq \alpha \leq m+1$. Then Y becomes the union of $Y_\alpha = Y \cap (X \times Z_\alpha)$ for all α. We choose α arbitrarily and identify $X \times Z_\alpha$ with Aff^{m+n} by using

$$(x_1, \dots, x_n, z_1/z_\alpha, \dots, z_{\alpha-1}/z_\alpha, z_{\alpha+1}/z_\alpha, \dots, z_{m+1}/z_\alpha)$$

as coordinates $(t_1, \dots, t_{m+n})$ on Aff^{m+n}. Then Y_α is a closed subset of Aff^{m+n}, the ideal $I(Y_\alpha)$ has a basis in $F[t] = F[t_1, \dots, t_{m+n}]$, and the local ring $\mathcal{O}_b$ of Y_α at every point $b = (b_1, \dots, b_{m+n})$ of Y_α is regular of dimension n. Therefore, if we denote the image of t_i in $\mathcal{O}_b$ by y_i for $1 \leq i \leq m+n$, then $y_{i_1} - b_{i_1}, \dots, y_{i_n} - b_{i_n}$ for some $1 \leq i_1 < \dots < i_n \leq m+n$ generate the maximal ideal $\mathfrak{m}_b$ of $\mathcal{O}_b$, and if we denote the image of $y_i - b_i$ in $\mathfrak{m}_b/\mathfrak{m}_b^2$ by dy_i for all i, then $dy_{i_1}, \dots, dy_{i_n}$ form an Ω-basis for $\mathfrak{m}_b/\mathfrak{m}_b^2$. If we now write all E's which contain b by $E_1, \dots, E_p$, then there exist $f_1(t), \dots, f_p(t), g(t)$ in $F[t]$ with $g(b) \neq 0$ such that $f_1(y), \dots, f_p(y)$ can be included in an ideal basis for $\mathfrak{m}_b$ and further $E_i \cap (Y_\alpha)_g = f_i^{-1}(0) \cap (Y_\alpha)_g$ for $1 \leq i \leq p$, in which $(Y_\alpha)_g = Y_\alpha \backslash g^{-1}(0)$. Finally, we have $h(y) = (y_1, \dots, y_n)$, $h^*(dx_i) = dy_i$ for $1 \leq i \leq n$, hence $(f \circ h)(y) = f(y_1, \dots, y_n)$, $h^*(dx_1 \wedge \dots \wedge dx_n) = dy_1 \wedge \dots \wedge dy_n$, and

$$(f \circ h)(y) = \varepsilon \cdot \prod_{1 \leq i \leq p} f_i(y)^{N_i},$$

$$h^*(dx_1 \wedge \dots \wedge dx_n) = \eta \cdot \prod_{1 \leq i \leq p} f_i(y)^{n_i - 1} \cdot dy_{i_1} \wedge \dots \wedge dy_{i_n},$$

in which ε, η are units of $\mathcal{O}_b$ and $(N_i, n_i) = (N_E, n_E)$, where $E = E_i$ for $1 \leq i \leq p$. In the above example $m = n-1$, $\alpha = 1$, and $(i_1, \dots, i_n) = (1, n+1, \dots, 2n-1)$; that $\mathcal{E} = \{E_1, E_2\}$, $f_1(t) = t_1$, $f_2(t) = f(1, t_{n+1}, \dots, f_{2n-1})$, $g(t) = \varepsilon = \eta = 1$, and $(N_E, n_E) = (N, n)$, $(1, 1)$ respectively for $E = E_1$, E_2. At any rate, we can state one form of Hironaka's desingularization theorem in [20] as follows:

Theorem 11.3.1 *If $\mathrm{char}(F) = 0$, then a Hironaka's desingularization of any F-hypersurface in Aff^n exists.*

We shall now take an algebraic number field k as F and denote any p-adic completion of k by K, the maximal compact subring of K by O_K, the maximal ideal

of O_K by πO_K, and put $O_K/\pi O_K = \mathbb{F}_q$ as before. Furthermore, for any F-closed subset X of Aff^n we denote by $F[X]$ the factor ring of $F[x] = F[x_1, \ldots, x_n]$ by its ideal $F[x] \cap I(X)$. If $f(x)$ is now in $k[x]\backslash k$, then by Theorem 11.3.1 a Hironaka's desingularization $h : Y \to X = \mathrm{Aff}^n$ of the hypersurface in X defined by $f(x)$ exists. We observe that if all nonzero coefficients of $f(x)$ are units of O_K, by applying the homomorphism $O_K \to \mathbb{F}_q$ to them, we get an $\bar{f}(x)$ in $\mathbb{F}_q[x]\backslash\mathbb{F}_q$. The fact is that for almost all K, i.e., except for a finite number of K, the above $h : Y \to X$ gives rise to a Hironaka's desingularization of the hypersurface in $\bar{X} = \mathrm{Aff}^n$ defined by $\bar{f}(x)$. It is understood that the new Aff^n is relative to an algebraically closed field containing $\mathbb{F}_q$. In the following, we shall give some details to this basic fact.

We have expressed $X \times \mathrm{Proj}^m$ as the union of $X \times Z_\alpha = \mathrm{Aff}^{m+n}$ and Y as the union of $Y_\alpha = Y \cap (X \times Z_\alpha)$ for $1 \leq \alpha \leq m+1$; for each α we choose a finite subset $\{g_\beta(t)\}$ of $k[t]\backslash\{0\}$, where $k[t] = k[t_1, \ldots, t_{m+n}]$, and express Aff^{m+n} as the union of its open subset

$$U_\beta = \mathrm{Aff}^{m+n}\backslash g_\beta^{-1}(0)$$

so that Y_α becomes the union of $Y_{\alpha\beta} = Y_\alpha \cap U_\beta$ for all β. We keep in mind that we can get an arbitrarily fine k-open covering of Aff^{m+n}, hence that of Y_α, in that way. We shall impose three conditions on the choice of $\{g_\beta(t)\}$. The first condition is that for each β there exist $h_1(t), \ldots, h_m(t)$ in $k[t]$ such that

$$Y_{\alpha\beta} = h_1^{-1}(0) \cap \ldots \cap h_m^{-1}(0) \cap U_\beta.$$

If we write all E's which intersect $Y_{\alpha\beta}$ by $E_1, \ldots, E_p$, then the second condition is that there exist $f_1(t), \ldots, f_n(t)$ in $k[t]$ such that $E_i \cap Y_{\alpha\beta} = f_i^{-1}(0) \cap Y_{\alpha\beta}$ for $1 \leq i \leq p$ and

$$d(t) = \partial(f_1, \ldots, f_n, h_1, \ldots, h_m)/\partial(t_1, \ldots, t_{m+n})$$

is a unit of $k[U_\beta]$. The third condition is that if we denote the image of t_i in $\Omega[t]/I(Y_\alpha)$ by y_i for $1 \leq i \leq m+n$, then

$$f \circ h\big|Y_{\alpha\beta} = \varepsilon \cdot \prod_{1 \leq i \leq p} f_i(y)^{N_i},$$

$$h^*(dx_1 \wedge \ldots \wedge dx_n)\big|Y_{\alpha\beta} = \eta \cdot \prod_{1 \leq i \leq p} f_i(y)^{n_i - 1} \cdot df_1(y) \wedge \ldots \wedge df_n(y),$$

in which ε, η are units of $k[Y_{\alpha\beta}]$. These conditions are satisfied for a suitable choice of $\{g_\beta(t)\}$.

We shall express the above conditions by identities in $k[t]$; we shall use e_0, e, etc. to denote nonnegative integers. First of all, by Hilbert's Nullstellensatz there exist $g'_\beta(t)$ in $k[t]$ satisfying $\sum g'_\beta(t) g_\beta(t) = 1$. If we put

$$\mathfrak{a} = k[t]h_1(t) + \ldots + k[t]h_m(t),$$

then $k[U_\beta] = k[t, 1/g_\beta(t)]$ implies $k[Y_{\alpha\beta}] = k[U_\beta]/k[U_\beta]\mathfrak{a} = k[y, 1/g_\beta(y)]$. Therefore, every element of $k[Y_{\alpha\beta}]$ is of the form $P(y)/g_\beta(y)^{e_0}$ for some $P(t)$ in $k[t]$ and e_0; it

is a unit of $k[Y_{\alpha\beta}]$ if and only if $P'(t)P(t) \equiv g_\beta(t)^e \bmod \mathfrak{a}$ for some $P'(t)$ in $k[t]$ and e. In particular, $\varepsilon = \varepsilon_0(y)/g_\beta(y)^{e_\varepsilon}$, $\eta = \eta_0(y)/g_\beta(y)^{e_\eta}$ and

$$\varepsilon_0'(t)\varepsilon_0(t) \equiv \eta_0'(t)\eta_0(t) \equiv g_\beta(t)^e \mod \mathfrak{a}$$

for some $\varepsilon_0(t)$, $\varepsilon_0'(t)$, $\eta_0(t)$, $\eta_0'(t)$ in $k[t]$ and e_ε, e_η, e. Furthermore,

$$d'(t)d(t) = g_\beta(t)^e$$

for some $d'(t)$ in $k[t]$ and e, and

$$g_\beta(t)^e f(t) \equiv \varepsilon_0(t) g_\beta(t)^{e_0} \cdot \prod_{1\le i\le p} f_i(t)^{N_i} \mod \mathfrak{a}$$

where $e = e_0 + e_\varepsilon$ for some e_0. Finally, if we denote the jacobian matrix of $f_1, \dots, f_n,\ h_1, \dots, h_m$ by $t_1, \dots, t_{m+n}$ as

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} 1_n & B \\ 0 & D \end{pmatrix} \begin{pmatrix} A - BD^{-1}C & 0 \\ D^{-1}C & 1_m \end{pmatrix}$$

with $m \times m$ matrix $D = D(t)$, etc., since $d(t)$ is its determinant, we get $d(t) = \det(D)\det(A - BD^{-1}C)$ provided that $\det(D) \not\equiv 0$. We shall show that $\det(D(y)) \not\equiv 0$. If for a moment we denote the (i,j)-entries of C, D by c_{ij}, d_{ij}, then we have

$$\sum_{1\le j\le n} c_{ij}(y)\ dy_j + \sum_{1\le j\le m} d_{ij}(y)\ dy_{n+j} = 0$$

for $1 \le i \le m$. Since $dy_1, \dots, dy_n$ are linearly independent, if $\det(D(y)) = 0$, then we will have $\operatorname{rank}(C(y)\ D(y)) < m$. This brings the contradiction that $d(y) = 0$. Furthermore, the above proof implies that

$$df_1(y) \wedge \ldots \wedge df_n(y) = \det(A - BD^{-1}C)(y) \cdot h^*(dx_1 \wedge \ldots \wedge dx_n)\big|Y_{\alpha\beta}.$$

Therefore, the condition on $h^*(dx_1 \wedge \ldots \wedge dx_n)|Y_{\alpha\beta}$ can be written as

$$\det(D)(y) = d(y)\eta \cdot \prod_{1\le i\le p} f_i(y)^{n_i - 1}, \quad \text{i.e.,}$$

$$g_\beta(t)^e \det(D) \equiv d(t)\eta_0(t) g_\beta(t)^{e_0} \cdot \prod_{1\le i\le p} f_i(t)^{n_i - 1} \mod \mathfrak{a}$$

where $e = e_0 + e_\eta$. We have used the same e_0, e above because that is permissible after making them larger. Also, $P(t) \equiv 0 \bmod \mathfrak{a}$ means, of course, that $P(t) = A_1(t)h_1(t) + \ldots + A_m(t)h_m(t)$ for some $A_1(t), \dots, A_m(t)$ in $k[t]$. If we replace the above congruences mod $\mathfrak{a}$ by equations of this form, we get a finite number of identities in $k[t]$. We now take a p-adic completion K of k such that, in addition to the coefficients of $f(x)$ being units of O_K, the coefficients of all $P(t)$ in $k[t]$, which appear in the above identities, are all in O_K. This condition is satisfied by almost all K. Furthermore, if we replace all such $P(t)$ by its image $\bar{P}(t)$ in $\mathbb{F}_q[t]$, then it is rather obvious that the data so obtained will give a Hironaka's desingularization of the hypersurface in $\bar{X} = \mathrm{Aff}^n$ defined by $\bar{f}(x)$.

11.4 Weil's zeta functions over finite fields

We shall explain the main theorem on Weil's zeta functions over finite fields. Since the proof will not be given, or rather, can not be given because it is beyond the level of this book, we shall explain two examples. Although the following first example is incomparably simpler, these are the examples mentioned in Weil's paper [57] of 1949 in which he announced the above-mentioned theorem as a conjecture. The explanation will be with proof except for some topological results. More precisely, if for any d-dimensional compact $\mathbb{C}$-analytic manifold M we define its Poincaré polynomial $P(M,t)$ as

$$P(M,t) = \sum_{0 \le i \le 2d} B_i t^i,$$

in which B_i is the i-dimensional Betti number of M, hence $B_i = B_{2d-i}$ by the Poincaré duality, then we shall just mention the explicit forms of $P(M,t)$ in the two examples without proof.

We shall explain the first example. If $Q(x)$ is a reduced quadratic form in $n \ge 3$ variables $x_1, \ldots, x_n$ with coefficients in $\mathbb{F}_q$ and Ω is an algebraically closed field containing $\mathbb{F}_q$, then $Q(x)$ defines an irreducible smooth $(n-2)$-dimensional projective $\mathbb{F}_q$-variety X in Proj^{n-1} . Furthermore,

$$\mathrm{card}(X(\mathbb{F}_q)) = 1 + q + \ldots + q^{n-2} + \chi(Q) q^{n/2-1},$$

in which $\chi(Q) = 0$ if n is odd and $\chi(Q) = \pm 1$ according as $Q(x)$ is hyperbolic or not if n is even. This follows immediately from the formula for $\mathrm{card}(Q^{-1}(0))$ in Theorem 9.2.1. On the other hand, if M is the hypersurface in $P_{n-1}(\mathbb{C})$, i.e., Proj^{n-1} for $\Omega = \mathbb{C}$, defined as the set of zeros of $x_1x_2 + \ldots + x_{n-1}x_n$ or $x_1x_2 + \ldots + x_{n-2}x_{n-1} + x_n^2$ according to whether n is even or odd, then it is well known that

$$P(M,t) = 1 + t^2 + \ldots + t^{2(n-2)} + (1/2)(1 + (-1)^n) t^{n-2}.$$

We might mention the proof in the special case where $n = 4$. If we use the notation in section 11.2, then $\mathrm{Proj}^1 \times \mathrm{Proj}^1$ is isomorphic to the surface in Proj^3 defined by $t_{11}t_{22} - t_{12}t_{21}$, hence M is $\mathbb{C}$-bianalytic to $P_1(\mathbb{C}) \times P_1(\mathbb{C})$, and hence

$$P(M,t) = P(P_1(\mathbb{C}),t)^2 = 1 + 2t^2 + t^4.$$

We might also mention that if $Q(x)$ is of the above form, then the open subset of X defined by $x_1 \ne 0$ is isomorphic to Aff^{n-2}.

Before we explain the second example, we shall recall a system of equations defining the Grassmann variety. We shall follow the presentation in G. B. Gurevich [17]. We take an m-dimensional vector space V over an arbitrary field F and examine $\bigwedge^n(V)$ for a fixed $0 < n \le m$. We shall write products of elements of $\bigwedge(V)$ without using $\bigwedge$. We first observe that if W is a subspace of V, then $\bigwedge^n(W)$ is a subspace of $\bigwedge^n(V)$. Furthermore, if W_1, W_2 are subspaces of V, then $\bigwedge^n(W_1 \cap W_2) = \bigwedge^n(W_1) \cap \bigwedge^n(W_2)$. Therefore, for any x in $\bigwedge^n(V)$ there exists the smallest subspace W_x of V such that x is contained in $\bigwedge^n(W_x)$. We shall later give an explicit description of W_x in terms of x. We observe that $\dim_F(W_x) \ge n$

if $x \neq 0$. We say that $x \neq 0$ is *decomposable* if $\dim_F(W_x) = n$, i.e., if $x = v_1 \dots v_n$ for some $v_1, \dots, v_n$ in W_x necessarily forming its F-basis. On the other hand if we choose an F-basis $e_1, \dots, e_m$ for V, then every x in $\bigwedge^n(V)$ can be uniquely expressed as

$$x = \sum_{i_1 < \dots < i_n} x_{i_1 \dots i_n} e_{i_1} \dots e_{i_n}$$

with $x_{i_1 \dots i_n}$ in F. We define $x_{i_1 \dots i_n}$ for all $1 \leq i_1, \dots, i_n \leq m$ so that we get an alternating tensor, which we call the *representative tensor* of x. We shall find the necessary and sufficient condition in terms of $x_{i_1 \dots i_n}$ for x to be decomposable. We observe that if x is decomposable, i.e., if $x = v_1 \dots v_n$ for some $v_1, \dots, v_n$ in V, hence $v_j = y_{1j}e_1 + \dots + y_{mj}e_m$ with y_{ij} in F, then the representative tensor of x becomes

$$x_{i_1 \dots i_n} = \pi_{i_1 \dots i_n}(y),$$

in which y is the $m \times n$ matrix with y_{ij} as its (i,j)-entry and $\pi_{i_1 \dots i_n}(y)$ for $i_1 < \dots < i_n$ is the determinant of the $n \times n$ submatrix of y obtained by crossing out its k-th rows for $k \neq i_1, \dots, i_n$, and they are not all 0.

We take x from $\bigwedge^n(V)$ and φ from the dual space V^* of V. If $x_{i_1 \dots i_n}$ is the representative tensor of x, then we define $\partial_\varphi x$ in $\bigwedge^{n-1}(V)$ as

$$(\partial_\varphi x)_{i_1 \dots i_{n-1}} = \sum_{1 \leq i \leq m} x_{i_1 \dots i_{n-1} i}\, \varphi(e_i)$$

for all $i_1, \dots, i_{n-1}$. We observe that $\partial_\varphi x$ is determined by x and φ independently of the choice of $e_1, \dots, e_m$. Furthermore if x, x' are in $\bigwedge^n(V)$ with the representative tensors $x_{i_1 \dots i_n}$, $x'_{i_1 \dots i_n}$ and if $\partial_i = \partial_\varphi$ for $\varphi = \varphi_i$ in V^* for $1 < i \leq n$, then we can easily verify the formal identity

(∗) $\quad (x(\partial_2 \dots \partial_n x'))_{i_1 \dots i_{n+1}}$

$$= (-1)^{n+1} \Big\{ \sum_{1 \leq j_2, \dots, j_n \leq m} z_{i_1 \dots i_{n+1}, j_2 \dots j_n} \varphi_2(e_{j_2}) \dots \varphi_n(e_{j_n}) \Big\},$$

in which

$$z_{i_1 \dots i_{n+1}, j_2 \dots j_n} = \sum_{1 \leq k \leq n+1} (-1)^k x_{i_1 \dots i_{k-1} i_{k+1} \dots i_{n+1}} x'_{i_k j_2 \dots j_n},$$

for $i_1 < \dots < i_{n+1}$.

In the above notation we shall show that W_x and the F-span W of $\partial_2 \dots \partial_n x$ for all $\varphi_2, \dots, \varphi_n$ in V^* coincide. If we choose an F-basis $e_1, \dots, e_m$ for V such that $e_1, \dots, e_r$ form an F-basis for W_x, then $x_{i_1 \dots i_n} \neq 0$ only for $i_1, \dots, i_n \leq r$, hence $\partial_2 \dots \partial_n x$ is in W_x, and hence W is contained in W_x. If we choose another F-basis $e_1, \dots, e_m$ for V such that $e_1, \dots, e_s$ form an F basis for W, then

$$\sum_{1 \leq i_2, \dots, i_n \leq m} x_{i i_2 \dots i_n} \varphi_2(e_{i_2}) \dots \varphi_n(e_{i_n}) = 0$$

for all $i > s$ and for all $\varphi_2, \dots, \varphi_n$ in V^*. This implies that $x_{ii_2\dots i_n} = 0$ for all $i_2, \dots, i_n$ if $i > s$, hence $x_{i_1\dots i_n} \neq 0$ only for $i_1, \dots, i_n \leq s$. Therefore x is in $\bigwedge^n(W)$, hence W_x is contained in W, hence $W_x = W$.

We are ready to show that $x \neq 0$ in $\bigwedge^n(V)$ is decomposable if and only if its representative tensor satisfies the following quadratic equations:

$$(**) \qquad \sum_{1\leq k\leq n+1} (-1)^k x_{i_1\dots i_{k-1}i_{k+1}\dots i_{n+1}} x_{i_k j_2\dots j_n} = 0$$

for all $i_1 < \dots < i_{n+1}$ and $j_2, \dots, j_n$. First, suppose that x is decomposable. Then $xv = 0$ for all v in W_x, hence for all $v = \partial_2 \dots \partial_n x$. Then by $(*)$ we get $(**)$. Next, suppose that $(**)$ is satisfied. Then by $(*)$ we get $xW_x = 0$. If we choose an F-basis $v_1, \dots, v_r$ for W_x, then x can be expressed uniquely as an F-linear combination of $v_{i_1} \dots v_{i_n}$ for $1 \leq i_1 < \dots < i_n \leq r$. Since $xv_i = 0$ for $1 \leq i \leq r$, we see that $r = n$ and x is in $Fv_1 \dots v_n$.

We shall now explain the second example. We shall take $\mathbb{F}_q$, Ω and later $\mathbb{C}$ as F. We denote by Y the open subset of $M_{m,n}$ consisting of all y with linearly independent columns and consider Proj^N for $N + 1 = \binom{m}{n}$ with homogeneous coordinates $x_{i_1\dots i_n}$ for $1 \leq i_1 < \dots < i_n \leq m$. Then the correspondence $y \mapsto x$ where $x_{i_1\dots i_n} = \pi_{i_1\dots i_n}(y)$ gives a morphism from Y to the projective variety X in Proj^N defined by $(**)$, which is called the *Grassmann variety*. We have seen in Chapter 10.6, though in different language, that the open subset of X defined by $x_{i_1\dots i_n} \neq 0$ is isomorphic to $M_{m-n,n}$ for every $i_1, \dots, i_n$. Therefore, X is an irreducible smooth d-dimensional projective F-variety for $d = (m-n)n$. Furthermore, if $F = \mathbb{F}_q$, then the results there imply that

$$\mathrm{card}(X(\mathbb{F}_q)) = \prod_{1\leq k\leq n} (1 - q^{m-k+1})/(1 - q^k).$$

We recall that in the notation of Chapter 9.6 the RHS is $F_{m-n,n}(q)$. We further recall the Gauss identity:

$$\sum_{0\leq n\leq m} F_{m-n,n}(q)\, q^{n(n-1)/2} t^n = \prod_{0\leq i\leq m-1} (1 + q^i t).$$

If we equate the coefficients of t^n on both sides, we get

$$F_{m-n,n}(q) = q^{-n(n-1)/2} \cdot \sum q^{i_1+\dots+i_n},$$

in which the summation is for $0 \leq i_1 < \dots < i_n \leq m-1$. Therefore, if we replace i_k by $f_k + k - 1$ for $1 \leq k \leq n$, we get

$$\mathrm{card}(X(\mathbb{F}_q)) = \sum_{0\leq k\leq d} B_{2k} q^k,$$

in which B_{2k} denotes the number of partitions $k = f_1 + \dots + f_n$ satisfying $0 \leq f_1 \leq \dots \leq f_n \leq m-n$. We observe that if we put $f_i^* = (m-n) - f_{n-i+1}$ for $1 \leq i \leq n$, then $d - k = f_1^* + \dots + f_n^*$ and $0 \leq f_1^* \leq \dots \leq f_n^* \leq m-n$, hence $B_{2k} = B_{2d-2k}$ for

$0 \leq k \leq d$. On the other hand, if we take $\mathbb{C}$ as Ω and denote the corresponding X by M, then

$$P(M,t) = \sum_{0 \leq k \leq d} B_{2k} t^{2k}.$$

This fact was known in classical algebraic geometry dealing with Schubert varieties. We refer to C. Ehresmann [13] for a topological proof.

After these rather special examples, we shall state the *main theorem* on *Weil's zeta functions*. We recall that an element α of an extension of $\mathbb{Q}$ is called an algebraic integer if it is a zero of a monic polynomial with coefficients in $\mathbb{Z}$.

Theorem 11.4.1 *Let X denote a smooth everywhere d-dimensional projective $\mathbb{F}_q$-variety. Then there exist nonnegative integers B_i for $0 \leq i \leq 2d$ satisfying $B_i = B_{2d-i}$ and for each i algebraic integers $\alpha_{ij} \neq 0$, in fact, all their conjugates over $\mathbb{Q}$ in $\mathbb{C}$ having the absolute value $q^{i/2}$, for $1 \leq i \leq B_i$ with the following properties: Firstly,*

$$\operatorname{card}(X(\mathbb{F}_{q^e})) = \sum_{0 \leq i \leq 2d} \sum_{1 \leq j \leq B_i} (-1)^i \alpha_{ij}^e$$

for all $e \geq 1$ and secondly,

$$\{q^d/\alpha_{ij};\ 1 \leq j \leq B_i\} = \{\alpha_{2d-i,j};\ 1 \leq j \leq B_{2d-i}\}$$

for $0 \leq i \leq 2d$.

As we have stated in the Introduction, this is one of the two theorems which we shall use without proof. Actually, the deeper part of the theorem stating that α_{ij} are algebraic integers of absolute value $q^{i/2}$ will not be used. At any rate, the theorem stated above was conjectured by A. Weil and proved, in the above general form by A. Grothendieck and P. Deligne. We refer to Deligne [8] for the history up to his decisive contribution after the work of B. Dwork, Grothendieck and others all with references. We might at least recall that *Weil's zeta function* $Z(t)$ of X is defined for t near 0 in $\mathbb{C}$ as

$$d\log Z(t)/dt = \sum_{e \geq 1} \operatorname{card}(X(\mathbb{F}_{q^e}))t^{e-1}, \qquad Z(0) = 1.$$

The first and the second parts of the theorem then imply its rationality

$$Z(t) = \prod_{0 \leq i \leq 2d} \prod_{1 \leq j \leq B_i} (1 - \alpha_{ij} t)^{\varepsilon_i}, \qquad \varepsilon_i = (-1)^{i+1}$$

and its functional equation

$$Z(1/q^d t) = \pm (q^{d/2} t)^{\chi} Z(t),$$

in which $\chi = \sum (-1)^i B_i = B_0 - B_1 + \ldots + B_{2d}$. We observe that the above expression of $Z(t)$ shows that the formula for $\operatorname{card}(X(\mathbb{F}_{q^e}))$ determines the set $\{\alpha_{ij};\ 0 \leq i \leq 2d,\ 1 \leq j \leq B_i\}$ and further, if we incorporate the statement on the absolute value of α_{ij}, the set $\{\alpha_{ij};\ 1 \leq j \leq B_i\}$ for each i.

Remark. Some irreducible components of X in Theorem 11.4.1 may not be an $\mathbb{F}_q$-variety and yet Theorem 11.4.1 in the case where X is irreducible implies the general case. We shall give an example which will illustrate this situation. We take any θ from $\mathbb{F}_{q^3}$ which is not a zero of

$$P(t) = \big(t - t^q\big)\big(t + t^q + t^{q^2}\big)\big(t + t^q - 2t^{q^2}\big);$$

such a θ exists for every q and $\mathbb{F}_{q^3} = \mathbb{F}_q(\theta)$. We denote by σ the $\mathbb{F}_q$-automorphism of $\mathbb{F}_{q^3}$ defined by $\sigma\theta = \theta^q$ and by a, b the points of $\mathrm{Proj}^3(\mathbb{F}_{q^3})$ respectively with $(\theta, \sigma\theta, \sigma^2\theta, 1)$, $(\theta, \sigma^2\theta, \sigma\theta, 0)$ as their homogeneous coordinates. We further denote by L, L', L'' the lines in Proj^3 respectively through $\{a, b\}$, $\{\sigma a, \sigma b\}$, $\{\sigma^2 a, \sigma^2 b\}$. Then by the choice of θ we see that L, L', L'' are mutually disjoint, σ gives a permutation $L \mapsto L'$, $L' \mapsto L''$, $L'' \mapsto L$, and their union X is a smooth everywhere 1-dimensional projective $\mathbb{F}_q$-variety. Since $\mathrm{card}(\mathrm{Proj}^1(\mathbb{F}_q)) = 1 + q$ for every q, we get $\mathrm{card}(X(\mathbb{F}_{q^e})) = 3(1 + q^e)$ or 0 according as $e \geq 1$ is in $3\mathbb{Z}$ or not. If ζ is any element of $\mathbb{C}$ satisfying $1 + \zeta + \zeta^2 = 0$, then we can write

$$\mathrm{card}(X(\mathbb{F}_{q^e})) = (1 + \zeta^e + \zeta^{2e})(1 + q^e)$$

for every $e \geq 1$. Therefore, $B_0 = B_2 = 3$, $B_1 = 0$, $\{\alpha_{01}, \alpha_{02}, \alpha_{03}\} = \{1, \zeta, \zeta^2\}$, and $\{\alpha_{21}, \alpha_{22}, \alpha_{23}\} = \{q, \zeta q, \zeta^2 q\}$. In the general case the situation, hence also the proof, is entirely similar.

11.5 Degree of $Z(s)$

We shall start with the following problem proposed in [25]: Assume that a homogeneous polynomial $f(x)$ with coefficients in O_K has a good reduction mod π; do we then always have $\deg_t(Z(s)) + \deg(f) = 0$? If we start with a homogeneous polynomial $f(x)$ with coefficients in an algebraic number field k, then we can ask the above relation for almost all p-adic completions K of k thus avoiding the use of "good reduction mod π". We recall that if the critical set C_f of f is contained in $\{0\}$, i.e., if the discriminant of $f(x)$ is not 0, then Proposition 10.2.1 implies that the answer is affirmative. In fact this is one of the examples which motivated the above problem. Now D. Meuser [42] showed more generally that the answer is affirmative if C_f is contained in the union of the coordinate hyperplanes. In connection with other examples, we remark that if $f(x)$ is a basic relative invariant of an irreducible regular prehomogeneous vector space, this condition on C_f implies $\deg(f) \leq 2$. In the general case, i.e., for an arbitrary homogeneous polynomial $f(x)$ in $k[x]\backslash k$, the problem was settled by J. Denef [9]. In the following we shall explain how Denef solved the problem.

We shall use the same notation as in section 11.3 and, in fact, the setup after Theorem 11.3.1. We recall that $f(x)$ is arbitrary in $k[x]\backslash k$, Y is a closed smooth n-dimensional k-subvariety of $X \times \mathrm{Proj}^m$, and $h : Y \to X$ is a Hironaka's desingularization of the hypersurface in $X = \mathrm{Aff}^n$ defined by $f(x)$. Furthermore, the p-adic completion K of k satisfies the condition that the homomorphism

$O_K \to \mathbb{F}_q = O_K/\pi O_K$ can be applied to the coefficients of a finite number of polynomial identities which describe the above desingularization to give a Hironaka's desingularization $\bar{h} : \bar{Y} \to \bar{X}$ of the hypersurface in $\bar{X} = \mathrm{Aff}^n$ defined by the image $\bar{f}(x)$ of $f(x)$ in $\mathbb{F}_q[x]$. We observe that $\mathrm{Proj}^m(K)$ can also be defined as the factor space of $O_K^{m+1} \backslash \pi O_K^{m+1}$ by $O_K^\times$ and that it is covered by $(Z_\alpha)^\circ$ consisting of all points with homogeneous coordinates in O_K and the α-th coordinate equal to 1 for $1 \le \alpha \le m+1$. We denote $\mathrm{Proj}^m(K)$ with the above open covering by $(\mathrm{Proj}^m)^\circ$, $X(O_K) = O_K^n$ by X°, put

$$(X \times \mathrm{Proj}^m)^\circ = X^\circ \times (\mathrm{Proj}^m)^\circ, \qquad (X \times Z_\alpha)^\circ = X^\circ \times (Z_\alpha)^\circ,$$

and define Y°, $(Y_\alpha)^\circ$ as their respective intersections with $Y(K)$ for all α. We introduce the coordinates $(t_1, \dots, t_{m+n})$ as in section 11.3 and identify $(X \times Z_\alpha)^\circ$ with O_K^{m+n}. If we denote by $(Y_{\alpha\beta})^\circ$ the open subset of $(Y_\alpha)^\circ$ consisting of all b such that $g_\beta(b)$ is a unit of O_K, i.e., the set of all b in O_K^{m+n} satisfying $h_1(b) = \dots = h_m(b) = 0$ and $g_\beta(b)$ in $O_K^\times$, then $(Y_\alpha)^\circ$ becomes the union of $(Y_{\alpha\beta})^\circ$ for all β. We keep in mind that X° and Y° are compact n-dimensional K-analytic manifolds.

We shall restrict our attention to $h|Y^\circ : Y^\circ \to X^\circ$ and also to $\bar{h}|\bar{Y}(\mathbb{F}_q) : \bar{Y}(\mathbb{F}_q) \to \bar{X}(\mathbb{F}_q)$ sometimes without explicitly saying so. We denote by dx the normalized Haar measure on X° and by μ_Y the measure on Y° defined by $h^*(dx_1 \wedge \dots \wedge dx_n)$ as in Chapter 7.4. We take a arbitrarily from X° and for $\mathrm{Re}(s) > 0$ we put

$$Z_a(s) = \int_{a+\pi X^\circ} |f(x)|_K^s \, dx = \int_{h^{-1}(a+\pi X^\circ)} |f(h(y))|_K^s \, \mu_Y(y).$$

We observe that $Z_a(s)$ depends on the image $\bar{a}$ of a in $\bar{X}(\mathbb{F}_q)$ rather than a itself. If we take any b from $h^{-1}(a + \pi X^\circ)$, then b is in $(Y_{\alpha\beta})^\circ$ for some α, β. We observe that if b' is any point of Y° with the same image in $\bar{Y}(\mathbb{F}_q)$ as b, then b' is also in $(Y_{\alpha\beta})^\circ$ because b' is in $(Y_\alpha)^\circ$ and $g_\beta(b')$ is a unit of O_K. Furthermore,

$$(\partial(f_1, \dots, f_n, h_1, \dots, h_m)/\partial(t_1, \dots, t_{m+n}))(b)$$

is also a unit of O_K. Therefore if we put $b' = b + \pi y$, where y is a variable in O_K^{m+n}, then by Lemma 7.4.3 we see that the correspondence

$$b' \mapsto (f_1(b'), \dots, f_n(b'), h_1(b'), \dots, h_m(b'))$$

gives a K-bianalytic map from $b + \pi O_K^{m+n}$ to $c + \pi O_K^{m+n}$, in which c is the image of b. Furthermore, if we introduce z_i as $f_i(b') = c_i + \pi z_i$ for $1 \le i \le n$, where $c = (c_1, \dots, c_{m+n})$, then the set of all b' in Y° having the same image as b in $\bar{Y}(\mathbb{F}_q)$ becomes K-bianalytic to O_K^n under the correspondence $b' \mapsto (z_1, \dots, z_n)$. Therefore, if I is the set of all i satisfying $\bar{f}_i(\bar{b}) = 0$, then after replacing $\pi^{-1}c_i + z_i$ by z_i we get

$$|f(h(b + \pi y))|_K = |\varepsilon \cdot \prod_{i \in I} f_i(b + \pi y)^{N_i}|_K = \prod_{i \in I} |\pi z_i|_K^{N_i},$$

$$\mu_Y(b + \pi y) = |\eta \cdot \prod_{i \in I} f_i(b + \pi y)^{n_i - 1}|_K \cdot q^{-n} dz = q^{-n} \cdot \prod_{i \in I} |\pi z_i|_K^{n_i - 1} \cdot dz.$$

This implies

$$Z_a(s) = q^{-n} \cdot \sum_{\bar{b}} \int_{O_K^n} \prod_{i \in I} |\pi z_i|_K^{N_i s + n_i - 1} \, dz,$$

in which the summation is over the set $\bar{h}^{-1}(\bar{a})(\mathbb{F}_q)$ and I for each $\bar{b}$ can be identified with the set of all $\bar{E}$'s which contain $\bar{b}$. Since the integral of $|z|_K^{s-1}$ over O_K is $(1-q^{-1})/(1-q^{-s})$, the above formula implies the following *theorem of Denef*:

Theorem 11.5.1 *Take an arbitrary subset I of $\mathcal{E}$ and a point a of X° with its image $\bar{a}$ in $\bar{X}(\mathbb{F}_q)$; denote by $c_I = c_I(\bar{a})$ the number of all $\bar{b}$ in $\bar{h}^{-1}(\bar{a})(\mathbb{F}_q)$ such that $\bar{b}$ is in $\bar{E}(\mathbb{F}_q)$ if and only if E is in I. Then*

$$Z_a(s) = \int_{a+\pi X^\circ} |f(x)|_K^s \, dx = q^{-n} \cdot \sum_I c_I \cdot \prod_{E \in I} ((q-1)/(q^{N_E s + n_E} - 1)).$$

Corollary 11.5.1 *We have*

$$\lim_{\mathrm{Re}(s) \to -\infty} q^n Z_a(s) \equiv 1 \mod q$$

in the sense that the LHS is in $1 + q\mathbb{Z}$.

Proof. If $\mathrm{char}(\mathbb{F}_q) = p$, since $(1+q\mathbb{Z}_p) \cap \mathbb{Z} = 1 + q\mathbb{Z}$, we have only to show that the LHS is both in $1 + q\mathbb{Z}_p$ and in $\mathbb{Z}$. By definition, we have

$$q^n Z_a(0) = q^n \cdot \lim_{s \to 0} \int_{a+\pi X^\circ} |f(x)|_K^s \, dx = q^n \cdot q^{-n} = 1$$

and by Theorem 11.5.1 we also have

$$q^n Z_a(0) = \sum_I c_I \cdot \prod_{E \in I} \big((q-1)/(q^{n_E} - 1)\big) \equiv \sum_I c_I \mod q\mathbb{Z}_p.$$

On the other hand again by Theorem 11.5.1 we have

$$\lim_{\mathrm{Re}(s) \to -\infty} q^n Z_a(s) = \sum_I c_I (1-q)^{\mathrm{card}(I)} \equiv \sum_I c_I \mod q,$$

and $\sum c_I \equiv 1 \mod q\mathbb{Z}_p$.

Corollary 11.5.2 *If $f(x)$ is homogeneous and $t = q^{-s}$, then*

$$\deg_t(Z(s)) = -\deg(f).$$

Proof. Put $\deg(f) = d$. Then, as in Chapter 10.3, we have

$$Z(s) = (1 - q^{-n} t^d)^{-1} \cdot \int_{X^\circ \setminus \pi X^\circ} |f(x)|_K^s \, dx.$$

Therefore, by Corollary 11.5.1 we get

$$\lim_{|t| \to \infty} t^d Z(s) = - \lim_{\mathrm{Re}(s) \to -\infty} q^n \cdot \int_{X^\circ \setminus \pi X^\circ} |f(x)|_K^s \, dx \equiv -(q^n - 1) \equiv 1 \mod q.$$

Consequently, the above limit is finite and different from 0. Since $Z(s)$ is a rational function of t, this implies that $\deg_t(Z(s)) = -d$.

Corollary 11.5.3 *If we put*

$$\bar{E}_I = \bigcap_{E\in I} \bar{E}, \qquad \bar{E}_I^0 = \bar{E}_I \backslash \Big(\bigcup_{E\notin I} \bar{E}\Big),$$

then we have

$$Z(s) = q^{-n} \cdot \sum_I \operatorname{card}(\bar{E}_I^0(\mathbb{F}_q)) \cdot \prod_{E\in I} \big((q-1)/(q^{N_E s+n_E}-1)\big).$$

Proof. In the notation of Theorem 11.5.1 we have

$$\sum_{\bar{a}\in \bar{X}(\mathbb{F}_q)} c_I(\bar{a}) = \sum_{\bar{a}\in \bar{X}(\mathbb{F}_q)} \operatorname{card}\big\{\bar{b}\in \bar{E}_I^0(\mathbb{F}_q);\ \bar{b}\in \bar{h}^{-1}(\bar{a})\big\} = \operatorname{card}(\bar{E}_I^0(\mathbb{F}_q)).$$

This implies the corollary.

We might mention that if $I = \emptyset$, then

$$\operatorname{card}(\bar{E}_I^0(\mathbb{F}_q)) = \operatorname{card}\big(\bar{Y}(\mathbb{F}_q)\backslash\big(\bigcup_{E\in\mathcal{E}} \bar{E}(\mathbb{F}_q)\big) = \operatorname{card}\big(\bar{X}(\mathbb{F}_q)\backslash \bar{f}^{-1}(0)(\mathbb{F}_q)\big).$$

Therefore, the contribution of $I = \emptyset$ to $Z(s)$ is $1 - q^{-n}\cdot \operatorname{card}(\bar{f}^{-1}(0)(\mathbb{F}_q))$.

11.6 The field K_e (a digression)

We shall prove, just for the sake of completeness, some basic facts on algebraic extensions of p-adic fields. In a fixed algebraically closed field there exists a unique extension of $\mathbb{F}_q$ of any given degree $e \geq 1$, i.e., $\mathbb{F}_{q^e}$. The corresponding statement for a p-adic field is as follows:

Theorem 11.6.1 *Let K denote a p-adic field with $\mathbb{F}_q$ as its residue class field. Then in a fixed algebraically closed field there exists a unique extension K_e of K of any given degree $e \geq 1$ with $\mathbb{F}_{q^e}$ as its residue class field.*

We shall give a classical proof by using Hensel's lemma. We shall also prove the fact that any extension of K of finite degree is a p-adic field. We shall start with a simple remark; for the time being the finiteness of the residue class field $F = O_K/\pi O_K$ will not be used.

We take an element A of $M_{m,n}(O_K)$ for any $m,\ n \geq 1$ and denote by $\bar{A}$ its image in $M_{m,n}(F)$. If $\bar{A}\bar{x} = \bar{y}$ is solvable by $\bar{x}$ in F^n for every $\bar{y}$ in F^m, then $Ax = y$ is solvable by x in O_K^n for every y in O_K^m. In fact, the above solvability of $\bar{A}\bar{x} = \bar{y}$ is equivalent to $\operatorname{rank}(\bar{A}) = m$ necessarily with $m \leq n$, and this is equivalent by Lemma 7.4.1 to the existence of g, h respectively in $\mathrm{GL}_m(O_K)$, $\mathrm{GL}_n(O_K)$ satisfying $A = g(1_m\ 0)h$. Then the equation $Ax = y$ can be rewritten as $(1_m\ 0)hx = g^{-1}y$. We may clearly replace hx, $g^{-1}y$ respectively by x, y. Then the equation becomes $(1_m\ 0)x = y$, which is solvable.

If now $f(t)$, etc. are elements of $O_K[t]$, where t is a variable, we shall denote their images in $F[t]$ by $\bar{f}(t)$, etc. We take $g_0(t)$, $h_0(t)$ from $O_K[t]$ such that $\bar{g}_0(t)$,

$\bar{h}_0(t)$ are relatively prime and $\bar{g}_0(t) \neq 0$, $\deg(\bar{g}_0) = \deg(g_0)$. Also, we fix an integer $d \geq \deg(g_0 h_0)$ and take any $c(t)$ from $O_K[t]$ with $\deg(c) \leq d$. Then there exist $a(t)$, $b(t)$ in $O_K[t]$ satisfying

$$a(t)h_0(t) + b(t)g_0(t) = c(t), \qquad \deg(a) < \deg(\bar{g}_0), \qquad \deg(b) \leq d - \deg(\bar{g}_0).$$

In fact, since $\bar{g}_0(t)$, $\bar{h}_0(t)$ are relatively prime, we have

$$\bar{a}(t)\bar{h}_0(t) + \bar{b}(t)\bar{g}_0(t) = \bar{c}(t)$$

for some $\bar{a}(t)$, $\bar{b}(t)$ in $F[t]$. By replacing $\bar{a}(t)$ by its residue mod $\bar{g}_0(t)$, we may assume that $\deg(\bar{a}) < \deg(\bar{g}_0)$. We then have $\deg(\bar{b}) \leq d - \deg(\bar{g}_0)$. Therefore, we have only to apply the above remark with $m = n = d+1$ to the coefficients of $a(t)$, $b(t)$ as x and the coefficients of $c(t)$ as y. We are ready to prove *Hensel's lemma*, which is as follows:

Lemma 11.6.1 *Let $f(t)$ denote any element of $O_K[t]\backslash O_K$ such that its image $\bar{f}(t)$ in $F[t]$, where $F = O_K/\pi O_K$, splits as $\bar{f}(t) = \bar{g}_0(t)\bar{h}_0(t)$, in which $\bar{g}_0(t)$, $\bar{h}_0(t)$ are relatively prime and $\bar{g}_0(t) \neq 0$. Then there exist $g(t)$, $h(t)$ in $O_K[t]$ with* $\deg(g) = \deg(\bar{g}_0)$ *satisfying*

$$f(t) = g(t)h(t), \qquad \bar{g}(t) = \bar{g}_0(t), \qquad \bar{h}(t) = \bar{h}_0(t).$$

Proof. We shall exclude the trivially simple case where $\bar{f}(t) = 0$, hence $\bar{h}_0(t) = 0$. We put $d = \deg(f)$ and choose $g_0(t)$, $h_0(t)$ from $O_K[t]$ with $\bar{g}_0(t)$, $\bar{h}_0(t)$ as their images in $F[t]$ and satisfying $\deg(g_0) = \deg(\bar{g}_0)$, $\deg(h_0) = \deg(\bar{h}_0)$. That is clearly possible and $d \geq \deg(\bar{f}) = \deg(\bar{g}_0\bar{h}_0) = \deg(g_0 h_0)$. We introduce unknown elements $g_i(t)$, $h_i(t)$ of $O_K[t]$ satisfying

$$\deg(g_i) < \deg(\bar{g}_0), \qquad \deg(h_i) \leq d - \deg(\bar{g}_0)$$

for $i = 1, 2, 3, \ldots$ and put

$$g(t) = \sum_{i \geq 0} \pi^i g_i(t), \qquad h(t) = \sum_{i \geq 0} \pi^i h_i(t).$$

We have only to show that the equation $f(t) = g(t)h(t)$ is solvable. If we put $c_1(t) = \pi^{-1}(f(t) - g_0(t)h_0(t))$ and $c_k(t) = 0$ for $k > 1$, then $c_k(t)$ is in $O_K[t]$ and $\deg(c_k) \leq d$ for every k. Furthermore, the equation $g(t)h(t) = f(t)$ can be replaced by the following sequence of equations:

$$g_k(t)h_0(t) + h_k(t)g_0(t) = c_k(t) - \sum_{0<i<k} g_i(t)h_{k-i}(t)$$

for $k = 1, 2, 3, \ldots$. The first equation is $g_1(t)h_0(t) + h_1(t)g_0(t) = c_1(t)$, which is solvable in $g_1(t)$, $h_1(t)$ by the previous observation. Therefore, we shall apply an induction on k assuming that $k > 1$. Then in the k-th equation, the RHS is an already known polynomial in $O_K[t]$ of degree at most d, hence for the same reason it is also solvable in $g_k(t)$, $h_k(t)$.

Corollary 11.6.1 *If $f_0(t)$ is an irreducible monic polynomial in $K[t]$ with $f_0(0)$ in O_K, then necessarily $f_0(t)$ is in $O_K[t]$.*

Proof. Put $d = \deg(f_0)$ and assume that $f_0(t)$ is not in $O_K[t]$. Choose the smallest integer e so that $f(t) = \pi^e f_0(t)$ is in $O_K[t]$. Then $e > 0$, $\deg(f) = d$, and $0 < \deg(\bar{f}) < d$. In Lemma 11.6.1 we can take $\bar{g}_0(t) = \bar{f}(t)$, $\bar{h}_0(t) = 1$ and we get $f(t) = g(t)h(t)$ with $0 < \deg(g) < d$. This implies that $f_0(t)$ is reducible in $K[t]$, a contradiction.

Proposition 11.6.1 *Let K denote a complete nonarchimedean field with πO_K for some $\pi = \pi_K$ as the ideal of nonunits of O_K; let L denote a finite extension of K. Then L is also a complete nonarchimedean field with $\pi_L O_L$ for some π_L as the ideal of nonunits of O_L. Furthermore, if we define r, e as*

$$\pi O_L = \pi_L^r O_L, \qquad [O_L/\pi_L O_L : O_K/\pi O_K] = e,$$

then $[L : K] = re$.

Proof. We shall first show that L has a nonarchimedean absolute value $|\cdot|_L$ satisfying $|a|_L = |a|_K^n$ for every a in K, where $n = [L : K]$. We start with a review of the norm N from L to K for any field K. We choose a K-basis $u_1, \ldots, u_n$ for L. Then we get a K-algebra homomorphism $\rho : L \to M_n(K)$ as

$$\alpha(u_1 \ldots u_n) = (u_1 \ldots u_n)\rho(\alpha).$$

Since $\rho(\alpha)$ is unique up to $\rho(\alpha) \mapsto g\rho(\alpha)g^{-1}$ for some g in $\mathrm{GL}_n(K)$ coming from a change of the K-basis for L, $N\alpha = \det(\rho(\alpha))$ is well defined. Furthermore, $N(\alpha\beta) = (N\alpha)(N\beta)$ for every α, β in L. We need another property of $N\alpha$. If $f_0(t)$ is the irreducible monic polynomial in $K[t]$ of degree d satisfying $f_0(\alpha) = 0$, then $1, \alpha, \ldots, \alpha^{d-1}$ form a K-basis for $K(\alpha)$. If we compute the norm $N_0\alpha$ of α from $K(\alpha)$ to K by using this basis, we get $N_0\alpha = (-1)^d f_0(0)$. If we choose a $K(\alpha)$-basis $v_1, \ldots, v_e$ for L, then

$$v_1,\ \alpha v_1, \ldots, \alpha^{d-1}v_1, \ldots, v_e,\ \alpha v_e, \ldots, \alpha^{d-1}v_e$$

form a K-basis for L so that $n = de$. If we compute $N\alpha$ by using this basis, we get

$$N\alpha = (N_0\alpha)^e = (-1)^n f_0(0)^e.$$

We now go back to our field K, and in the above notation we put

$$|\alpha|_L = |N\alpha|_K = |f_0(0)|_K^e.$$

Then $|a|_L = |a|_K^n$ for every a in K. Furthermore, $|\cdot|_L$ satisfies AV 1, AV 2 in Chapter 2.1. We shall show that it also satisfies AV 3′ in Chapter 2.2. Since $|\alpha\beta|_L = |\alpha|_L|\beta|_L$ for every α, β in L, we have only to show that $|\alpha + 1|_L \leq 1$ if $|\alpha|_L \leq 1$. Since $|\alpha|_L \leq 1$ implies $|f_0(0)|_K \leq 1$, by the above corollary $f_0(t)$ is in $O_K[t]$. Furthermore, $f_1(t) = f_0(t-1)$ is also an irreducible monic polynomial of degree d in $K[t]$ with coefficients in $O_K[t]$ and $f_1(\alpha + 1) = f_0(\alpha) = 0$. Since $f_1(0) = f_0(-1)$ is in O_K, we have $|\alpha + 1|_L = |f_1(0)|_K^e \leq 1$.

We shall show that L is complete, i.e., every Cauchy sequence $\{\alpha_i\}$ in L is convergent. We say that a sequence is zero if its terms are all zero. If we write

$$\alpha_i = \sum_{1\le j\le n} a_{ij}u_j$$

with a_{ij} in K for all i, j then, since K is complete, we have only to show that $\{a_{i1}\},\dots,\{a_{in}\}$ are all Cauchy sequences in K. If k denotes the number of nonzero sequences among them, the statement clearly holds for $k\le 1$. We shall therefore assume that $k>1$ and apply an induction on k. If we can derive a contradiction from the assumption that one of the k sequences is not a Cauchy sequence, then the induction will be complete. By converting the double sequence $\{\alpha_i-\alpha_j\}$ into a sequence and replacing it by a subsequence, we may assume that $\{\alpha_i\}$ is a null sequence in L while the absolute values of all terms of one of the k sequences in K are at least $\epsilon>0$. After a permutation of $u_1,\dots,u_n$, we may assume that $\{a_{i1}\},\dots,\{a_{ik}\}$ are the nonzero sequences and $|a_{ik}|_K\ge\epsilon$ for all i. Then the sequence in L with

$$\alpha_i/a_{ik}-u_k=\sum_{1\le j<k}(a_{ij}/a_{ik})u_j$$

as its i-th term is convergent, hence a Cauchy sequence, and hence the coefficients of $u_1,\dots,u_{k-1}$ form Cauchy sequences in K by induction. If we denote their limits by $b_1,\dots,b_{k-1}$, we get $b_1u_1+\ldots+b_{k-1}u_{k-1}+u_k=0$. This contradicts the fact that $u_1,\dots,u_n$ form a K-basis for L.

Finally, since the image of $L^\times$ under $|\cdot|_L$ is a subgroup of the image of $K^\times$ under $|\cdot|_K$, it is discrete. Therefore, the ideal of nonunits of O_L can be written as π_LO_L, and $\pi O_L=\pi_L^rO_L$ for some positive integer r. On the other hand, if $w_1,\dots,w_e$ are the elements of O_L such that their images $\bar w_1,\dots,\bar w_e$ in O_L/π_LO_L are linearly independent over $F=O_K/\pi O_K$, then $w_1,\dots,w_e$ are linearly independent over K, hence $e\le[L:K]$. We shall assume that $\bar w_1,\dots,\bar w_e$ form an F-basis for O_L/π_LO_L. Since

$$1,\ \pi_L,\dots,\pi_L^{r-1},\ \pi,\ \pi\pi_L,\dots,\pi\pi_L^{r-1},\dots$$

are elements of O_L whose orders are respectively $0,\ 1,\ 2,\dots$, every element α of O_L can be written as

$$\alpha=\sum_{0\le i<r}\ \sum_{1\le j\le e}a_{ij}w_j\pi_L^i$$

with a_{ij} in O_K for all i, j. We shall show that the expression is unique. We have only to show that if the RHS is 0, then $a_{ij}=0$ for all i, j. Suppose that the RHS is 0 for some a_{ij} in O_K not all 0. Then, after cancelling a power of π, we may assume that they are not all in πO_K, hence their images $\bar a_{ij}$ in $O_K/\pi O_K$ are not all 0. If we take the image of the RHS in O_L/π_LO_L, then we get $\bar a_{01}\bar w_1+\ldots+\bar a_{0e}\bar w_e=0$, hence $\bar a_{0j}=0$, and hence $a_{0j}=\pi b_{0j}$ with b_{0j} in O_K for all j. We can repeat the same argument after cancelling π_L, and we get $a_{1j}=\pi b_{1j}$ with b_{1j} in O_K for all j. By continuing this process, we will see that all a_{ij} are in πO_K, a contradiction. If we allow a_{ij} to have a power of π as a denominator, then every α in L can be expressed uniquely as above with a_{ij} in K. We have thus shown that $[L:K]=re$.

In the above proposition if K is a p-adic field, i.e., if $F = O_K/\pi O_K$ is finite, then $O_L/\pi_L O_L$ is also finite, hence L is a p-adic field. Furthermore, if $|\cdot|_K$ is normalized as $|\pi|_K = q^{-1}$, then $|\cdot|_L$ is normalized as $|\pi_L|_L = q_L^{-1}$, in which $q = \mathrm{card}(O_K/\pi O_K)$ and $q_L = \mathrm{card}(O_L/\pi_L O_L)$. This follows from $[L : K] = re$. We might mention that the standard notation for r and e are respectively "e" and "f." At any rate, we say that L is *unramified* if $r = 1$. Theorem 11.6.1 then states the unique existence of an unramified extension K_e of K of any given degree $e \geq 1$. The proof is as follows:

We shall start with the existence of K_e. We put

$$P(t) = t^{e^*} - 1 = \prod_{\zeta}(t - \zeta),$$

where $e^* = q^e - 1$, denote by W the set of all ζ above, and put $L = K(W)$. We shall show that $L = K_e$. We know by Proposition 11.6.1 that L is a p-adic field. We observe that W forms a cyclic group and it is mapped isomorphically, say, to $\bar{W}$ under the homomorphism $O_L \to O_L/\pi_l O_L$. Since $\mathbb{F}_{q^e} = \mathbb{F}_q(\bar{W})$, it is contained in $O_L/\pi_L O_L$, hence

$$e = [\mathbb{F}_{q^e} : \mathbb{F}_q] \leq [O_L/\pi_L O_L : \mathbb{F}_q] \leq [L : K].$$

Therefore, if we can show that $[L : K] = e$, then $O_L/\pi_L O_L = \mathbb{F}_{q^e}$ and $L = K_e$. We take a generator ζ of W and denote by $f(t)$ the irreducible monic polynomial in $K[t]$ satisfying $f(\zeta) = 0$. Since $f(t)$ is a factor of $P(t)$, a power of $f(0)$ is 1, hence $|f(0)|_K = 1$, and hence $f(t)$ is in $O_K[t]$ by Corollary 11.6.1. Furthermore, $\deg(f) = [L : K]$. If $\bar{\zeta}$ is the image of ζ in $\bar{W}$, then $\mathbb{F}_q(\bar{\zeta}) = \mathbb{F}_{q^e}$. Therefore, $\bar{f}(t)$ has a factor of degree e in $\mathbb{F}_q[t]$. Since $\bar{f}(t)$ splilts into a product of distinct linear factors in $\mathbb{F}_{q^e}[t]$, by Lemma 11.6.1 we see that $f(t)$ has a factor of degree e in $O_K[t]$, hence $\deg(f) = e$.

We shall prove the uniqueness of K_e. Namely, if M is any extension of K of degree e satisfying $O_M/\pi_M O_M = \mathbb{F}_{q^e}$, then $M = L$. We observe that the above $f(t)$ is in $O_M[t]$ and that $f(t)$ splits into linear factors in $O_M[t]$ by Lemma 11.6.1. Therefore ζ is in O_M, hence L is contained in M. Since they have the same degree over K, we get $M = L$.

11.7 Functional equation of $Z(s)$

We shall start with the following conjecture proposed in the preliminary but preprinted form of Part I of [29] which is mentioned in its introduction:

"(F1) $f(x)$ is a homogeneous polynomial in $O_K[x_1, \ldots, x_n]$ with good reduction mod π;

(F2) there exists an element $Z(u, v)$ of $\mathbb{Q}(u, v)$ such that for every finite algebraic extension L of K and $\mathrm{Re}(s) > 0$ we have

$$\int_{O_L^n} |f(x)|_L^s \, dx = Z(q_L^{-1}, q_L^{-s}).$$

.... It is very likely that the two conditions are sufficient for the functional equation $Z(u^{-1}, v^{-1}) = v^{\deg(f)} \cdot Z(u, v)$." The conjecture was investigated by D. Meuser by using Denef's formula in Theorem 11.5.1 and, under a certain condition on the numerical data, was settled by her discovery of the relation between the conjectural functional equation and the functional equations of Weil's zeta functions over finite fields. Later J. Denef succeeded in removing this condition and his proof was simplified by J. Oesterlé. We shall explain Denef-Meuser's joint paper [10] on this subject. As we shall see, their results go much further than the conjecture. We refer to their paper for more detailed history and further important results.

Lemma 11.7.1 *Let A_i denote a subset of a finite set S for all i in an index set I_0 and I, J subsets of I_0. Then for any given I, we have*

$$\mathrm{card}\Big(\big(\bigcap_{i\in I} A_i\big)\backslash\big(\bigcup_{i\notin I} A_i\big)\Big) = \sum_{J\supset I}(-1)^{\mathrm{card}(J\backslash I)}\mathrm{card}\big(\bigcap_{i\in J} A_i\big).$$

Proof. We take a arbitrarily from S and show that a contributes the same number to both sides of the identity. Now a is contained in $A_{i_1}, \ldots, A_{i_p}$ for some $i_1, \ldots, i_p$ but not in A_i for any other i. First, suppose that I is not contained in $\{i_1, \ldots, i_p\}$, i.e., a is not contained in A_i for some i in I. Then, clearly, a contributes 0 to both sides. Next, suppose that I is contained in $\{i_1, \ldots, i_p\}$. We put $n = p - \mathrm{card}(I)$. If $n = 0$, i.e., $I = \{i_1, \ldots, i_p\}$, then a contributes 1 to both sides. If $n > 0$, then a contributes 0 to the LHS. On the other hand, a is contained in A_i for all i in J if and only if J is a subset of $\{i_1, \ldots, i_p\}$. Therefore, the contribution of a to the RHS is

$$\sum_{0\le j\le n}(-1)^j\binom{n}{j} = (1-1)^n = 0.$$

Lemma 11.7.2 *Let I_0 denote a finite index set, i an element of I_0, and I, J subsets of I_0; further, let x_i, y_J denote variables. Then we have*

$$\sum_I \Big\{\sum_{J\supset I}(-1)^{\mathrm{card}(J\backslash I)}y_J\Big\}\cdot\prod_{i\in I}x_i = \sum_I y_I\cdot\prod_{i\in I}(x_i-1).$$

Proof. We clearly have

$$\sum_I y_I\cdot\prod_{i\in I}(1+x_i) = \sum_I y_I\big(\sum_{J\subset I}\prod_{i\in J}x_i\big) = \sum_J\big(\sum_{I\supset J}y_I\big)\prod_{i\in J}x_i.$$

If we permute I, J on the RHS and replace x_i, y_I by $-x_i$, $(-1)^{\mathrm{card}(I)}y_I$ on both sides, then we get the identity in the lemma.

We shall use the same setup as in section 11.5, e.g., k is an algebraic number field, $f(x)$ is a homogeneous polynomial in $k[x]\backslash k$ of degree d, where $k[x] = k[x_1, \ldots, x_n]$, and $h : Y \to X = \mathrm{Aff}^n$ is a Hironaka's desingularization of the hypersurface in $\mathrm{Aff}^n = \Omega^n$ defined by $f(x)$. We now need a Hironaka's desingularization of the hypersurface in Proj^{n-1} defined by $f(x)$, which can be explained, e.g., as follows. We observe that every λ in $\Omega^\times$ gives an Ω-automorphism of $\Omega[x]$ as $x_i \mapsto \lambda x_i$ for $1 \le i \le n$. This gives rise to an action of $\Omega^\times$ on X under which the hypersurface

in X defined by $f(x)$ is invariant. The fact, which we accept, is that the above $h : Y \to X$ can be constructed in such a way that it is preserved under the action of $\Omega^\times$. We shall give some details. We recall that $X^* = \mathrm{Proj}^{n-1}$ is the factor space of $X\backslash\{0\}$ by $\Omega^\times$. If Y^* denotes the factor space of $Y\backslash h^{-1}(0)$ by $\Omega^\times$, then Y^* becomes a smooth $(n-1)$-dimensional k-subvariety of $X^* \times \mathrm{Proj}^m$ and h gives rise to a Hironaka's desingularization $h^* : Y^* \to X^*$ of the hypersurface in X^* defined by $f(x)$. Furthermore, if $\mathcal{E}'$ denotes the set of all E in $\mathcal{E}$ not contained in $h^{-1}(0)$, then for every E in $\mathcal{E}'$ the factor space E^* of $E\backslash h^{-1}(0)$ by $\Omega^\times$ becomes a smooth $(n-2)$-dimensional k-subvariety of Y^*. More generally, for every subset I of $\mathcal{E}'$

$$E_I^* = \bigcap_{E\in I} E^*$$

is either empty or a smooth k-subvariety of Y^* of dimension $r_I = n - \mathrm{card}(I) - 1$. Furthermore, if K is a p-adic completion of k which we have used in section 11.5, then a similarly defined $\bar{E}_I^*$ becomes a smooth r_I-dimensional projective $\mathbb{F}_q$-variety and

$$\mathrm{card}(\bar{E}_I^*(\mathbb{F}_q)) = (q-1)^{-1} \cdot \mathrm{card}\big((\bar{E}_I\backslash\bar{h}^{-1}(0))(\mathbb{F}_q)\big).$$

On the other hand, if we put

$$x_E = (q-1)/(q^{N_E s + n_E} - 1),$$

then by applying Theorem 11.5.1 to the integral in

$$Z(s) = (1 - q^{-(ds+n)})^{-1} \cdot \int_{X^\circ\backslash\pi X^\circ} |f(x)|_K^s \, dx$$

we will have

$$\int_{X^\circ\backslash\pi X^\circ} |f(x)|_K^s \, dx = q^{-n} \sum_{I\subset\mathcal{E}'} \mathrm{card}\big((\bar{E}_I^0\backslash\bar{h}^{-1}(0))(\mathbb{F}_q)\big) \cdot \prod_{E\in I} x_E.$$

We shall now apply Lemmas 11.7.1, 11.7.2 to the above summation in I with $I_0 = \mathcal{E}'$, $A_E = (\bar{E}\backslash\bar{h}^{-1}(0))(\mathbb{F}_q)$, and

$$y_I = \mathrm{card}\big(\bigcap_{E\in I} A_E\big).$$

In doing so, we use the obvious fact that if S, S_0 are subsets of a set, then the operation $S \mapsto S\backslash S_0$ commutes with the taking of union, intersection, and difference. We see that $y_I = (q-1)\mathrm{card}(\bar{E}_I^*(\mathbb{F}_q))$ and that the above summation in I is equal to

$$(q-1) \cdot \sum_{I\subset\mathcal{E}'} \mathrm{card}(\bar{E}_I^*(\mathbb{F}_q)) \cdot \prod_{E\in I} (x_E - 1).$$

Since we shall be using only the desingularization $h^* : Y^* \to X^*$ of the hypersurface in $X^* = \mathrm{Proj}^{n-1}$ defined by $f(x)$, we change our notation and state the above result in the following self-contained form:

Theorem 11.7.1 *If $f(x)$ is a homogeneous polynomial of degree $d > 0$ in n variables with coefficients in an algebraic number field k, then there exists a finite set $\mathcal{E} = \{E\}$, where each E is equipped with a pair of positive integers (N_E, n_E), such that for almost all p-adic completion K of k we have*

$$\begin{aligned} Z(s) =&(q-1)q^{ds}/(q^{ds+n}-1) \\ &\cdot \sum_{I\subset\mathcal{E}} \operatorname{card}(\bar{E}_I(\mathbb{F}_q)) \cdot \prod_{E\in I} \big((q-1)/(q^{N_E s+n_E}-1)-1\big), \end{aligned}$$

in which every $\bar{E}_I$ is either empty or a smooth r_I-dimensional projective $\mathbb{F}_q$-variety for $r_I = n - \operatorname{card}(I) - 1$.

We keep in mind that we can replace the above K by any finite algebraic extension L, e.g., by K_e in Theorem 11.6.1. We shall now explain an observation by J. Oesterlé about the extendability of certain functions on $\mathbb{N}\backslash\{0\}$ to $\mathbb{Z}\backslash\{0\}$. It depends on the following lemma:

Lemma 11.7.3 *We denote by A the ring of functions on $\mathbb{N}\backslash\{0\}$ generated by $n \mapsto \alpha^n$ for all α in $\mathbb{C}^\times$, i.e., functions of the form*

$$\varphi(n) = \sum_{1\le i\le r} m_i \alpha_i^n$$

with m_i in $\mathbb{Z}$ and α_i in $\mathbb{C}^\times$ for $1 \le i \le r$, and for some $r \ge 0$. If $m_i \ne 0$ and $\alpha_i \ne \alpha_j$ for all i and $i \ne j$, then the set $\{(m_i, \alpha_i);\ 1 \le i \le r\}$ is uniquely determined by φ.

Proof. If φ is as above and t is a complex variable satisfying $|\alpha_i t| < 1$ for $1 \le i \le r$, then

$$\exp\Big\{\sum_{n>0} \varphi(n)t^n/n\Big\} = \prod_{1\le i\le r} (1-\alpha_i t)^{-m_i}.$$

We observe that the rational function of t so defined depends only on φ and that it has α_i^{-1} as a pole or a zero of order $|m_i|$ according to whether m_i is positive or negative for $1 \le i \le r$.

If now φ in A is expressed as in Lemma 11.7.3 possibly with $m_i = 0$ for some i and $\alpha_i = \alpha_j$ for some $i \ne j$, then the function $\varphi^\#$ on $\mathbb{Z}$ defined by the same expression for all n in $\mathbb{Z}$ depends only on φ. In order to prove this fact, we have only to show that $\varphi = 0$ implies $\varphi^\# = 0$. Let $\{\beta\}$ denote the set of distinct $\alpha_1, \dots, \alpha_r$ and for each β define m_β as the sum of all m_i for $\alpha_i = \beta$. Then $\varphi = 0$ implies $m_\beta = 0$ for all β by Lemma 11.7.3, hence

$$\varphi^\#(n) = \sum_{1\le i\le r} m_i \alpha_i^n = \sum_\beta m_\beta \beta^n = 0$$

for all n in $\mathbb{Z}$, and hence $\varphi^\# = 0$. As its immediate consequence, if we denote by $A^\#$ the set of all such $\varphi^\#$, then $A^\#$ forms a ring and the correspondence $\varphi \mapsto \varphi^\#$ gives an isomorphism from A to $A^\#$.

In the following we shall restrict n to $\mathbb{Z}\backslash\{0\}$ sometimes without saying so. We take a complex variable z and introduce the rings B, $B^{\#}$ of functions respectively on $\mathbb{C}^{\times} \times (\mathbb{N}\backslash\{0\})$, $\mathbb{C}^{\times} \times (\mathbb{Z}\backslash\{0\})$ consisting of

$$\sum_i \varphi_i(n) z^{in}, \qquad \sum_i \varphi_i^{\#}(n) z^{in},$$

in which φ_i is in A and $\varphi_i^{\#}$ is in $A^{\#}$ for all i in $\mathbb{N}$. We observe that B, $B^{\#}$ are commutative rings with 1 and the subsets S, $S^{\#}$ of B, $B^{\#}$ defined by the condition that $\sum \varphi_i^{\#}(n) z^{in} \neq 0$ for every n in $\mathbb{Z}\backslash\{0\}$ and for a variable z in $\mathbb{C}^{\times}$ are both multiplicative and free from zero divisors. Therefore, $C = S^{-1}B$, $C^{\#} = (S^{\#})^{-1}B^{\#}$ are defined, and C consists of elements of the form

$$\Phi(z, n) = \big(\sum_i \varphi_i(n) z^{in}\big) / \big(\sum_i \psi_i(n) z^{in}\big),$$

in which the denominator is in S. We shall show that the element

$$\Phi^{\#}(z, n) = \big(\sum_i \varphi_i^{\#}(n) z^{in}\big) / \big(\sum_i \psi_i^{\#}(n) z^{in}\big)$$

of $C^{\#}$ depends only on $\Phi(z, n)$. In fact if $\Phi(z, n)$ is expressed similarly as

$$\Phi(z, n) = \big(\sum_i \varphi_i'(n) z^{in}\big) / \big(\sum_i \psi_i'(n) z^{in}\big),$$

then we get $\sum(\varphi_i \psi_j' - \psi_i \varphi_j') = 0$ where the summation is in i, j in $\mathbb{N}$ satisfying $i + j = k$ for every k in $\mathbb{N}$. This implies $\sum(\varphi_i^{\#}(\psi_j')^{\#} - \psi_i^{\#}(\varphi_j')^{\#}) = 0$ for the same summation $i + j = k$ for every k, hence

$$\Phi^{\#}(z, n) = \big(\sum_i (\varphi_i')^{\#}(n) z^{in}\big) / \big(\sum_i (\psi_i')^{\#}(n) z^{in}\big).$$

We now go back to Theorem 11.7.1 and replace K there by $L = K_e$. If we denote the corresponding $Z_L(s)$ by $Z_e(s)$, then we get

$$Z_e(s) = R(e) \cdot \sum_{I \subset \mathcal{E}} \operatorname{card}\big(\bar{E}_I(\mathbb{F}_{q^e})\big) R_I(e),$$

in which

$$R(e) = (q^e - 1) q^{des} / (q^{e(ds+n)} - 1),$$
$$R_I(e) = \prod_{E \in I} \big((q^e - 1)/(q^{e(N_E s + n_E)} - 1) - 1\big)$$

for all e in $\mathbb{N}\backslash\{0\}$. We recall that $\bar{E}_I$ is either empty or a smooth projective $\mathbb{F}_q$-variety of dimension $r_I = n - \operatorname{card}(I) - 1$. Therefore, Theorem 11.4.1 is applicable to $\bar{E}_I$. In that way, we get

$$\operatorname{card}(\bar{E}_I(\mathbb{F}_{q^e})) = \sum_{0 \leq i \leq 2r_I} \sum_{1 \leq j \leq B_{Ii}} (-1)^i \alpha_{Iij}^e$$

for some α_{Iij} in $\mathbb{C}^\times$ with the property

$$(*) \qquad \{q^{r_I}/\alpha_{Iij};\ 1 \le j \le B_{Ii}\} = \{\alpha_{I,2r_I-i,j};\ 1 \le j \le B_{I,2r_I-i} = B_{Ii}\}$$

for $0 \le i \le 2r_I$. If in the above-explained observation by Oesterlé we use e as n and q^s as z, then the denominator

$$(q^{e(ds+n)} - 1) \prod_{E \in \mathcal{E}} (q^{e(N_E s + n_E)} - 1)$$

of $Z_e(s)$ is in S, hence $Z_e(s)$ is in C. Therefore, $Z_e(s)$ extends to an element $Z(s,e)$ of $C^\#$ where e is arbitrary in $\mathbb{Z}\backslash\{0\}$. Furthermore, $R(e)$, $R_I(e)$ also extend to elements of $C^\#$ and, as such, they satisfy

$$R(-e) = q^{-(ds-(n-1))e} R(e), \qquad R_I(-e) = q^{-\mathrm{card}(I)e} R_I(e).$$

By using these and $(*)$ above, we can easily verify that

$$Z(s,-e) = q^{-des} Z(s,e).$$

In this way, we get the following theorem of *Denef and Meuser*:

Theorem 11.7.2 *In the same situation as in Theorem 11.7.1, if for every $L = K_e$, where e in in $\mathbb{N}\backslash\{0\}$, we put*

$$Z_e(s) = \int_{O_L^n} |f(x)|_L^s \, dx,$$

then $e \mapsto Z_e(s)$ extends to a function $Z(s,e)$ on $\mathbb{Z}\backslash\{0\}$ satisfying the functional equation $Z(s,-e) = q^{-des} Z(s,e)$.

Corollary 11.7.1 *If there exists an element $Z(u,v)$ of $\mathbb{C}(u,v)$, where u, v are variables, satisfying $Z(q^{-e}, q^{-es}) = Z_e(s)$ for all $e > 0$ in $e_0\mathbb{Z}$ for some integer $e_0 > 0$, then the obviously unique $Z(u,v)$ satisfies the functional equation $Z(u^{-1}, v^{-1}) = v^d Z(u,v)$.*

Proof. In the notation of Theorem 11.7.2, we have

$$Z(q^e, q^{es}) = Z(s,-e) = q^{-des} Z(s,e) = (q^{-es})^d Z(q^{-e}, q^{-es})$$

for all $e > 0$ in $e_0\mathbb{Z}$ and for a variable s. This implies the functional equation in the corollary.

The above corollary completely settles the conjecture which we have recalled in the beginning of this section. We might mention that a certain p-adic zeta function associated with an algebraic group satisfies a functional equation of the same kind; cf. [29], pp. 708-709. It would be interesting to examine whether or not there exists a common ground for all such functional equations.

That concludes this introductory book to the theory of local zeta functions. As the last word, we would like to recommend to the readers to proceed to Denef's Bourbaki report [11] and our own expository paper [31] which we have mentioned in the Introduction. The readers will find in these references not only further important results but also problems whose solutions will undoubtedly enrich the theory.

Bibliography

[1] M. F. Atiyah, Resolution of singularities and division of distributions, Comm. Pure Appl. Math., 23 (1970), 145-150.

[2] I. N. Bernstein and S. I. Gel'fand, Meromorphic property of the functions P^λ, Functional Anal. Appl., 3 (1969), 68-69.

[3] I. N. Bernstein, The analytic continuation of generalized functions with respect to a parameter, Functional Anal. Appl., 6 (1972), 273-285.

[4] A. Borel and J.-P. Serre, Le théorème de Riemann-Roch, Bull. Soc. math. France, 86 (1958), 97-136.

[5] S. I. Borewicz and I. R. Šafarevič, Zahlentheorie, Birkhäuser (1966).

[6] F. Bruhat, Distributions sur un groupe localement compact et applications à l'étude des représentations des groupes p-adiques, Bull. Soc. math. France, 89 (1961), 43-75.

[7] C. Chevalley, The algebraic theory of spinors, Columbia Univ. Press (1954).

[8] P. Deligne, La conjecture de Weil, Inst. Hautes Études Sci. Publ. Math., 43 (1974), 273-307.

[9] J. Denef, On the degree of Igusa's local zeta function, Amer. J. Math., 109 (1987), 991-1008.

[10] J. Denef and D. Meuser, A functional equation of Igusa's local zeta functions, Amer. J. Math., 113 (1991), 1135-1152.

[11] J. Denef, Report on Igusa's local zeta functions, Sém. Bourbaki 741 (1991), 1-25; Asterisque No. 201-203, 359-386.

[12] L. E. Dickson, Linear groups with an exposition of the Galois field theory, B. G. Teubner (1901).

[13] C. Ehresmann, Sur la topologie de certains espaces homogènes, Ann. Math., 35 (1934), 396-443.

[14] H. Freudenthal, Beziehungen der E_7 und E_8 zur Oktavenebene. I, Prok. Konkl. Ned. Akad. Wet., A 57 (1954), 218-230.

[15] C. F. Gauss, Hundert Theoreme über die neuen Transscendenten, Werke III (1876), 461-469.

[16] I. M. Gel'fand and G. E. Shilov, Generalized functions. I, Academic Press (1964).

[17] G. B. Gurevich, Foundations of the theory of algebraic invariants, Noordhoff (1964).

[18] A. Gyoja, Functional equation for Igusa local zeta functions, JAMI lecture (1993).

[19] D. Hilbert, Über die vollen Invariantensysteme, Math. Ann. 42 (1893), 313-373.

[20] H. Hironaka, Resolution of singularities of an algebraic variety over a field of characteristic zero. I-II, Ann. Math., 79 (1964), 109-326.

[21] J. Igusa, Analytic groups over complete fields, Proc. Nat. Acad. Sci., 42 (1956), 540-541.

[22] J. Igusa, A classification of spinors up to dimension twelve, Amer. J. Math., 92 (1970), 997-1028.

[23] J. Igusa, Complex powers and asymptotic expansions. I, Crelles J. Math., 268/269 (1974), 110-130; II, ibid., 278/279 (1975), 307-321.

[24] J. Igusa, On the first terms of certain asymptotic expansions, Complex Analysis and Algebraic Geometry, Iwanami Shoten (1977), 357-368.

[25] J. Igusa, Some results on p-adic complex powers, Amer. J. Math., 106 (1984), 1013-1032.

[26] J. Igusa, Complex powers of irreducible algebroid curves, Geometry Today, Birkhäuser (1985) , 207-230.

[27] J. Igusa, On functional equations of complex powers, Invent. math., 85 (1986), 1-29.

[28] J. Igusa, On the arithmetic of a singular invariant, Amer. J. Math., 110 (1988), 197-233.

[29] J. Igusa, Universal p-adic zeta functions and their functional equations, Amer. J. Math., 111 (1989), 671-716.

[30] J. Igusa, A stationary phase formula for p-adic integrals and its applications, Algebraic Geometry and its Applications, Springer-Verlag (1994), 175-194.

[31] J. Igusa, On local zeta functions, Amer. Math. Soc. Transl. (2) 172, (1996), 1-20.

[32] N. Jacobson, Structure and representations of Jordan algebras, Amer. Math. Soc. Publ., 39 (1968).

[33] M. Kashiwara, B-functions and holonomic systems (Rationality of b-functions), Invent. math., 38 (1976), 33-53.

[34] T. Kimura, The b-functions and holonomy diagrams of irreducible regular prehomogeneous vector spaces, Nogoya Math. J., 85 (1982), 1-80.

[35] T. Kimura, F. Sato, and X.-W. Zhu, On the poles of p-adic complex powers and b-functions of prehomogeneous vector spaces, Amer. J. Math., 112 (1990), 423-437.

[36] W. Krull, Dimensionstheorie in Stellenringen, Crelles J. Math., 179 (1938), 204-226.

[37] F. Loeser, Fonctions d'Igusa p-adiques et polynômes de Bernstein, Amer. J. Math., 110 (1988), 1-22.

[38] F. Loeser, Fonctions d'Igusa p-adiques, polynômes de Bernstein, et polyèdres de Newton, Crelles J. Math., 412 (1990), 75-96.

[39] J. G. M. Mars, Les nombres de Tamagawa de certains groupes exceptionnels, Bull. Soc. math. France 94 (1966), 97-140.

[40] H. Mellin, Abriss einer einheitlichen Theorie der Gamma- und der hypergeometrischen Funktionen, Math. Ann., 68 (1910), 305-337.

[41] D. Meuser, On the poles of a local zeta function for curves, Invent. math., 73 (1983), 445-465.

[42] D. Meuser, On the degree of a local zeta function, Comp. Math., 62 (1987), 17-29.

[43] G. D. Mostow, Self-adjoint groups, Ann. Math., 62 (1955), 44-55.

[44] M. Nagata, Local rings, Interscience Tracts in Pure and Appl. Math., 13 (1962).

[45] L. S. Pontrjagin, Topologische Gruppen. I, B. G. Teubner (1957).

[46] M. M. Robinson, The Igusa local zeta function associated with the singular cases of the determinant and the Pfaffian, J. Number Theory, 57 (1996), 385-408.

[47] P. Samuel, La notion de multiplicité en algèbre et en géométrie algébrique, Thèses, Gauthier-Villars (1951).

[48] M. Sato, Theory of prehomogeneous vector spaces (notes by T. Shintani), Sugaku-no-ayumi 15-1 (1970), 85-156 (in Japanese).

[49] M. Sato and T. Kimura, A classification of irreducible prehomogeneous vector spaces and their relative invariants, Nagoya Math. J., 65 (1977), 1-155.

[50] M. Sato, M. Kashiwara, T. Kimura, and T. Oshima, Micro-local analysis of prehomogeneous vector spaces, Invent. math., 62 (1980), 117-179.

[51] L. Schwartz, Théorie des distributions. I, II, Hermann & Cie (1950,1951).

[52] J.-P. Serre, Classification des variétés analytiques p-adiques compactes, Topology 3 (1965), 409-412.

[53] H. Späth, Der Weierstrasssche Vorbereitungssatz, Crelles J. Math. 161 (1929), 95-100.

[54] L. Strauss, Poles of a two variable p-adic complex power, Trans. Amer. Math. Soc., 278 (1983), 481-493.

[55] J. Tate, Fourier analysis in number fields and Hecke's zeta-functions, Thesis, Princeton (1950).

[56] A. Weil, L'Intégration dans les groupes topologiques et ses applications, Hermann & Cie (1940).

[57] A. Weil, Numbers of solutions of equations in finite fields, Bull. Amer. Math. Soc., VI, 55 (1949), 497-508.

[58] A, Weil, Sur la formule de Siegel dans la théorie des groupes classiques, Acta Math., 113 (1965), 1-87.

[59] H. Weyl, Gruppentheorie und Quantenmechanik, S. Hirzel (1928).

[60] H. Weyl, The classical groups, Princeton Math. Series 1 (1946).

[61] E. Witt, Theorie der quadratischen Formen in beliebigen Körpern, Crelles J. Math., 176 (1937), 31-44.

[62] O. Zariski, Foundations of a general theory of birational correspondences, Trans. Amer. Math. Soc., 53 (1943), 490-542.

[63] O. Zariski, The concept of a simple point of an abstract algebraic variety, Trans. Amer. Math. Soc., 62 (1947), 1-52.

Index

This book is an introductory presentation to the theory of local zeta functions. Viewed as distributions, and mostly in the archimedean case, local zeta functions are also called complex powers. The volume contains major results on analytic and algebraic properties of complex powers by Atiyah, Bernstein, I. M. Gelfand, S. I. Gelfand, and Sato. Chapters devoted to p-adic local zeta functions present Serre's structure theorem, a rationality theorem, and many examples found by the author. The presentation concludes with theorems by Denef and Meuser.

American Mathematical Society
www.ams.org

International Press
www.intlpress.com

ISBN 978-0-8218-2907-3

AMSIP/14.S