Lectures on Some Aspects of *p*-Adic Analysis

By

F. Bruhat

Notes by

Sunder Lal

Tata Institute of Fundamental Research
Bombay
1963

Introduction

These lectures are divided in three parts, almost independent part *I* is devoted to the more less classical theory of valuated fields (Hensel's lemma, extension of a valuation, locally compact fields, etc.,)

In the second part, we give some recent results about representations of classical groups over a locally compact valuated field. We first recall some facts about induced representations of locally compact groups and representations of semi-simple real Lie groups (in connexion with the theory of "spherical functions"). Afterwards, we construct a class of maximal compact subgroups K for any type of classical group G over a p-acid field and the study of the left coset and double coset modulo K decomposition of G allows us to prove the first results about spherical functions on G. Some open problems are indicated.

Part *III* is devoted to Dwork's proof of the rationality of the zeta function of an algebraic variety over a finite field. We first need some results (well known, but nowhere published) about analytic and meromorphic functions on an algebraically closed complete valuated field. Then we settle the elementary facts about the zeta function of a scheme (in the sense of Grothendieck) of finite type over Z and we give, following Dwork, the proof of the rationality of these zeta functions

Contents

Part I

Classical Theory of Valuated Fields

Chapter 1

Theory of Valuations-I

In this and the next chapter we give a short account of the classical theory of valuated fields. Unless otherwise stated by a ring we mean a commutative ring with the unit element 1 and without zero divisors. 1

1

Definition. Let A be a ring and Γ a totally ordered comutative group [1]. A valuation v of the ring A is a mapping from A^* (the set of non-zero elements of A) into Γ such that

(I) $v(xy) = v(x) + v(y)$ for every x, y in A^*.

(II) $v(x + y) \geq \inf(v(x), v(y))$ for every x, y in $A*$.

We extend v to A by setting $v(0) = \infty$; where ∞ is an abstract element added to the group Γ satisfying the equation

$$\infty + \infty = \alpha + \infty = \infty + \alpha = \infty \text{ for } \alpha \text{ in } \Gamma.$$

We assume that $\alpha < \infty$ for every α in Γ. The valuation v is said to be improper if $v(x) = 0$ for all x in A^*, otherwise v is said to be proper.

The following are immediate consequences of our definition.

(a) $v(1) = 0$. For, $v(x.1) = v(x) = v(x) + v(1)$, therefore $v(1) = 0$

(b) If for x in A, x^{-1} is also in A, we have $v(x^{-1}) = -v(x)$, because $v(1) = v(xx^{-1}) = v(x) + v(x^{-1}) = 0$ 2

(c) If x is a root of unity, then $v(x) = 0$. In particular $v(-1) = 0$, which implies that $v(-x) = v(x)$

(d) Por n in Z (the ring of integers)

$$v(n) = v(1 + - - - + 1) \geq \inf(v(1)) = 0.$$

(e) If for x, y in A $v(x) \neq v(y)$, then $v(x+y) = \inf(v(x), v(y))$. Let us assume that $v(x) > v(y)$ and $v(x+y) > v(y)$. Then $v(y) = v(x+y-x) \geq\geq \inf(v(x+y), v(-x)) > v(y)$, which is impossible.

If x_i belongs to A for $i = n, 1, 2, \ldots, n$, then one can prove by induction on n that $v(\sum_{i=1}^{n} x_i) \geq \inf_{1\leq i\leq n}(v(x_i))$ and that the equality holds if there exists only one j such that $v(x_j) = \inf_{1\leq i\leq n}(v(x_i))$. In particular if $\sum_{i=1}^{n} x_i = 0\,(n \geq 2)$ then $v(x_i) = v(x_j) = \inf_{1\leq k\leq n}(v(x_k))$ for at least one pair of unequal indices i and j. For, let x_i be such that $v(x_i) \leq v(x_l)$ for $i \neq l$. Then $v(x_i) \geq \inf_{1\leq k\leq n\ k\neq i}(v(x_k)) = v(x_j)$, which proves that $v(x_i) = v(x_j)$.

Obviously we have

Proposition 1. *Let A be a ring with a valuation v. Then there exists one and only one valuation w of the quotient field K of A which extends v.*

It is seen immediately that $w\left(\frac{x}{y}\right) = v(x) - v(y)$ *for x, y in A.*

3 So without loss of generality we can confine ourselves to a field. The image of K^* (the set of non-zero elements of field K) by v is a subgroup of Γ which we shall denote by Γ_v

Proposition 2. *Let K be a field with a valuation v. Then*

(a) *The set $\mathscr{O} = \{x | x \in K, v(x) \geq 0\}$ is a subring of K, which we shall call the ring of integers of K with respect to the valuation v.*

(b) *The set $\mathscr{Y} = \{x | x \in K, v(x) > 0\}$ is an ideal in $\mathscr{O}$ called the ideal of valuation v.*

(c) *$\mathscr{O}* = \mathscr{O} - \mathscr{Y} = \{x | x \in K, v(x) = 0\}$ is the set of inversible elements of $\mathscr{O}$*

(d) *$\mathscr{O}$ is a local ring (not necessarily Noetherian) and $\mathscr{Y}$ is the unique maximal ideal of $\mathscr{O}$.*

We omit the proof of this simple proposition. The field $k = \mathscr{O}/\mathscr{Y}$ is called the residual field of the valuation v.

It is obvious form the proposition 2 that the valuation v of K which is a homomorphism form K^* to Γ can be split up as follows

$$K^* \xrightarrow{v_1} K^*/\mathscr{O}^* \xrightarrow{v_2} \Gamma_v \xrightarrow{v_3} \Gamma.$$

where v_1 is the canonical homomorphism, v_2 the map carrying an element $x\mathscr{O}^*$ to $v(x)$ and (v_3) the inclusion map of Γ_v into Γ.

Definition. Two valuations v and v' of a field K are said to be equivalent if there exists an order preserving isomorphism σ of Γ_v onto Γ'_V such that

$$v' = \sigma \circ v.$$

From the splitting of the homomorphism v it is obvious that a valuation of a field K is completely characterised upto an equivalence by any one of $\mathscr{O}$, or $\mathscr{Y}$. **4**

A valuation of a field K is said to be *real* if Γ_v is contained in R (the field fo real numbers). Since any subgroup of R is either discrete i.e., isomorphic to a subgroup of integers or dense in R, either Γ_v is contained in Z or Γ_v is dense in R. In the former case we say that v is a discrete valuation and in the latter non-discrete. Moreover v is completely determined upto a real constant factor, because if v and v' are two non-discrete equivalent valuations of K, the isomorphism of Γ_v onto Γ'_v can be extended to R by continuity, which is nothing but multiplication by a element of R. If v and v' are discrete and equivalent, the assertion is trivial. If $\Gamma_v = z$ we call v a normed discrete valuation.

Definition. Let K be a field with a normed discrete valuation v. In K we can find an element π with $v(\pi) = 1$. The element π is called a uniformising parameter for the valuation v.

Let K be a field with a normed discrete valuation v and $\mathscr{O} \neq (0)$ an ideal in $\mathscr{O}$. Let $\alpha = \inf\limits_{x \in \mathscr{O}}(v(x))$. Such an α exists because $v(x) > 0$ for every x in $\mathscr{O}$. Moreover there exists an element x_0 in $\mathscr{O}$ such that
5 $v(x_\circ) = \alpha$, because the valuation is discrete. Then $\mathscr{O} = \mathscr{O}x_0 = \mathscr{O}\pi^\alpha$ For, x belongs to $\mathscr{O} \iff v(x) \geq v(x_0) \iff v(\dfrac{x}{x_0}) \geq 0 \iff x/x_0$ belongs to $\mathscr{O} \iff x$ belongs to $\mathscr{O}x_0$. Since $v(\dfrac{x_o}{\pi^\alpha}) = v(x_0) - \alpha v(\pi) = 0$, we get that x_0 is in $\mathscr{O}\pi^\alpha$, conversely π^α belongs to $\mathscr{O}x_0$ is obvious. Therefore $\mathscr{O} = \mathscr{O}\pi^\alpha$. In particular $\mathscr{Y} = \mathscr{O}\pi$. In general let v be any valuation of a field K. Let $\mathscr{O}$ be any ideal of $\mathscr{O}$ and $H_{\mathscr{O}} = \{\alpha | \alpha \in \Gamma_\vartheta$, such that there exists x in $\mathscr{O}$ with $v(x) = \alpha\}$. Then the map $\mathscr{O} \to H_{\mathscr{O}}$ is a $1-1$ correspondence between the set of ideals $\mathscr{O}$ in $\mathscr{O}$ and the subsets $H_{\mathscr{O}}$ of Γ_v having the property that if α belongs to $H_{\mathscr{O}}$ and β belonging to Γ_v is such that $\beta \geq \alpha$, then β belongs to $H_{\mathscr{O}}$. In particular if Γ_v is contained in R, then the ideals of $\mathscr{O}$ are of one of the two kinds

(i) $I'_\alpha = \{x | x \in \mathscr{O}, v(x) \geq \alpha\}$

(ii) $I_\alpha = \{x | x \in \mathscr{O}, v(x) > \alpha\}$

for any $\alpha > 0$.

Examples. (1) Let Q be the field of rational numbers. For any m in Q we have $m = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ uniquely, where $\alpha_1, \ldots, \alpha_r$ are in Z and $p_1, \ldots, p_r$ are distinct primes. If v is any valuation of Q, we have $v(m) = \sum\limits_{j=1}^{r} \alpha_j v(p_j)$. Therefore it is sufficient to define a valuation for primes in Z. We note that for a valuation v there exists atmost one p for which $v(p) > 0$. If possible let us suppose that there exist two primes p_1 and p_2 such that $v(p_i) > 0$ for $i = 1, 2$.

6 Since $(p_1, p_2) = 1$, there exist two integers a and b such that $ap_1 + bp_2 = 1$. This implies that $0 = v(1) \geq \inf(v(ap_1)), v(bp_2)) > 0$, which is impossible. Thus our assertion is proved, If there does not exist any prime p for which $v(p) > 0$, then v is improper.

For a prime p we define $v_p(p) = 1$ and $v_p(m) = \alpha$, where α is the highest power of p dividing m. It is easy to verify that this is a valuation of Q and any valuation of Q for which $v(p) > 0$ is equivalent to this valuation. It is a discrete normed valuation of Q. One can take p as a uniformising parameter and prove that the residual field is isomorphic to $Z/(p)$

(2) Let K be any field, $K((x))$ the field of formal power series over K. For any element $f(x) = \sum\limits_{r=m}^{\infty} a_r x^r$ of $K((x))$ we define $v(f(x)) = t$, if a_t is the first non-zero coefficient in $f(x)$. One an easily verify that v is a normed discrete valuation of $K((x))$. The ring of integers of the valuation is the ring of formal power series with non-negative exponents and the ideal is the set of those elements in the ring of integers for which the constant term is zero. One can take x as a uniformising parameter.

2 Valuation Rings and Places

This section is added for the sake of completeness. The results mentioned here will not be used in the sequel.

Remark. Let K be a field with a valuation v and ring of integers $\mathscr{O}$. **7**
Then for any x in K, either x belongs to $\mathscr{O}$ or x^{-1} belongs to $\mathscr{O}$.

Motivated by this we define

A subring A of a field K is called a *valuation ring* of K if for any x in K either x belongs to A or x^{-1} belongs to A. In general a ring A is said to be a valuation ring if it is a valuation ring for its quotient field.

Proposition 3. *A ring A is a valuation ring if and only if the set of principle of A is totally ordered by inclusion.*

Proof. Let A be a valuation ring. Let Ax and Ay be two proper principle ideals of A. Consider $z = \dfrac{x}{y}$ belonging to K the quotient field of A. Since A is a valuation ring, either z or z^{-1} belongs A. But this implies that either $Ax \subset Ay$ or $Ay \supset Ax$. Therefore the set of principal ideals is totally ordered conversely let $x = \dfrac{y}{z}$, where y and z belong to A and $x \neq 0$, be an element of K which is not in A. $x \notin A$ implies that y does not belong to Az. But the set of principle ideals of A is totally ordered, therefore we get $Az \subset Ay$ implying $z = ay$ for some a in A. But $a = x^{-1}$, therefore A is a valuation ring. □

Corollary. *A valuation ring is a local ring.*

If possible let $\mathcal{M}_1 \neq \mathcal{M}_2$ be two maximal ideals in a valuation ring A. $\mathcal{M}_1 \neq \mathcal{M}_2$ implies that there exists $x_1 \in \mathcal{M}_1$, $x_1 \notin \mathcal{M}_2$ and $x_2 \in \mathcal{M}_2$, $x_2 \notin \mathcal{M}_1$.

8 *$x_1 \notin \mathcal{M}_2 \implies Ax_1$ is not contained in $\mathcal{M}_2$ which implies that Ax_1 is not contained in Ax_1. Similarly x_2 not belonging to $\mathcal{M}_1$ implies that Ax_1. But this is impossible, therefore $\mathcal{M}_1 = \mathcal{M}_2$.*

Proposition 4. *A ring A is a valuation ring if and only if A is the ring of a valuation of its quotient field K determined upto an equivalence.*

Proof. Let $\mathcal{M}$ be the unique maximal ideal of the valuation ring A and $A^* = A/\mathcal{M}$. For x, y in K^* we define $x \geq y$ if and only if x belongs to Ay. It is easy to verify that this relation among the elements of K^* induces a total order in the group K^*/A^* and the canonical homomorphism K^* onto K^*/A^* is a valuation of K for which the ring of integers is A. The ring of integers of a valuation is a valuation ring has already been proved. □

Let k be a fields. By $k \cup \infty$ we mean the set of elements of k together with an element ∞. We extend the laws of k to (not everywhere defined) laws in $k \cup \infty$ in this way

(i) $\infty + a = a + \infty = \infty$ for a in k^*

(ii) $\infty \times a = a \times \infty = \infty \times \infty = \infty$, for a in k^*

$0 \times \infty$ and $\infty + \infty$ are not defined.

Let K be a field with a valuation v and let $k = \mathscr{O}/\mathscr{Y}$ be the residual fields of v. Then the canonical homomorphism ρ of $\mathscr{O}$ onto k extended to K by setting $\rho(x) = \infty$ for x not in $\mathscr{O}$ gives rise to a map of K onto $k \cup \infty$ called a place of K.

9 In general, we define

A place of a field K is a mapping ρ form K to $k \cup \infty$ such that

(i) $\rho(a + b) = \rho(a) + \rho(b)$

(ii) $\rho(ab) = \rho(a)\rho(b)$

for a, b in K and whenever the right hand side is meaningful.

It is easy to prove that $\mathscr{O} = \rho^{-1}(K)$ is a valuation ring with the maximal ideal $\mathscr{Y} = \rho^{-1}(0)$.

Thus there exists a $1-1$ correspondence between the set of valuation rings and the set of inequivalent places of a field (Two places ρ_1 and ρ_2 of a field K carrying K into $k \cup \infty$ and $k' \cup \infty$) respectively are said to be equivalent if there exists an isomorphism σ of k onto k' such that $\rho_2 = \sigma \circ \rho_1$, with $\sigma(\infty) = \infty$.

3 Topology Associated with a Valuation

Let K be a field with a valuation v. For any $\alpha \geq 0$ in Γ_v consider the ideal

$$I_\alpha = \{x | x \in K, v(x) > \alpha\}$$

Then there exists one and only topology on K for which

(1) I_α for different α in Γ_v form a fundamental system fo neighbourhoods of 0.

(2) K is a topological group for addition.

We see immediately that the operation of multiplication in K is continuous in topology. I_α for any $\alpha \geq 0$ in Γ_v is an open subgroup and hence a closed subgroup of K. Thus the residual field k is discrete for **10**
the quotient topology. The topology of K is discrete if and only if the valuation v is improper (if $\Gamma_v = \{o\}$). In particular K with a discrete and proper valuation is not discrete as a topological space. The topology of K is always Hausdorff, because if $x \neq 0$, then x does note belong to I_α with $\alpha = v(x)$, therefore $\bigcup\limits_{\alpha \in \Gamma_v} I_{\alpha\alpha} > 0 = (0)$ which proves our assertion.

Remark 1. If v is not improper, then the ideals I'_α for $\alpha \geq o$ in Γ_v also constitute a fundamental system of neighbourhoods of 0 for the topology of K. For, I'_α and for $\alpha > o$ I_α contains $I'_{2\alpha}$.

Remark 2. Let A be a ring a with a decreasing filtration by ideals i.e. there exists a sequence $(A_n)_{n \geq 0}$ of ideals such that $A_n \supset A_{n+1}$ and

$A_nA_m \subset A_{m+n}$. Then there exists one and only one topology for which A is an additive topological group and $(A_n)_{n\geq o}$ constitute a fundamental system of neighbourhoods of 0. A is a topological ring this topology.

Let $\mathcal{M}$ be any ideals of a ring A. Then A can be made into a topological ring by taking $A_n = \mathcal{M}^n$. We call the topology defined by $\mathcal{M}$ on A the $\mathcal{M}-$ adic topology. In particular the ring of integers of a field K which a real valuation v has the $\mathcal{M}-$ adic topology for every $\mathcal{M} = \{x/v(x) \geq \alpha > 0\}$ We shall speak of this topology of K as the $\mathcal{M}-$adic topology.

11 If the valuation v is discrete and normed. We can take $\alpha = 1$ and $\mathcal{M} = \mathscr{Y}$.

Remark 3. If K is a field with a real valuation v, then the $\mathscr{Y}-$adic topology completely characterises the valuation upto a constant factor, because x belongs to $\mathscr{Y}$ if and only if x^n tends to zero as n tends to infinity.

4 Approximation Theorem

For the sake of simplicity we confine ourselves in this section to real valuations though analogous results could be prove for any valuation. In this section we deal with the question whether there exists any connection between various inequivalent valuations of a field. We first prove:-

Lemma 1. Let K be a field with two valuations v_1 and v_2. Then v_1 and v_2 are inequivalent if an only if $\mathscr{O}_1$, the ring of integers of v_1, is not contained in $\mathscr{O}_2$, the ring of integers of v_2.

Proof. If $\mathscr{O}_1 \subset \mathscr{O}_2$, then $K - \mathscr{O}_1$ contains $K - \mathscr{O}_2$ implying $\mathscr{Y}_2 \subset \mathscr{Y}_1 \subset \mathscr{O}_1 \subset \mathscr{O}_2$. Therefore $\mathscr{Y}_2$ is a prime ideal in $\mathscr{O}_1$. Assume $\mathscr{Y}_2 \neq \mathscr{Y}_1$, then there exists x in $\mathscr{Y}_1$ which does not belong to $\mathscr{Y}_2$. Since $\mathscr{Y}_2$ is an ideal in $\mathscr{O}_1$, there exists $\alpha > 0$ in Γ_{v_1} such that $\mathscr{Y}_2$ contains I_α. Let $v_1(x) = \beta$. □

Then for large enough q we have

$$v_1(x^q) = qv_1(x) = q\beta > \alpha,$$

which means that x^q belongs to $\mathscr{Y}_2$, but $\mathscr{Y}_2$is a prime ideal, therefore x belongs to $\mathscr{Y}_2$. Hence our assumption is wrong.

Therefore $\mathscr{Y}_2 = \mathscr{Y}_1$ and v_1 is equivalent to v_2. The converse is obvious. 12

Lemma 2. Let K be a field with $v_1, \ldots, v_n (n \geq 2)$ proper valuations such that v_i is inequivalent to v_j for $i \neq j$. Then there exists an element z in K such that $v_1(z) > 0, v_2(z) < 0$ and $v_i(z) \neq 0$ for $i = 1, 2, \ldots, n$.

Proof. We shall prove the results by induction on n. When $n = 2, v_1$ inequivalent to $v_2$implies that $\mathscr{O}_1$ is not contained in $\mathscr{O}_2$ (lemma 1). Therefore there exists x in $\mathscr{O}_1$ and not in $\mathscr{O}_2$. Moreover $\mathscr{O}_2$ not contained in $\mathscr{O}_1$ implies that $\mathscr{Y}_1$ is not contained in $\mathscr{Y}_2$. □

Therefore there exists y in $\mathscr{Y}_1$ and not in $\mathscr{Y}_2$. Then $z = xy$ is the required element.

When $n > 2$. By induction there exists an element x in K such that $v_1(x) > 0, v_2(x) < 0$ and $v_i(x) \neq 0$ for $i = 1, 2, \ldots, n-1$. If $v_n(x) \neq 0$, we have nothing to prove. If $v_n(x) = 0$, we take an element y with $v_n(y) \neq 0$. Let $z = yx^s$, s a positive integer. Then for sufficiently large s, z fulfills the requirements of the lemma.

Theorem 1. *Let K be a field with $v_1, \ldots, v_r$ proper valuations such that v_i is inequivalent to v_j for $i \neq j$. Let K_i be the field K with the topology defined by v_i and ρ the canonical map from $K \to \prod\limits_{i=1}^{r} K_i = P$ i.e. $\rho(a) = (a, a, \ldots, a)$. Then $\rho(K) = D$ is dense in P.*

Equivalently stated if $a_1, \ldots, a_r$ are any r elements in K, then for every $\alpha_1, \ldots, \alpha_r$ in R there exists an element x in K such that 13

$$v(x - a_i) > \alpha_i \text{ for } i = 1, 2, \ldots, r.$$

Proof. The theorem is trivial for $r = 1$. Let us assume that it is true in case the number of valuations is less then r. □

By lemma 2 there exists an elements x in K such that $v_1(x) > 0, v_r(x) < 0$ and $v_i(x) \neq 0$ for $1 \leq i \leq r$, then $y_n = \dfrac{x^n}{1 + x^n}$ tends to

0 in K_1, to 1 in K_r and to 0 or 1 in others as n tends to infinity. Let the notation be so chosen that $\rho(y_n) \to (0, 0, \ldots, 0, 1, \ldots, 1)$ as n tends to infinity, 0 occurring in s places where $1 \leq s \leq r - 1$. Now D is a subspace of P over K, therefore

$$\operatorname*{lt}_{n\to\infty} x\rho(y_n) = \operatorname*{lt}_{n\to\infty} \rho(xy_n) = (0, \ldots 0,\ x, \ldots, x)$$

and $(0, 0, \ldots, 0, x, x, \ldots, x)$ is in $\bar{D}$. Consider the product $\prod_{i=s+1}^{r} K_i$, by induction assumption the diagonal of $\prod_{i=s+1}^{r} K_i$ which is imbedded in $\bar{D}$ is dense in the product which implies that $(0, \ldots, 0, a_{s+1}, \ldots, a_r)$ belongs to $\bar{D}$ for a_i in K, $s + 1 \leq i \leq r$. Similarly $(a_1, a_2, \ldots, a_s, 0, \ldots, 0)$ belongs to $\bar{D}$. But $\bar{D}$ is a vector space over K, therefore $(a_1, a_2, \ldots, a_r)$ is in $\bar{D}$. Hence $\prod_{i=1}^{r} K_i = \bar{D}$.

Corollary. *Under the assumptions of the theorem for $\alpha_j \in \Gamma_{v_j}(j = 1, 2, \ldots, r)$ there exists x in K such that $v_j(x) = \alpha_j$.*

14 For α_j in Γ_{v_j}, there exists $a_j \in K$ such that $v(a_j) = \alpha_j$. By approximation theorem there exists an element x in K such that $v(x - a_j) > \alpha_j$. By definition we have $v(x) = v(x - a_j + a_j) = \inf v((x - a_j), v(a_j)) = v(a_j) = \alpha_j$.

5 Completion of a field with a valuation

Let K be a field with a valuation v. Since K is a commutative topological group for the topology defined by v, it is a uniform space. Let $\hat{K}$ denote the completion K. The composition laws of addition and multiplication can be extended by continuity to $\hat{K}$, for which $\hat{K}$ is a topological ring. In fact $\hat{K}$ is a topological field, because if Φ is a Cauchy filter on K converging to $a \neq 0$, then Φ^{-1}(the image of Φ by the map $x \to x^{-1}$ in K) is a Cauchy filter. For Φ not converging to 0 implies that there exists $\alpha \geq 0$ in Γ_v and a set A in Φ such that $v(x) < \alpha$ for every x in A. Since Φ is a Cauchy filter, for every β in Γ_v, there exists a set B in Φ contained in A such that

$$v(x - y) > 2\alpha + \beta \text{ for } x, y \text{ in } B.$$

Then

$$v(x^{-1}-y^{-1}) = v(x^{-1}y^{-1}(y-x)) = -v(x)-v(y)+v(y-x) > -\alpha-\alpha+2\alpha+\beta$$

which implies that Φ^{-1} is a Cauchy filter converging to a^{-1} in $\hat{K}$. The valuation v can also be extended to be valuation $\hat{v}$ of $\hat{K}$, in fact it is a continuous representation of K^* onto Γ_v considered as a discrete topological group, so v can be extended as a continuous representation $\hat{v}$ of $\hat{K}^*$ in Γ and we get $\hat{v}(x+y) \geq \inf(\hat{v}(x), \hat{v}(y))$ by continuity. Moreover 15
$\mathscr{O}_{\hat{K}}$ (the ring of integers of $\hat{K}$) $= \hat{\mathscr{O}}_K = \bar{\mathscr{O}}_K$, since $\mathscr{O}_{\hat{K}}$ is open in $\hat{K}$ and $\bar{K}$ is hence in $\hat{K}$, $\mathscr{O}_{\hat{K}} \cap K = \mathscr{O}_K$ is dense in $\mathscr{O}_{\hat{K}}$, this implies that $\mathscr{O}_{\hat{K}} \supset \bar{\mathscr{O}}_K$. But $\bar{\mathscr{O}}_K \supset \mathscr{O}_{\hat{K}}$, therefore our result is proved. More generally

$$\hat{I}_\alpha = \left\{x|\hat{v}(x) > \alpha, x \in \hat{K}\right\} = \bar{I}_\alpha = \overline{\left\{x|v(x) > \alpha, x \in K\right\}}$$

In particular $\mathscr{Y}_{\hat{K}} = \bar{\mathscr{Y}}_K$. We have $\mathscr{Y}_K = \mathscr{O}_K \cap \mathscr{Y}_{\hat{K}}$, so we may identify $\mathscr{O}_K/\mathscr{Y}_K$ with a subset of $\mathscr{O}_{\hat{K}}/\mathscr{Y}_{\hat{K}}$, and $\mathscr{O}_K/\mathscr{Y}_K$ is dense in $\mathscr{O}_{\hat{K}}/\mathscr{Y}_{\hat{K}}$. But $\mathscr{O}_{\hat{K}}/\mathscr{Y}_{\hat{K}}$ is discrete, therefore $\mathscr{O}_{\hat{K}}/\mathscr{Y}_{\hat{K}} = \mathscr{O}_K/\mathscr{Y}_K$.

Remark. Let K be a field with a real valuation v, with v we associate a map from K to R. We defined for any x in K the absolute value $|x| = a^{-v(x)}$, where a is a real number > 1. The map $||$ satisfies the following properties

(1) $|x| = 0$ if and only if $x = 0$

(2) $|xy| = |x|\ |y|$

(3) $|x+y| \leq \sup\ (|x|, |y|) \leq |x| + |y|$.

The absolute value of elements of K, which defines the same topology on K as the valuation v.

By Q_p we shall always denote the completions of the field Q for p-adic valuation and by Z_p the ring of integers in Q_p. For the absolute 16
value associated to the p-adic valuation. We take $a = p$ so that $|x|_p = p^{-v}p^{(x)}$

6 Infinite Series in a Complete Field

Let K be a complete field for a real valuation v. Since every Cauchy sequence in K has a limit in K, the definition of convergence of infinite series and Cauchy criterium can be given in the same way as in the case of real numbers. However in this case we have the following.

Theorem 2. *A family $(u_i)_{i\in I}$ of an infinite number of elements of K is summable if and only if u_i tends to* 0 *following the filter of the complements of finite subsets of I.*

Proof. The condition is clearly necessary. Conversely for any α in Γ_v we can find a finite subset J of I such that for i not in $J, v(u_i) > \alpha$, then for $i_1, \ldots, i_r$ not in J we have $v\left(\sum\limits_{j=1}^{r} \cup_{i_j}\right) > \alpha$ which is nothing but Cauchy Criterium. Hence the family is summable. □

Corollary. *Let $\sum\limits_{n=0}^{\infty} u_n$ be infinite series of elements of K Then the following conditions are equivalent.*

(a) $\sum\limits_{n=0}^{\infty} u_n$ *is convergent.*

(b) $\sum\limits_{n=0}^{\infty} u_n$ *is commutatively convergent.*

(c) u_n *tends to* 0 *as n tends to infinity.*

17 **Application.** Let K be a complete field for a normed discrete real valuation v, π a uniformising parameter for $K, \mathscr{R}$ a fixed system of representatives in $\mathscr{O}$ for the elements of the residual field K. Then the series $\sum\limits_{q=m}^{\infty} r_q \pi^q$, where r_q belongs to $\mathscr{R}$ is convergent to an element x in K and conversely every x in K can be represented in this form in one and only one way. The series is convergent because $v(r_q \pi^q) \geq q$ for $q \neq 0$ and therefore tends to infinity as q tends to infinity. Conversely by multiplying with a suitable power of π we can take x in $\mathscr{O}$, then there exists a unique $r_0 \in \mathscr{R}$ such that $x \equiv r_0 \pmod{\mathscr{Y}}$.

This implies that $(x - r_0)\pi^{-1}$ is in $\mathscr{O}$. Therefore there exists unique r_1 in $\mathscr{R}$ such that

$$(x - x_0)\pi^{-1} \equiv r_1 \pmod{\mathscr{Y}}.$$

or

$$x \equiv r_0 + r_1\pi \pmod{\mathscr{Y}^2}.$$

Proceeding in this way we prove by induction that

$$x \equiv r_o + r_1\pi \cdots + r_m\pi^m \pmod{\mathscr{Y}^{m+1}}$$

Now it is obvious that the series $\sum\limits_{r=0}^{\infty} r_m\pi^m$, is convergent and that $x = \sum\limits_{q=0}^{\infty} r_q\pi^q$. The uniqueness of the series is obvious from the construction.

In particular if, $K = Q_P$ then any x in Q_p can be represented in the form $\sum\limits_{q=m}^{\infty} r_q p^q$, where $r_q \in \{0, 1, 2 \ldots, p - 1\}$.

7 Locally Compact Fields

In this section we give certain equivalent conditions for valuated fields to be locally compact. Later on we shall completely characterise the locally compact valuated fields. **18**

Theorem 3. *Let K be a field with a proper valuation v. Then the following conditions are equivalent.*

(a) *K is locally compact.*

(b) *$\mathscr{O}$ is compact.*

(c) *K is complete, v is a discrete valuation and k is a finite field.*

Proof. $(a) \Longrightarrow (b)$. Since $(I'_\alpha)_{\alpha\in\Gamma_v}$ form a fundamental system of closed neighbourhoods for 0, there exists an α such that I'_α is compact. But m $I'_\alpha = \mathscr{O}_{x_o}$, if $v(x_0) = \alpha$, therefore $\mathscr{O} = x_0^{-1} I_\alpha$ is compact.

$(b) \Longrightarrow (a)$ is trivial, as $\mathscr{O}$ is a compact neighbourhood of 0.

$(a) \Longrightarrow (c) K$ is complete because it is a locally compact commutative group. For any $\alpha > 0$ in Γ_v $\mathscr{O}/I_\alpha$ is compact because $\mathscr{O}$ is compact.

But $\mathscr{O}/I_\alpha$ is a discrete space, therefore it contains only a finite number of elements. In particular $k = \mathscr{O}/\mathscr{Y}$ is finite field. For any β in $\Gamma_v, 0 < \beta < \alpha$, we have $I_\alpha \subset I_\beta \subset \mathscr{O}$, therefore I_β/I_α is a nontrivial ideal of $\mathscr{O}/I_\alpha$ and distinct elements give rise to distinct ideals. But $\mathscr{O}/I_\alpha$ is a
19 finite set, therefore there exist only a finite number of β with $0 < \beta < \alpha$, so we get that

(i) Γ_v has a smallest positive element

(ii) Γ_v is Archimedian.

Thus Γ_v is isomorphic to Z and the valuation v is discrete. $(c) \implies (b)$. We shall prove that discreteness of the valuation v and finiteness of k implies that $\mathscr{O}$ is precompact, which together with the fact that K is complete implies that $\mathscr{O}$ is compact. Let V be any neighbourhood of 0. Since v is discrete, for some $n > 0$ V contains $\mathscr{Y}^n$. We shall show by induction on n that $\mathscr{O}/\mathscr{Y}^n$ is finite for $n > 0$. The result is true for $n = 1$; let us assume it to be true for all $r < n$. We have $\mathscr{O}/\mathscr{Y}^{n-1} \simeq \mathscr{O}/\mathscr{Y}^n/\mathscr{Y}^{n-1}/\mathscr{Y}^n$ But $\mathscr{O}/\mathscr{Y}^{n-1}$ is finite by induction hypothesis and $\mathscr{Y}^{n-1}/\mathscr{Y}^n$ is finite because it is isomorphic to $\mathscr{O}/\mathscr{Y}$, therefore $\mathscr{O}/\mathscr{Y}^n$ is finite. Hence there exist a finite number of elements $x_1 - - - x_r$ in $\mathscr{O}$ such that $\mathscr{O} \subset \bigcup_{i=1}^{r}(x_i + \mathscr{Y}^n) \subset \bigcup_{i=1}^{r}(x_i + V)$ and since this is true for every neighbourhood of $0, \mathscr{O}$ is precompact. □

8 Convergent Power Series

Let K be complete field with a real valuation v. Then the power series $f(x) = \sum_{n=0}^{\infty} a_n x^n$ with coefficients from K is said to be convergent at a point x of K if the series $\sum_{n=0}^{\infty} a_n x^n$ is convergent. It has already been
20 proved that the series $\sum_{n=0}^{\infty} a_n x^n$ converges if and only if

$$v(a_n x^n) = v(a_n) + nv(x) \to \infty \; as \; n \to \infty \tag{1}$$

From (1) it is obvious that if take $t = \liminf_n \frac{1}{n}(v(a_n))$, then the series f converges for all x which $v(x) > -t$ and does not converge for those x for which $v(x) < -t$ and for those x for which $v(x) = -t$ either the series converges for all x or does not converge at all. The number $-t$ is called the order of convergence of the power series f and the set $\{x|v(x) > -t\}$ or $\{x|v(x) \geq -t$, if the series converges at a point x with $v(x) = -t\}$ is called the disc of convergence, which we shall denote by D_f. If we consider the absolute value associated to v then the radius of convergence is

$$\rho = a^{-t} = \left\{\lim_{n\to\infty} \sup(|a|_n)^{1/n}\right\}^{-1}$$

and $$D_f = \{x|\, |x| < \rho\} \quad \text{or} \quad \{x|\, |x| \leq \rho\}$$

The mapping $x \to f(x)$ from D_f to K is continuous because it is a uniform limit of polynomials namely the partial sums of the series $\sum_{n=0}^{\infty} a_n x^n$ in the disc $\{x|v(x) \geq -t_1$, for all $t_1 > t\}$ or in the disc $\{x|v(x) \geq -t\}$ if the series converges on the disc. The classical results about addition and multiplication, ... of power series can be carried over to the power series with coefficient in a complete valuated field. For instance if $f(x) = \sum_{n=0}^{\infty} a_n x^n$ and $g(x) = \sum_{n=0}^{\infty} b_n x^n$ are two power series with D_f and D_g as their discs of convergence respectively; then if for one x in D_f, 21
$a_i x^i$ belongs to D_g for every i, $f(x)$ also belongs to D_g and we have

$$g(f(x)) = \sum_{r=0}^{\infty} c_r x^r, \text{ where}$$

$$c_r = \sum_{q=0}^{\infty} b_q \sum_{i_1+i_2+\cdots+i_q=r} a_{i_1} a_{i_2} \ldots a_{i_q},$$

all the series being convergent.

Remark 1. If $k = \mathscr{O}/\mathscr{Y}$ is an infinite field, then

$$\inf_i (v(a_i x^i)) = \inf_{v(y)=v(x)} (v(f(y))).$$

For, $v(f(x)) \geq \inf_i(v(a_i x^i))$. We get equality, if there does not exist any two terms of the same valuation. In the exceptional case as the series as the series $\sum\limits_{n=0}^{\infty} a_n y^n$ is convergent, we have

$f(y) = \sum\limits_{r=i_\circ}^{j_\circ} a_r y^r +$ terms of higher valuation, where $i_\circ \leq r \leq j_\circ < \infty$.

and without loss of generality we can assume that $v(x) = 0$ and $\inf_i v(a_i x^i) = 0$. Now $v(f(y)) > 0$ if and only if $\sum\limits_{r=i_\circ}^{j_\circ} a_r y^r$ belongs to $\mathscr{Y}$ i.e., if and only if the polynomial $\sum\limits_{r=i_\circ}^{j_\circ} \overline{a}_r \overline{y}^r$ (the image in k) $= 0$. But k has infinite number of elements and the above polynomial not being identically zero has only a finite number of zeros, therefore there exists
22 atleast one y for which $v(f(y)) = 0$ and $v(x) = v(y)$. Thus in this case whenever x is in D_f and $f(y)$ belongs to D_g for all those y for which $v(x) = v(y)$, we have

$$\inf_i v(a_i x^i) = \inf_{v(y)=v(x)} v(f(y)).$$

Then $f(g(x)) = \sum\limits_{r=0}^{\infty} c_r x^r$ with

$$c_r = \sum_{r=0}^{\infty} b_q \sum_{v_1+--+v_q=r} a_{v_1} \cdots a_{v_q}.$$

Remark 2. Let A be a ring with a topology defined by a decreasing filtration $(A_n)_{n\geq 0}$ of ideals for which A is Hausdorff and complete space. Then the formal power series $\sum\limits_{n=0}^{\infty} a_n x^n$ converges at x in A if and only if $a_n x^n \to 0$ as n tends to infinity and obviously the series converges everywhere in A if and only if a_n tends to 0 as n tends to infinity.

Chapter 2

Theory of Valuations -II

1 Hensel's Lemma

In this section we give a proof of Hensel's lemma and deduce certain corollaries which will be used quite often in the following. In this section by a ring we mean a commutative ring with unity (It may have zero divisors). 23

Definition. Let A be a ring. Two elements x and y in A are said to be strongly relatively prime if and only if $Ax + Ay = A$ i.e. if and only if there exist two elements u and v in A such that $ux + vy = 1$.

In particular if $k[x]$ is the ring of polynomials over a filed k then any two elements in $k[x]$ are strongly relatively prime if and only if they are coprime in the ordinary sense.

It is obvious that if $x$and y are two strongly relatively prime elements in a ring A, then for any z in A x divides y z implies that x divides z.

Lemma 1. Let P and P' be two polynomials with coefficients in a ring A such that P is monic and P and P' are strongly relatively prime. Let us assume that degree $P = d(P) = s$ and $d(P') = s'$. Then for every polynomial Q in $A[x]$ there exists one and only one pair of polynomials U and V such that

$$Q = UP + VP' \text{ with } d(V) < s$$

and for every $t > s'$, $d(Q) < t + s$ if and only if $d(U) < t$. 24

Proof. The existence of one pair U and Vsuch that $Q = UP + VP'$ is trivial. If $d(V) > s$, we write $V = AP + B$ where $d(B) < s$, which is possible because P is a monic polynomial, so we get

$$q = (U + A).P + BP' \text{with} d(B) < s. \qquad \square$$

Thus we can assume in the beginning itself that $d(V) < s$. If possible let there exists another pair U' and V' such that

$$Q = U'P + V'P', d(V') < s.$$

Then

$U'P + V'P' = UP + VP'$ implies that $(U - U')P = (V' - V)P'$.

But P and P' are strongly relatively prime, therefore P divides $V' - V$. Since $d(V' - V) < s, V' - V = 0$. This implies that $P(U - U') = 0$. As P is monic we must have $U = U'$. Let $d(Q) < t + s$. Then $d(UP) = d(Q - VP')$. But $d(V) < s$ and $d(P') = s' < t$, therefore $d(UP) < t + s$, which implies that $d(U) < t$ because P is a monic polynomial of degree s. It is obvious that $d(V) < t\,(t > s')$ implies that $d(Q) < t + s$.

Definition. Let A be a ring, the intersection of all the maximal ideals is called the radical of A and shall be denoted by $r(A)$.

It can be easily proved that any element x of A belongs to $r(A)$ if and only if 1-xy is invertible for all $y \in A$.

25 **Lemma 2.** Let A be a ring $\mathscr{O}$ an ideal in A contained in $r(A)$. Then two polynomials P and P' in $A[x]$ ane of which (say P) is minic are strongly relatively prime if and only if $\overline{P}$ and $\overline{P}'$ (the images of P and P' in $A/\mathscr{O}[x]$) are strongly relatively prime.

Proof. P and P' are strongly relatively prime implies $\overline{P}$ and $\overline{P}'$ are strongly relatively prime is obvious. $\square$

Suppose that $d(P') = s'$ and $d(P) = s$. Then $d(\overline{P}) = d(P) = s$, because P is monic. Let $E = \{f | f \in A[x], d(f) < s + t, \text{ for some } t > s'\}$. Then E is a module of finite type over A. Let $\overline{E} = E/\mathscr{O}E$, since $\overline{P}$ and $\overline{P}'$ are strongly relatively prime in $A/\mathscr{O}[x]$, $\overline{E}'$ is generated by the polynomials $X^u\overline{P}$ and $X^v\overline{P}'$ for $0 \leq u \leq s$. For, by Lemma 1 for every polynomials $\overline{Q}$ in $\overline{E}$ there exists one only one pair of polynomials $\overline{U}$ and $\overline{V}$ in $A/\mathscr{O}[X]$ such that

$$\overline{Q} = \overline{U}\overline{P} + \overline{V}'\overline{P}' \quad d(\overline{V}) < t + s.$$

But $d(\overline{Q}) < t + s$, therefore $d(\overline{U}) < t$. Thus

$$\overline{U} = \sum_{\lambda=0}^{u} \overline{a}_\lambda X^\lambda, 0 \leq u \leq t$$

$$\overline{V} = \sum_{\mu=0}^{v} \overline{b}_\mu X^\mu, 0 \leq v \leq s$$

and $\overline{Q} = \sum\limits_{\lambda=0}^{u} \overline{a}_\lambda (X^\lambda \overline{P}) + \sum\limits_{\mu=0}^{v} \overline{b}_\mu (X^\mu \overline{P}')$.

By a simple corollary of Nakayama's lemma (For proof see Algebre by N. Bourbaki chapter 8 section 6) which states that if E is a module **26**
of finite type over a ring A and q and ideal in $r(A)$ then if $(a_1, \ldots, a_n)$ generate E module qE, they generate E also, we get X^uP and X^vP for $0 \leq u \leq t$ and $0 \leq v \leq s$ constitute a set of generators for E. Therefore

$$1 = \left(\sum_{r=0}^{u} a_r X^r\right) P + \left(\sum_{k=0}^{v} b^k X^k\right) P'$$

because 1 belongs to E. Hence P and P' are strongly relatively prime in $A[X]$.

Let A be a ring with a decreasing filtration of ideals $(\mathscr{O}_n)_{n>0}$, defining a topology on A for which A is a complete Hausdorff space. If $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n$ is a power series over A converging everywhere in A then $\lambda_n(f) = \sup\limits_{a_i \notin \mathscr{O}_n} (i)$

$(\lambda_n(f) < \infty$, because $a_n \to 0$ as $n \to \infty)$ is an increasing function of n i.e., $\lambda_n(f) \leq \lambda_{n+1}(f)$ and $f(x)$ is a polynomial if and only if $\lambda_n(f)$ is constant for n sufficiently large.

We shall denote by $\overline{f}$ the image of f in $A/\mathscr{O}_1[X]$.

Hensel's Lemma. Let A be a ring with a decreasing filtration of ideals $(\mathscr{O}_n)_{n>0}$. Let A for this topology be a complete Hausdorff space. If $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n$ is an everywhere convergent power series over A and if there exist two polynomial φ and ψ an $A/\mathscr{O}_1[X]$ such that

(1) φ is monic of degree s

(2) φ and ψ are strongly relatively prime

(3) $\overline{f} = \varphi\psi$

27 then there exists one and only pair (g, h) such that

(a) g is a monic polynomial of degree s in $A[X]$ and $\overline{g} = \varphi$.

(b) h is every where convergent power series over A and $\overline{h} = \psi$.

(c) $f = gh$

Moreover $\lambda_n(h) = \lambda_n(f) - s$. If f is a polynomial then h is a polynomial and g and h are strongly relatively prime.

Proof. Existence We construct two sequences of polynomials (g_n) and (h_n) an $A[X]$ by induction on n such that

$$\begin{aligned}
&(\alpha)\, g_n \text{ is monic of degree s}, \overline{g}_n = \varphi \text{ and}\\
&g_n + 1 \equiv g_n \pmod{\mathscr{O}_{n+1}} \text{ for } n \geq 0\\
&(\beta)\, \overline{h}_n = \psi, h_{n+1} \equiv h_n \pmod{\mathscr{O}_{n+1}} \text{ and}\\
&d(h_n) = \lambda_{n+1}(f) - s\\
&(\gamma)\, f \equiv g_n h_n \pmod{\mathscr{O}_{n+1}}, n \geq 0
\end{aligned}$$

For $n = 0$, we take $g_o = \sum\limits_{r=0}^{s-1} a_r X^r + X^s$ if

$$\varphi = \sum_{r=0}^{s-1} \overline{a}_r X^r + X^s \text{ and } h_o = \sum_{u=0}^{t} b_u X^u \text{ if}$$

$$\psi = \sum_{u=0}^{t} \overline{b}_u X^u, \text{ with } t = d(\psi) = d(\overline{f}) - s = \lambda_1(f) - s.$$

Let us assume that we have constructed the polynomials $g_1, g_2 \cdots g_{n-1}$ and $h_1, \ldots, h_{n-1}$ satisfying the conditions $(\alpha), (\beta)$, and (γ). By lemma (2) g_{n-1} and h_{n-1} are strongly relatively prime modulo $\mathcal{O}_q$ for every integer $q \geq 1$, because g_{n-1} and h_{n-1} are strongly relatively prime **28**
in $A/\mathcal{O}_1[X] = A/\mathcal{O}_{q}\Big/_{\mathcal{O}_1/\mathcal{O}_g}[X]$ and $\mathcal{O}_1/\mathcal{O}_q$ is contained in $r(A/\mathcal{O}_q)$, every element of $\mathcal{O}_1/\mathcal{O}_g$ being nil potent. Therefore by lemma (1) there exist polynomials X_n and Y_n in $A(X)$ such that

$$f - g_{n-1}h_{n-1} \equiv Y_n g_{n-1} + X_n h_{n-1} \pmod{\mathcal{O}_{n+1}}$$

and $d(X_n) < s$. □

But by induction assumption $f - g_{n-1}h_{n-1} \equiv 0 \pmod{\mathcal{O}_n}$ therefore $0 \equiv Y_n g_{n-1} + X_n h_{n-1} \pmod{\mathcal{O}_n}$. Thus from the uniqueness part of lemma (1) we get $X_n \equiv 0 \pmod{\mathcal{O}_n}$ and $Y_n \equiv 0(\mathcal{O}_n)$. We take $g_n = g_{n-1} + X_n$ and $h_n = h_{n-1} + Y_n$ obviously the polynomials g_n and h_n satisfy the conditions $(\alpha), (\beta)$ and (γ). Hence we get two sequences of polynomials (g_n) and (h_n). The respective coefficients of (g_n) and (h_n) converge as n tends to infinity because of the condition $g_{n+1} \equiv g_n \pmod{\mathcal{O}_{n+1}}$ and $h_{n+1} \equiv h_n \pmod{\mathcal{O}_{n+1}}$. Therefore $\lim\limits_{n\to\infty} g_n = g$ is a monic polynomial of degree s and $\lim\limits_{n\to\infty} h_n = b$ is power series over A which converges everywhere in A, because $h \equiv h_n \pmod{\mathcal{O}_{n+1}}$. We see immediately that $\underline{f} = gh\ \overline{h} = \psi$ and $\overline{g} = \varphi$. Moreover $\lambda_n(h) = d(h_n) = \lambda_n(f) - s$, because $h \equiv h_n \pmod{\mathcal{O}_{n+1}} \implies \lambda_{n+1}(h) = \lambda_{n+1}(h_n) = d(h_n) \leq \lambda_{n+1}(f) - s$ but $f = gh$ implies that $\lambda_{n+1}(f) \leq s + \lambda_{n+1}(h)$, therefore we get our result. If **29**
f is a polynomial then $\lambda_n(f)$ is constant for n sufficiently large implying $\lambda_n(h)$ is constant for n large, therefore h is a polynomial. Since g_n and h_n are strongly relatively prime modulo $\mathcal{O}_{n+1}$, there exist by lemma (1) polynomials a_n and b_n such that

$$1 \equiv a_n g_n + b_n h_n \pmod{\mathcal{O}_{n+1}},$$

where $$d(b_n) < s \quad \text{and} \quad d(a_n) < d(h_n) = \lambda_{n+1}(f) - s.$$

Similarly we have polynomials a_{n+1} and b_{n+1} such that

$$1 \equiv a_{n+1}g_{n+1} + b_{n+1}h_{n+1} \pmod{\mathscr{O}_{n+2}}$$

where $$d(b_{n+1}) < s \text{ and } d(a_{n+1}) < d(h_{n+1}) = \lambda_{n+2}(f) - s.$$

Combining these two we get

$$(a_{n+1} - a_n)g_n + (b_{n+1} - b_n)h_n \equiv 0 \pmod{\mathscr{O}_{n+1}}$$

Hence by uniqueness if lemma (1) we get $a_{n+1} \equiv a_n \pmod{\mathscr{O}_{n+1}}$ and $b_{n+1} \equiv b_n \pmod{\mathscr{O}_{n+1}}$. Since $d(b_n) < s$ for every n, we get that $\lim\limits_{n\to\infty} b_n = b$ is a polynomial, moreover $\lim\limits_{n\to\infty} a_n = a$ is everywhere convergent power series in A; a is a polynomial if f is a polynomial. Hence we get $1 \equiv ag + bh \pmod{\mathscr{O}_{n+1}}$ for every $n \geq 1$, which implies that g and h are strongly relatively prime in $A\,[[X]]$.

Uniqueness. If possible let us suppose that there exists another pair (g', h') satisfying the requirements of the lemma. Let $V = h - h'$ and $U = g' - g$. Since $\overline{g} = \overline{g'} = \varphi$ and $\overline{h} = \overline{h'} = \psi$, U is in $\mathscr{O}[X]$ and V is in $\mathscr{O}_1[[X]]$.

30 Let us assume that U belongs to $\mathscr{O}_n[X]$ and V belongs to $\mathscr{O}_n[[X]]$ for all $n < m, m > 1$. We have

$$f = gh = g'h' = (U + g)(V + h) = UV + Uh + gV + gh$$

which implies that $-UV = Uh + gV$. But UV is in $\mathscr{O}_{2n-2}[[X]]$ ($2n - 2 > n$, as $n > 1$), therefore

$$Uh + gV \equiv 0 \pmod{\mathscr{O}_n}$$

Let ρ_n be the canonical homomorphism from $\mathscr{O}_n A[[X]]$ onto $A/\mathscr{O}_n$ $[[X]]$. Obviously we have

$$\rho_n(U)\rho_n(h) + \rho_n(g)\rho_n(V) = 0, d(U) < s \tag{1}$$

But $\rho_n(h)$ and $\rho_n(g)$ are strongly relatively prime in $A\mathscr{O}_n[[X]]$, because they are so in $A/\mathscr{O}_1[[X]]$ and $\mathscr{O}_1/\mathscr{O}_n$ is contained in $r(A/\mathscr{O}_n)$, therefore by uniqueness part of lemma (1) we get from (1)

$$\rho_n(U) = 0 \text{ and } \rho_n(V) = 0$$

This means that $V = h - h' \equiv 0 \pmod{\mathscr{O}_n}$ and $U = g - g' \equiv 0 \pmod{\mathscr{O}_n}$ for every n. But $\cap \mathscr{O}_n = 0$, because A is a Hausdorff space, therefore $U = 0$ and $V = 0$. Hence the uniqueness of g and h is established.

Corollary 1. *Let K be a complete filed for a real valuation v. Let $f(X) = \sum_{n=0}^{\infty} a_n X^n$ be an every-where convergent powerseries with coefficient from $\mathscr{O}$. Let φ and ψ be two polynomials in $\mathscr{O}/\mathscr{Y}[X] = k[X]$ such that*

(1) *φ is monic of degree s.* 31

(2) *φ and ψ are strongly relatively prime in $k[X]$*

(3) *$\bar{f}$ (image of f in $k[X]$)$= \varphi\psi$*

Then there exists one and only one pair g and h such that

(1) *$g \in \mathscr{O}[X]$, g is monic of degree s and $\bar{g} = \varphi$*

(2) *$h \in \mathscr{O}[X]$, h converges everywhere in $\mathscr{O}$ and $\bar{h} = \psi$*

(3) *$f = gh$.*

and the radius of convergence of h is the same as that of f. If f is a polynomial, then h is a polynomial. Moreover g and h are strongly relatively prime.

Proof. Suppose that $\varphi = \sum_{r=o}^{s-1} \bar{a}_r X^r + X^s$ and $\psi = \sum_{u=0}^{t} \bar{b}_u X^u$. □

Let $\varphi_\circ = \sum_{r=0}^{s-1} a_r X^r + X^s, \psi_\circ u = \sum_{u=0}^{t} \bar{a}_u X^u$.

Obviously $\varphi_\circ$ is monic of degree s and $\bar{f} = \varphi_\circ\psi_\circ$, which implies that $f - \varphi_\circ\psi_\circ$ belongs to $\mathscr{Y}[[X]]$ i.e., if $f - \varphi_\circ\psi_\circ = \sum b_n X^n$, then $v(b_n) > 0$ for every n. Let $\alpha = \inf v(b_n), \alpha$ is obviously strictly positive. Let $\mathscr{O}_1 = \{x^n / x \in \mathscr{O}, v(x) \geq \alpha\}$, then $(\mathscr{O}_n)_{n>0}, \mathscr{O}_n = \mathscr{O}_1^n$ defines a decreasing filtration on $\mathscr{O}$. Obviously $\tilde{\varphi}_\circ$ and $\tilde{\psi}_\circ$ (images of φ and ψ in $\mathscr{O}/\mathscr{O}[X]$) are strongly relatively prime modulo $\mathscr{O}_1$ and $\tilde{\varphi}_\circ$ and $\tilde{\psi}_\circ$ satisfy all the requirements of Hensel's lemma, therefore there exists one and only one pair (g, h) such that

(i) g is monic polynomial of degree s and $\tilde{g} = \tilde{\varphi}_\circ$ **32**

(ii) h is an every where convergent powerseries in $\mathscr{O}$, $\tilde{h} = \psi_\circ$ and $\lambda_n(f) - s$.

(iii) $f = gh$

Form the choice of $\varphi_\circ$ and $\psi_\circ$ it is obvious that this pair (g, h) satisfies the conditions (1), (2) and (3) of the corollary.

If possible let there exist another pair (g', h') satisfying the conditions stated in the corollary. Let $g'' = g - g'$, $h'' = h - h'$ Since $\overline{g}''$ and $\overline{h}''$ are in $\mathscr{Y}[x]$, there exists $\alpha' > 0$ such that g'' and h'' are in $\mathscr{O}'_1[[x]]$ where $\mathscr{O}'_1 = \{x | x \in \mathscr{O}, v(x) \geq \alpha'\}$. Let us take in Hensel's lemma instead of $\mathscr{O}$ the ideal $\mathscr{O}'_1$ and the filtration defined by $(\mathscr{O}_n)$ where $\mathscr{O}'_n = \mathscr{O}^n_1$. But then have two pairs (g, h) and (g', h') satisfying the conditions $(a), (b), (c)$ of the lemma, which is not possible, therefore $g = g'$ and $h = h'$.

If f is a polynomial, the result about radius of convergence is obvious. Let us assume that f is not a polynomial, then $\lambda_n(f)$ tends to infinity as n tends to infinity. It has already been proved that $t_f = \lim_i \inf \dfrac{v(a_i)}{i}$. Since v is a real valuation, for any i we can find an integer k such that$(k-1)\alpha \leq v(a_i) \leq k\alpha, \Longrightarrow \lambda_k(f)$. Therefore $\dfrac{v(a_i)}{i} \geq \dfrac{(k-1)\alpha}{\lambda_k(f)}$ and

$$\lim_{i\to\infty} \inf \frac{v(ai)}{i} \geq \lim_{i\to\infty} \inf \frac{k\alpha}{\lambda_k(f)}$$

33 moreover for $i = \lambda_k(f)$ we have

$$\frac{k\alpha}{\lambda_k(f)} \geq \frac{v(a_i)}{i}.$$

Let $k \to \infty$, which implies that $i = \lambda_k(f) \to \infty$. Then we get

$$\lim_{i\to\infty} \inf \frac{k\alpha}{\lambda_k(f)} \geq \frac{v(a_i)}{i}$$

Thus $$\lim_{i\to\infty} \inf \frac{v(ai)}{i} = \lim_{n\to\infty} \frac{n\alpha}{\lambda_n(f)} = \lim_{n\to\infty} \frac{n\alpha}{\lambda_n(h)}$$

This proves that $t_f = t_n$.

Corollary 2. *Let K be a complete valuated field with a real valuation v and f a polynomial in $\mathscr{O}[X]$. Then if α in k is a simple root of $\overline{f}$, there exists one and only one element a in $\mathscr{O}$ such that a is a simple root of f and $\overline{a} = \alpha$.*

Proof. Since α is a simple root of $\overline{f}$, we have $\overline{f}(X) = (X-\alpha)\,\psi(X)$ where $\psi(\alpha) = 0$. Moreover $(X - \alpha)$ and $\psi(X)$ are strongly relatively prime in $k[X], (X - \alpha)$ being a prime element. Therefore form corollary 1, we have in one and only one way $f(X) = (X - a)h(X)$, where $\overline{h} = \psi$ and $\overline{a} = \alpha$. Moreover a is a simple root of f because

$$h(\overline{a}) = \overline{h}(\alpha) = \psi(\alpha) = 0.$$

In particular if K is a locally compact field such that characteristic $k \neq 2$, then we shall show that $K^*/(K^*)^2$ is a group of order 4.

K locally compact implies that v is discrete and k is a finite. Let π be 34
a uniformising parameter and let $C \in \mathscr{O}^* = \mathscr{O} - \mathscr{Y}$ be an element such that $\overline{C}$ is not a square in k, such an element exists because $k^*/(k^*)^2$ is of order 2. Then it can be seen that $1, C, \pi, C\pi$ represent the distinct cosets in $K^*/(K^*)^2$ and any element in K^* is congruent to one of them modulo $(K^*)^2$. ◻

2 Extension of Valuations - Transcendental case

In order to prove that a valuation of a field can be extended to an extension field it is sufficient to consider the following two cases:

(i) When the extension field is an algebraic extension.

(ii) When the extension field is a purely transcendental extension.

Proposition 1. *Let $L = K(X)$ be a purely transcendental extension of a field K with a valuation v, let Γ' be any totally ordered group containing Γ_v. Then for ξ in Γ' there exists one and only one valuation ω_{ξ_n} of L extending v such that*

$$w_\xi\left(\sum_{j=0}^{n} a_j x^j\right) = \inf_{0\leq j\leq n}\Big(v(a_j) + j\xi\Big)$$

Proof. It is sufficient to verify that w_ξ satisfies the axioms of a valuation for $K[X]$. The axioms $a_\xi(P) = \infty \Longleftrightarrow P = 0$ and $w_\xi(P + Q) \geq \inf(w_\xi(P), w_\xi(Q))$ can be easily verified. To prove $w_\xi(PQ) = w_\xi(P) + w_\xi(Q)$, where $P = \sum\limits_{j=0}^{n} a_j X^j$,

$Q = \sum\limits_{i=0}^{m} b_i X^i$ and $PQ \neq 0$, we write $P = P_1 + P_2, Q = Q_1 + Q_2, P_1$
35 being the sum of all terms $a_j X^j$ of P such that $w_\xi(P) = v(a_j) + j\xi$ and Q_1 being the sum of those terms $b_i X^i$ of Q for which $w_\xi(Q) = v(b_i) + i\xi$. Let j_o and k_o be the degree of P_1 and Q_1 respectively. If $P_1 Q_1 = \sum C_r X^r$, then we have

$$\begin{aligned} w_\xi(P_1 Q_1) &= v(C_{j_o + k_o}) + \xi(j_o + k_o) \\ &= v(a_{j_o}) + \xi j_o + v(b_{k_o}) + \xi k_o = w_\xi(P_1) + w_\xi(Q_1). \end{aligned}$$

Now

$$w_\xi(PQ) = w_\xi(P_1 Q_1 + P_1 Q_2 + Q_1 P_2 + P_2 Q_2) = w\xi(P_1 Q_1),$$

because the valuation of the other terms is greater than $w_\xi(P_1 Q_1)$. $\square$

This implies that

$$w_\xi(PQ) = w_\xi(P_1 Q_1) = w_\xi(P_1) + w_\xi(Q_1) = w_\xi(P) + w_\xi(Q).$$

Corollary. *There exists one and only one valuation w of $K(X)$ such that*

(i) *w extends v.*

(ii) $w(X) = 0$.

(iii) *The class $\overline{X}$ of X in k_w is transcendental over k_v.*

The valuation w is the valuation w_ξ for $\xi = 0$ and k_w is a purely transcendental extension of degree 1 *over k_v.*

It is obvious that w_o(i.e. w_ξ for $\xi = 0$) satisfies (1) and (2) and that $k_{w_o} = k_v(\overline{X}_n)$.If $\overline{X}$ were algebraic over k_v, then there exists a polynomial $\overline{P}(Y) = \sum\limits_{j=0}^{n} \overline{a}_j Y_j$ such that at least one $\overline{a}_j \neq 0$ and $\overline{P}(\overline{X}) = 0$, which means

36 that $P(X) = \sum_{j=0}^{n} a_j X^j$ is in $\mathscr{Y}_w$, where at least one a_j is not in $\mathscr{Y}_v$ and all a_j are in $\mathscr{O}_v$. But this is impossible because $w(P(X)) = \inf_j v(a_j) = 0$. Conversely let w be a valuation of $K(X)$ satisfying 1), 2), 3). Let $P = \sum_{i=0}^{m} a_i X^i$ be a polynomial over K. We have to prove that $w(P) = \inf v(a_i)$. Let $P = \sum_{i=0}^{m} a_i X^i$ be a polynomial over K. We can assume without loss of generality that a_i are in $\mathscr{Y}_v$ and at least one of them is not in $\mathscr{Y}_y$, then $\inf_i v(a_i) = 0$. If $w(P) > 0$, then $\overline{P} = 0$ in k_w, which implies, that $\overline{X}$ is algebraic over k_v, which is a contradiction. But we know that

$$w\left(\sum_i a_i X^i\right) \geq \inf_i \{v(a_i) + iw(X)\} = 0$$

therefore $w(P) = \inf_i v(a_i)$.

3 Residual Degree and Ramification Index

Let L be a field and K a subfield of L. Let w be a valuation of L and v the restriction of w on K. Since $\mathscr{Y}_w \cap K = \mathscr{Y}_v$, the filed k_v can be imbedded in the field k_w. We shall say the dimension of k_w over k_v the *residual degree of w with respect to v* or of L with respect to K. We shall denote it by $f(w, v)$.

The index of the group Γ_v in Γ_w is called the *ramification index of w* with respect to v or of L with respect to K and is denoted by $e(w, v)$.

If no confusion is possible, we shall denote $f(w, y)$ by $f(L, K)$ and 37
$e(w, v)$ by $e(L, K)$.

If $e(w, v) = 1$, then L is said to be an *unramified extension* of K.

If $f(w, v) = 1$, L is said to be *totally ramified* extension of K.

Since the group of values and residual field of $\hat{K}$ are the same as that of K we have

$$e(\hat{L}, \hat{K}) = e(L, K) \text{ and } f(\hat{L}, \hat{K}) = f(L, K)$$

Proposition 2. *Let L be a filed with a valuation w and let K be a field contained in L and v the restriction of w on K. Then $e(L,K)f(L,K) \leq (L:K) = n$, where $(L:K)$ is dimension of L over K.*

Proof. If n is infinite, the result is trivial. Let us assume that n is a finite number. Let $r \leq e$ and $s \leq f$ be two positive integers, then we can find r elements $X_1, \ldots, X_r$ in L^* such that $w(X_i) \not\equiv w(X_j) \pmod{\Gamma v}$ for $i \neq j$ and s elements $\overline{Y}_1, \ldots \overline{Y}_s$ in k_w such that they are linearly independent over k_v. Let $Y_1, \ldots Y_s$ be a system of representatives for $Y_1, \ldots Y_s$ in $\mathscr{O}_w^*$. Then the elements $(X_iY_j, i = 1, \ldots, r; j = 1, 2, \ldots s)$ are linearly independent over K. If they are not linearly independent, then there exists elements a_{ij} in K not all 0 such that

$$\sum_{i,j} a_{ij} X_i Y_j = 0$$

38 Let $\alpha = \inf_{i,j} w(a_{ij}X_iY_j)$, obviously α is finite and belongs to Γw. Therefore $w(a_{kl}X_kY_l) = \alpha$ for some k and l. We have

$$\begin{aligned} w(a_{ij}X_iY_j) &= w(a_{ij}) + w(X_i) + w(Y_j) \\ &= w(a_{kl}) + w(X_k) + w(Y_l) \\ \text{if } w(a_{ij}X_iY_j) &= \alpha \text{ for some } i \text{ and } j. \end{aligned}$$

But $w(Y_j) = w(Y_l) = 0$, therefore we get $w(X_i) \equiv w(X_k) \pmod{\Gamma_v}$, which is possible only if $i = k$. Thus we get

$$a_{kl}X_kY_l + \sum_{j \neq l} a_{kj}X_kY_j \equiv 0 \pmod{\mathscr{O}'} \tag{1}$$

where $\mathscr{O}' = \{X/X \in L, w(X) > \alpha\}$

Multiplying the congruence (1) with $a_{kl}^{-1}X_k^{-1}$ we get

$$Y_l + \sum_{j \neq l} a_{kl}^{-1} a_{kj} Y_j \equiv 0 \pmod{\mathscr{Y}_w}.$$

Therefore

$$\overline{Y}_l + \sum_{j \neq l} \overline{(a_{kl}^{-1}a_{kj})}\,\overline{Y}_j = 0, \text{ where } \overline{a_{kl}^{-1}a_{kj}} \text{ are in } k_v.$$

But this is impossible, because $\overline{Y}_1 - - - \overline{Y}s$ are linearly independent over k_v, therefore $(X_i Y_j)$ are linearly independent over K. Since $(L : K) = n$, the number of linearly independent vectors in L over K cannot be greater than n.

Hence $ef \leq n$. □

Corollary 3. *If L is algebraic over K, then k_w is algebraic over k_v and Γ_l / Γ_k is a torsion group of order $\leq (L : K)$.*

The assertion is trivial when $(L : K)$ is finite. When $(L : K)$ is infinite we can write $L = \bigcup_{i \in I} L_i$ and $k_L = \cup k_{Li}$, where L_i is a finite algebraic extension of K.

Then Γ_L / Γ_K is the union of the quotient groups Γ_{L_i} / Γ_K for i in I and 39
therefore it is a torsion group.

Corollary 4. *Suppose that L is algebraic over K, then w is improper if and only if v is improper.*

v improper implies that $\Gamma_v = \{0\}$. Therefore by corollary (3) Γ_w is a torsion group. But Γ_w is a totally ordered and abelian group, therefore it consists of identity only.

Corollary 5. *Let $(L : K)$ be finite. Then w is discrete if and only v is discrete.*

v discrete implies that Γ_v is isomorphic to Z and $(L : k)$ finite implies Γ_w / Γ_v is of finite order. Moreover Γ_w is Archimedian, because if α and β are in Γ_w, then $n\alpha$ and $n\beta$ where n = order Γ_w / Γ_v, are in Γ_v; therefore there exists an integer q such that $qn\alpha > n\beta$, which shows that $q\alpha > \beta$. There exists a smallest positive element in Γ_w. For, each coset of Γ_w / Γ_v has a smallest positive element, the smallest among them is the smallest positive element fo Γ_w. Hence Γ_w is isomorphic to z.

Corollary 6. *If the valuation v on K is discrete, K is complete and $(L : K)$ is finite, then $ef = (L : K)$.*

Proof. Let π be a uniformising parameter in L. Let $\overline{Y}_1, \ldots, \overline{Y}_f$ be a basis of k_w over k_v and $Y_1, \ldots, Y_f$ their representatives in $\mathcal{O}_w^*$. Let $\mathscr{R}$ denote a system of representatives of k_v in $\mathcal{O}_v^*$. □

40 Then any element X in $\mathscr{O}_w$ can be written in the form $\sum_{i=1}^{f} \alpha_i Y_i$ modulo $\mathscr{Y}_w$ with $\alpha_i \in \mathscr{R}$ in one and only one way. Let L' be vector space over K generated by $(Y_i \pi^j)$ for $i = 1, 2, \ldots, f$ and $j = 0, 1, 2, \ldots, e-1$. Since L' is a finite dimensional vectorspace over a complete field K, L' is complete (for proof see Espaces Vectoriels Topologiques by N. Bourbaki, chapter I section 2) and therefore closed in L. But L' is dense in L, because for every element X in L and an integer n there exists an element X_n is L' such that $v(X - X_n) \geq n\ e$. For sufficiently small n the result is obviously true. Let us assume that it is true for all integers $r \leq n$. Since n e is in Γ_v, there exists an element U in K such that $w(U) = v(U) = n\ e$. Therefore $U^{-1}(X - X_n)$ belongs to $\mathscr{O}_w$ and we have

$$U^{-1}(X - X_n) \equiv \sum_i \alpha_{io} Y_i \pmod{\mathscr{Y}_w = \mathscr{O}_w \pi}$$

This means that $\pi^{-1}[(U^{-1}(X - X_n) - \sum_i \alpha_{io} Y_i]$ belongs to $\mathscr{O}_w$, therefore

$$\pi^{-1}\left[(U^{-1}(X - X_n) - \sum_i \alpha_{io} Y_i)\right] \equiv \sum_i \alpha_{i1} Y_i \pmod{\mathscr{Y}_w}$$

Proceeding in this way we obtain

$$U^{-1}(X - X_n) \equiv \sum_i \alpha_{io} Y_i + \cdots + \sum_i \alpha_{ie-1} Y_i \pi^{e-1} \pmod{\mathscr{Y}_w^e}$$

or
$$(X - X_n) \equiv U\left[\sum_{j=0}^{e-1} \sum_i \alpha_{ij} Y_i \pi^j\right] \pmod{\mathscr{Y}_w^{(n+1)e}}$$

41 Let us take $X_{n+1} = X_n + U\left[\sum_{j=0}^{e-1} \sum_i \alpha_{ij} Y_i \pi^j\right]$.

Then $w(X - X_{n+1}) \geq (n + 1)e$. Thus L' is dense in L and therefore $L' = L$. So $n = (L : K) \leq ef$. But we know that $ef \leq n$, therefore $n = ef$.

4 Locally compact Fields

Proposition 3. *If K is a locally compact filed of characteristic o with a discrete valuation v, then K is a finite extension of Q_p where p is* *characteristic of the residual field k.*

Proof. Since characteristic $K = 0, K$ contains Q the field of retinal numbers. We see immediately that v is proper, because if v is improper then Q is contained in k which is a finite field by theorem in §7.1 and this is impossible. The restriction of v to Q is v_p for some p because p adic valuations are the only proper valuations on Q and this p is the characteristic of k. We have already proved in §7.1 that K is complete, therefore K contains Q_P. The valuation v on K is discrete, therefore Γ_v is isomorphic to Z, but Γ_{v_p} is also isomorphic to Z and is contained in Γ_v, therefore $= (\Gamma_v : \Gamma_{v_p})$ is finite. Moreover $f = (k_v : k_{v_p})$ is also finite, because k_v is a finite filed. Hence $(K : Q_p) = e\ f$ (by corollary 4 of **42**
§3.2) is finite. ◻

Proposition 4. *Let K be complete filed for a real proper valuation v such that*

(1) *characteristic K= characteristic k.*

(2) *k and all its sub fields are perfect.*

Then there exists a subfield $F \subset \mathscr{O}$ which is a system of representatives of k in $\mathscr{O}$. Moreover if v is discrete then K is isomorphic to $k((x))$.

Proof. Let Φ be the family of subfields S of $\mathscr{O}$ such that the restriction of φ, the canonical homomorphism from $\mathscr{O}$ onto k to S is an isomorphism onto a subfield of k. The family $\Phi \neq \phi$, because the prime fields contained in $\mathscr{O}$ and k are the same. Obviously Φ is inductively ordered by inclusion, therefore by Zorn's lemma it has a maximal element F. We shall prove that $k = \varphi(F)$. The field k is algebraic over $\varphi(F)$. If possible let there exist an element $\bar{x}$ in k transcendental over $\varphi(F)$. Let $\varphi(x) = \bar{x}$, where x is in $\mathscr{O}$, then x is transcendental over F. It is obvious that $F(x)$ is isomorphic to $\varphi(F)(\bar{x})$, which contradicts the maximality of F, therefore k is algebraic over $\varphi(F)$. Suppose that $\varphi(F)$, then there exists one element $\bar{x}$ in k and not in $\varphi(F)$. Since $\varphi(F)$ is a perfect field, $\bar{x}$ is a simple root of an irreducible monic polynomial $\bar{P}$ over $\varphi(F)$. Let

$\bar{P} = X^s + \bar{a}_{s-1}X^{s-1} + \cdots + \bar{a}_o = (X - \bar{x})\bar{Q}$, where $\bar{Q}$ is some polynomial **43**
over $\varphi(F)$ and $\bar{Q}(\bar{x}) \neq 0$.

By Corollary (4) fo Hensel's lemma we obtain that the polynomial $P = X^S + a_{s-1}X^{s-1} + \cdots + a_0$ has a simple root x in $\mathscr{O}$ such that $\varphi(x) = \bar{x}$ and Q is an irreducible polynomial. Therefore $F(x)$ is isomorphic to $F[X]/(P)$. But $\varphi(F)(\bar{x})$ is isomorphic to $\varphi(F)[X]/(\bar{P})$ therefore we see that φ is still an isomorphism from $F(x)$ onto $\varphi(F)(\bar{x})$. But this is impossible, because F is a maximal element of Φ. Thus our theorem is proved. □

When v is discrete, we have seen that every element x in K is of the form $\sum\limits_{i=m}^{\infty} r_i\pi^i$ with r_i in F and conversely. Therefore the mapping $\sum\limits_{i=m}^{\infty} r_i\pi^i \to \sum\limits_{i=m}^{\infty} \varphi(r_i)X^i$ is from K onto $k((x))$. It is trivial to see that it is an isomorphism.

Corollary. *A non-discrete locally compact valuated field of characteristic $p > o$ is isomorphic to a field of formal power series over a finite field.*

Since we have already proved in §7.1 that a locally compact valuated field K is complete, its valuation is discrete and k is finite, our corollary follows from the theorem.

5 Extension of a Valuation to an Algebraic Extension (Case of a Complete Field)

44 **Theorem 1.** *If L is an algebraic extension of a complete field K with a real valuation v, then there exists one and only valuation w on L extending v.*

Proof. If v is improper w is necessarily improper. So we assume that v is a proper valuation. Suppose that L is a finite extension of K. If there exists a valuation w on L extending v, then w is unique, because on L any valuation defines the same topology as that of $K^{(L:K)}$ and the topology on L determines the valuation upto a constant factor and in this case the constant factor is also determined because the restriction of the valuation to K is v. □

Let L be a Galois extension of K. Then if w is a valuation on L extending v, $w\ o\ \sigma$ for any σ in $G(L/K)$ (the Galois group of L over K) is also a valuation extending v. Therefore by uniqueness of the extension $w(x) = Wo\sigma(x)$ for every x in L. This shows that

$$v\,(\underset{L/K}{N}(x)) = w(\prod_{\sigma}(x)) = \sum_{\sigma} w\ o\ \sigma(x) = n\ o\ w(x)$$

where $(L : K) = n$.

Thus

$$w(x) = \frac{1}{n}\, v\,(\underset{L/K}{N}(x)). \tag{1}$$

Now suppose that L is any finite extension of K of degree n. We **45**
define a mapping w on L by (1) and prove that it satisfies the axioms for a valuation. It is well known that (Bourbaki, algebra chapter V, §8) that if L is the separable closure of K is L, and if p is the characteristic exponent of K (i.e., $p = 1$ if characteristic $K = 0$ and p= characteristic $K \neq 0$), then

$$n = (L : K) = qp^e$$

with $q = (L' : K)$ and $p^e = (L : L')$. Moreover L is a purely inseparable extension of L', and for each K-isomorphism σ_i $(1 \leq i \leq q)$ of L', in an algebraic closure Ω of K there exists one and only one K-isomorphism of L which extends σ_i. This extended isomorphism will also be denoted by σ_i. Then

$$N_{L/K}(x) = \left[\prod_{i=1}^{q} \sigma_i(x)\right]^{p^e}$$

It is easy to prove that $w(x) = \infty$ if and only if $x = 0$ and $w(xy) = w(x) + w(y)$ for x, y in L. To prove that $w(x + y) \geq \inf(w(x), w(y))$, it is sufficient to prove that $w(\alpha) \geq 0$ implies that $w(1 + \alpha) \geq 0$ for any α in L. We know that if $P(X) = X^r + a_{r-1}X^{r-1} + \cdots + a_o$ is the monic irreducible polynomial of α over K, then $\underset{L/K}{N}\alpha = (a_o)^{\frac{n}{r}}$ and $P(1 - X)$ is the irreducible polynomial of $1 + \alpha$. Thus

$$\underset{L/K}{N}(1 + \alpha) = (-1)^r \{(1 + a_{r-1} + \cdots + (-1)^r a_o)\}^{\frac{n}{r}} = b_o$$

So to prove our result we have to show that b_o is in $\mathscr{O}$ when a_o is in $\mathscr{O}$, because $w(\alpha) = \dfrac{v(a_o)^{n/r}}{n}$. This will follow from the following theorem, which completely proves our theorem. 46

Theorem 2. *Let K be complete field with a real valuation v and x any element of an algebraic extension of K. If $f(X) = X^r + a_{r-1}X^{r-1} \cdots + a_o$ is the minimum polynomial of x over K, then a_o belonging to $\mathscr{O}$ implies that all the coefficients of $f(X)$ are in $\mathscr{O}$.*

Proof. If possible suppose that all a_i are not in $\mathscr{O}$, then $v(a_j) < 0$ for some $j, 0 < j < r$. Let $-\alpha = \inf v(a_j), \alpha > 0$ and j the smallest index such that $v(a_j) = -\alpha$. We have $o < j < r$. Since α belongs to Γ_v, there exists an element C in K such $v(C) = \alpha$. Consider the polynomial $g = Cf(X) = CX^k + \cdots + C_{a_j}X^j + \cdots + C_\circ a$. Because of the choice of $j, \overline{g} = \cdots + \overline{r}_j X^j$, where $\overline{r}_j = \overline{ca}_j \neq 0$. Therefore $\overline{g}$ has X^j as a factor which is a monic polynomial and if $\overline{g} = X^j\psi$, then X^j and ψ satisfy the requirements of Corollary (4) of Hensel's lemma, which gives that g is reducible, which is a contradiction. Hence all a_j are in $\mathscr{O}$. ◻

When L is infinite algebraic extension of K, we can express $L = \bigcup\limits_{i \in I} L_i$ where each L_i is a finite algebraic extension of K and the family
47 $\{L_i\}_{i \in I}$ is a directed set by the relation of inclusion. We define the valuation w for any x in L as $w(x) = w_i(x)$ if x is in L_i and w_i is the extension of v on L_i. It is obvious that w is the unique valuation on L extending v.

6 General Case

We shall study now how a valuation of an incomplete field can be extended to its algebraic extension.

Let K be field with a valuation v and L an algebraic extension of K. If w is a valuation of L extending v, we can look at the completion $\hat{L}$ of L. $\hat{L}$ contains L and $\hat{K}$, so it contains a well defined composite extension M_w of L and $\hat{K}$. Then there exist one and only one maximal ideal m_w in $L \underset{K}{\otimes} \hat{K}$ such that the canonical mapping from $L \underset{K}{\otimes} \hat{K} \to M_w$ gives an isomorphism from $L \underset{K}{\otimes} \hat{K}/m_w$ onto M_w. So we get a map φ from the set of the valuation w extending v to the set of the maximal ideals of $L \underset{K}{\otimes} \hat{K}$. Conversely if we start from a maximal ideal $\mathcal{M}$ in $L \underset{K}{\otimes} \hat{K}$, then the corresponding composite extension $M = L \otimes \hat{K}/\mathcal{M}$ is an algebraic extension of K and there one and only one valuation w_M of M which extends v and the restriction of w_M to L gives a valuation of L extending v. So we get a map ψ from the set of the maximal ideals of $L \underset{K}{\otimes} \hat{K}$ (or of the classes of complete extensions) to the set of the valuations of L extending v.

Moreover the completion $\hat{L}$ of L with respect to w_M is exactly $\hat{M}$ **48**
and the composite extension of L and $\hat{K}$ contained in $\hat{L}$ is M.So we have $\varphi \circ \psi = I$ (identity map)

Now we have also $\psi \circ \varphi = I$, for if w is any valuation of Lthen the valuation w_{M_w} is necessarily the same as w by the uniqueness of the extension to M of the valuation v of $\hat{K}$.

Hence there exists a 1-1 correspondence between the set of valuations on L extending v and the set of inequivalent composite extensions of L and $\hat{K}$.

In particular if $(L : K) = n < \infty$, then any composite extension of L and $\hat{K}$ is complete which means that $\hat{L} = L \underset{K}{\otimes} K/\mathcal{M}$, where $\mathcal{M}$ is some maximal ideal of $L \underset{K}{\otimes} \hat{K}$.

Suppose L is an algebraic extension of an incomplete valuated field K with a valuation v. Let $(w_i)_{i \in I}$ be the set of valuations on L extending v. We shall denote by L_i the field L with the valuation w_i, by e_i the ramification index $e(L_i : K) = e(\hat{L}_i : \hat{K})$ by f_i the residual degree $f(\hat{L}_i : \hat{K}) = f(L_i : K)$ and by n_i the dimension of $\hat{L}_i$ over $\hat{K}$.

The sequence

$$0 \to r(L \underset{K}{\otimes} \hat{K}) \to (L \underset{K}{\otimes} \hat{K}) \to \prod_{i \in I} \hat{L}_i$$

is exact, because the radical of $L \underset{K}{\otimes} \hat{K}$ is the intersection of all the maximal ideals of $L \underset{K}{\otimes} \hat{K}$, that is of all the kernels of the map $L \underset{K}{\otimes} \hat{K} \to L_i$. If the **49**
dimension of L over K is finite we have the following result.

Theorem 3. *If L is a finite extension of degree n of a field K with a real valuation v, then there exist, only finitely many different valuations (w_i) on L extending v. Moreover we have $\sum n_i \leq n$ and the sequence*

$$0 \to r(L \underset{K}{\otimes} \hat{K}) \to L \underset{K}{\otimes} K \to \prod \hat{L}_i \to 0$$

is exact.

Proof. We observe that w_i is not equivalent to w_j for $i \neq j$, because w_i equivalent to $w_j$means that they differ by a constant factor and since their restriction to K is same, we have $w_i = w_j$

The number of different valuations (w_i) on L extending v is finite because the number of inequivalent composite extensions of L and $\hat{K}$ is finite. To prove that the sequence is exact, we have to show that the mapping $\rho : L \underset{K}{\otimes} \hat{K} \to \prod \hat{L}_i$ is surjective.By the approximation theorem of valuations $\rho(L)$ is dense in $\prod \hat{L}_i$, therefore $\rho(L \underset{K}{\otimes} \hat{K})$ is dense in $\prod \hat{L}_i$, where ρ is the canonical map from $L \to \prod \hat{L}_i$. But $\rho(L \underset{K}{\otimes} \hat{K})$ is a finite dimensional vector space over $\hat{K}$ therefore it is complete. Hence $\rho(L \underset{K}{\otimes} \hat{K}) = \prod \hat{L}_i$ i.e., ρ is onto. Obviously dim $\prod \hat{L}_i \leq$ dim $L \underset{K}{\otimes} \hat{K}$ over $\hat{K}$,which means that $\sum n_i \leq n$. □

50 **Corollary.** *If $\hat{K}$ or L is separable over K, then we have $\sum n_i = n$.*

$\hat{K}$ or L separable over K implies that $r(\hat{K} \underset{K}{\otimes} L) = 0$ (for proof see Algebre by N. Bourbaki chapter 8 section 7), therefore ρ is an isomorphism.

7 Complete Algebraic Closure of a p-adic Field

Proposition 5. *Let K be a complete field with a real valuation v and Ω the algebraic closure of K.Then $\hat{\Omega}$ the completion of Ω by the valuation extending v is algebraically closed.*

We shall denote the extended valuation also by v.

Proof. To prove that $\hat{\Omega}$ is algebraically closed we have to show that any irreducible polynomial $f(X)$ in $\hat{\Omega}[X]$ has a root in $\hat{\Omega}$. Without loss of generality we a can assume that $f(X)$ is in $\mathscr{O}_{\hat{\Omega}}[X]$ and leading coefficient of $f(X)$ is 1. Suppose that $f(X) = X^r + a_{r-1}X^{r-1} + \cdots + a_0$ then for every integer m there exists a polynomial $\varphi_m(X) = X^r + b^{(m)}X^{r-1} + \cdots + b_\circ^{(m)}$ in $\mathscr{O}_\Omega[X]$ such that for every x in $\mathscr{O}_{\hat{\Omega}}^{r-1}$, $v(f(x) - \varphi_m(x) > rm$ Let $\varphi_m(X) = \prod_{j=1}^{r}(X - \alpha_{jm})$, α_{jm} are in $\mathscr{O}_\Omega$ as $\varphi_m(X)$ is in $\mathscr{O}_\Omega[X]$. Then

$$\varphi_{m+1}(\alpha_{jm}) = \varphi_{m+1}(\alpha_{jm}) - f(\alpha_{jm}) + f(\alpha_{jm}) - \varphi_m(\alpha_{jm})$$

implies that $$v(\varphi_{m+1}(\alpha_{jm})) > \text{ rm}$$

or $$\sum_{t=1}^{r} v(\alpha_{jm} - \alpha_{tm+1}) > \text{ rm.} \qquad \square$$

Therefore there exists a root α_{tm+1} of $\varphi_{m+1}(X)$ such that

$$v(\alpha_{jm} - \alpha_{t_{m+1}}) > m.$$

So we get a sequence $\left\{\varphi_m(X)\right\}$ of polynomials converging to f and 51
a sequence of elements $\left\{\beta_m\right\}$ converging to β in $\hat{\Omega}$ and each β_m is a root of $\varphi_m(X)$. Since polynomials are continuous functions, we have $\lim\limits_{m\to\infty} f(\beta_m) = f(\beta)$

But $\lim\limits_{m\to\infty} f(\beta_m) = 0$, because given integer $N > 0$, for $m > N$ we have $v(f(\beta_m)) = v(f(\beta_m) - \varphi_m(\beta_m)) > rm > N$.

Hence β is a root of $f(X)$.

One can easily prove that the residual field of $\hat{\Omega}$ is the algebraic closure of the residual field of K. In particular if $K = Q_p$, then the residual field of $\hat{\Omega}$ i.e., $k_{\hat{\Omega}}$ is algebraic closure of $Z/(P)$.Thus

$k_{\hat{\Omega}} = \cup F_i$, where each F_i is a finite extension of $Z/(P)$

8 Valuations of Non-Commutative Rings

We define a valuation of a non-commutative ring A without zero divisors containing the unit element in the same way as of a commutative ring. Almost all the results proved so far about valuated can be carried over to division rings with valuations with obvious modifications. WE mention the following facts far illustration.

Let L be a division ring with a valuation v.Then

(1) The set $\mathscr{O}_L = \left\{x/x \in L, v(x) \geq 0\right\}$ is a non-commutative ring,which we call the valuation ring of L with respect to the valuation v.

52 (2) $\mathscr{Y}_L = \left\{x/x \in L, v(x) > 0\right\}$ is the unique two sided maximal ideal of $\mathscr{O}_L$.

(3) Any ideal in $\mathscr{O}_L$ is a two sided ideal. For, $v(x^{-1}yx) = -v(x) + v(y) + v(x) \geq 0$ for x in L and y in $\mathscr{O}_L$ which means that $x^{-1}yx$ belongs to $\mathscr{O}_L$, therefore $yx = xz$ for some z in $\mathscr{O}_L$. Hence $\mathscr{O}_L x = x\mathscr{O}_L$.

(4) The ideals of $\mathscr{O}_L$ are any one of the two kinds

$$I_\alpha = \left\{x|v(x) > \alpha \geq 0\right\}$$
$$I'_\alpha = \left\{x|v(x) \geq \alpha > 0\right\}$$

(5) The division ring L is locally compact non-discrete division ring for the valuation v if and only if v is a discrete valuation, L is complete and $\mathscr{O}/\mathscr{Y}_L$ is finite

Regarding the extension of valuations to an extension division ring we prove the following.

Theorem 4. *Let $\widetilde{P}$ be a division algebra of finite rank over a complete valuated field P with a valuation v such that P is contained in the centre of $\widetilde{P}$. Then there exists one and only one valuation w of $\widetilde{P}$ which extends v.*

Proof. Existence We define $\underset{\widetilde{P}/P}{N}(x)$ = determinant of the endomorphism

$$\rho_x y \to xy \text{ of } \tilde{P}, \text{ for any } x \text{ in } \tilde{P}.$$

We shall prove that $w(x) = \dfrac{1}{r} v(\underset{\widetilde{P}|P}{N}(x)$ is a valuation of $\widetilde{P}$ if r is the
53 rank of $\widetilde{P}$ over P. The axioms $w(x) = \infty$ if and only if $x = 0$ and $w(xy) = w(x) + w(y)$ are obviously true.

To prove $w(x + y) \geq \inf(w(x), w(y))$ it is sufficient to prove that $w(x) \geq 0$ implies $w(1 + y) \geq 0$. Let $F = P(x)\, F$ is clearly a field containing P and $\widetilde{P}$ is a vector space over F by left multiplication. The mapping ρ_x is an F endomorphism. We know that if U is any F-endomorphism and U_p the P-endomorphism defined by U, then $\det U_p = \underset{F/P}{N}(\det U)$ and we have $\det \rho_x = (x)^{(\tilde{P}:F)}$ if ρ_x is considered as an F-endomorphism. Therefore we have

$$w(x) = \frac{1}{r}(\widetilde{P} : F) = v(\underset{F/P}{N}(x)).$$

□

Now $w(x) \geq 0 \iff vv(\underset{F/P}{N}(x)) \geq 0 \implies v(\underset{F/P}{N}(1 + x)) \geq 0$, because we have proved this for commutative case.Hence w is a valuation on $\tilde{P}$.

Uniqueness. Since P is complete and P is of finite rank r over P, any valuation defines the same topology on $\tilde{P}$ as that of P^r. But the topology determines the valuation upto a constant factor, If w_1 and w_2 are two valuations of $\widetilde{P}$ extending v then $w_1 = Cw_2$ for some C in P.But restriction of w_1 to w_2 to P is v, therefore $C = 1$ and $w_1 = w_2$.

Part II

Representations of classical groups over p-adic Fields

Chapter 3

Representations of Locally Compact and Semi-Simple Lie Groups

1 Representations of Locally Compact Groups

In this section we give a short account of some definitions and results 54
about the representations of locally compact groups.We assume the fundamental theorem on the existence and uniqueness (upto a constant factor) of right invariant Haar measure on a locally compact groups.For simplicity we assume that the locally compact groups in our discussion are unimodular i.e., the Haar measure is both right and left invariant.By $L(G)$ we shall denote the space of continuous complex valued functions with compact support and by $L(G, K)$, where K is some compact set of G,the set of elements of $L(G)$ whose support is contained in K.Obviously we have $L(G) = \underset{K \subset G}{\cup} L(G, K)$ and $L(G, K)$ is a Banach space under the norm $f = \sup\limits_{x \in K} |f(x)|$.

The space $L(G)$ can be provided with a topology by taking the direct limit of the topologies of $L(G, K)$. This topology makes $L(G)$ a locally convex topological vector space.

Let G be a locally compact group and H a Banach space

Definition 1. A continuous representation U of G in H is a map $x \to U_x \in \operatorname{Hom}(H, H)$ such that

(i) $U_{xy} = U_x \circ U_y$ for $x; y$ in G.

(ii) The map $H \times G \to H$ defined by $(a, x) \to U_x$ a is continuous.

55 **Definition.** Let H be a Hilbert space.The representation U is said to be Unitary if U_x is a unitary operator on H for every x in H.

Let $M(G)$ be the space of measures on G with compact support.The space $M(G)$ is an algebra for the convolution product defined by

$$\mu * \nu(f) = \int\int f(xy)\, d\mu(x)\, d\nu(y)$$

The space $L(G)$ can be imbedded into $M(G)$ by the map $f \to \mu_f = f(x)dx$. It is infact a subalgebra of $M(G)$ because $\mu_f * \mu_g = \mu_{f*g}$ where

$$f * g(x) = \int f(xy^{-1})g(y)dy.$$

Moreover if ν is any element of $M(G)$, then $\mu_f * \nu$ belongs to $L(G)$, because for any $g \in L(G)$ we have

$$\begin{aligned}(\mu_f * \nu)(g) &= \iint g(xy)f(x)dxd\nu(y)\\ &= \int d\nu(y) \int g(x)f(xy^{-1})dx.\\ &= \mu_h(g) \text{ where } h(x) = \int f(xy^{-1})d\nu(y)\end{aligned}$$

Thus we define the convolution of a measure μ and function $f \in L(G)$ by setting

$$(\mu * f)(y) = \int f(x^{-1}y)d\mu(x)$$
$$(f * \mu)(y) = \int f(yx^{-1})d\mu(x)$$

Let U be a representation of G in H. Then U can be extended to $M(G)$ by setting

$$U_\mu(a) = \int_G U_x a d\mu(x) \text{ (for a } \in H, \mu \in M(G))$$

Now let H be a Hibert space and U a Unitary representation. **56**
Then if μ and ν are any two elements in $M(G)$, we have

$$\begin{aligned}
\langle U_\nu U_\mu a, b\rangle &= \int \langle U_x U_\mu a, b\rangle d\nu(x)\\
&= \int \langle U_\mu a, U_{x^{-1}} b\rangle d\nu(x)\\
&= \int d\nu(x) \int \langle U_y a U_{x^{-1}} b\rangle d\mu(y)\\
&= \int \langle U_x U_y a, b\rangle d\nu(x) d\mu(y)
\end{aligned}$$

This means that $U_{\mu * \nu} = U_\mu \circ U_\nu$ i.e.,

U is a representation of the algebra M(G).It can be easily verified that map $\mu \to U_\mu$ is a continuous representation of the algebra M(G). Moreover

$$\begin{aligned}
\langle U_\mu^* a, b\rangle &= \langle \overline{U_\mu b, a}\rangle\\
&= \int \langle U_x a, b\rangle d\overline{\mu(x^{-1})}
\end{aligned}$$

This shows that $U_\mu^* = U_{\tilde{\mu}}$, where $d\tilde{\mu}(x) = d\overline{\mu(x^{-1})}$.

Thus the operator $U_{\mu * \tilde{\mu}}$ on H is Hermitian.

In particular we get a representation of $L(G)$ in H given by $f \to U_{\mu_f} = U_f$, where

$$U_f(a) = \int_G U_x a f(x) dx.$$

We can also get a representation of $M(G)$ by considering regular representations of G i.e., representations G by right or left translations in G in any function space connected with G with some convenient topology, for instance the space $L(G)$ or $L^2(G)$ (the space of square integrable functions).

We shall denote by σ_x the left regular representations and by τ_x the right regular representations of G i.e., for any function f on G we have 57

$$\sigma_x(f)(y) = f(x^{-1}y), \tau_x(f)(y) = f(yx)$$

we have for any μ in $M(G)$

$$\sigma_\mu(f) = \mu * f$$
$$\tau_\mu(f) = f * \overset{v}{\mu} \text{ where } d\overset{v}{\mu}(x) = d\mu(x^{-1})$$

Let K be a compact group, M an equivalence class of (unitary) irreducible representations of K. For any x belonging to G, let $M_x = (C^M_{ij}(x))$ be the matrix of M_x with respect to some basis of the representation space. Let r_M be the dimension of M and $\chi_M = \sum\limits_{i=1}^{r_m} C^M_{i\,i}$ the character of M. For any two irreducible unitary representations of K we have the following orthogonality relation,

(1) $C^M_{ij} * C^{M'}_{kl}$ if $M \neq M'$

(2) $C^M_{ij} * C^M_{kl} = \dfrac{l}{r_M}\delta_{jk}C^M_{il}$

where the value of the convolution product at the unit element e of G is given by $C^M_{ij} * C^M_{kl}(e) = \int C^{\overline{M}_{ji}(y)} C^M_{Kl}(y)dx.$

When we write (1) and (2) in terms of characters we get

(1) $\chi_M * \chi_{M'} = 0$ if $M \neq M'$

(2) $\chi_M * \chi_M = \dfrac{l}{r_M}\chi_M$

58 Obviously we have

$$(r_M\chi_M) * C^M_{ij} = C^M_{ij} * \chi_M r_M = C^M_{ij}$$

Let $L_M(K)$ be the vector space generated by the coefficients $C^{\overline{M}}_{ij}$, where $\overline{M}$ is the complex conjugate representation of M. If f is in $L^2(G)$, then by Peter-Weyl's theorem, $f = \sum_{i,j,N} \lambda_{ijN} C^N_{ij}$.Further if $r_m \chi_{\bar{M}} * f = f$, then we have $f = \sum_{i,j} \lambda_{ijM} C^{\bar{M}}_{ij}$, which means that f belong to $L_M(K)$. Conversely if f belongs to $L_M(K)$, then $f = \sum_{i,j} \lambda_{ij\bar{M}} C^{\bar{M}}_{ij}$. Therefore $r_M \chi_{\bar{M}} * f = f$.Hence $f \in L^2(G)$ is in $L_M(K)$ if and only if $r_M \chi_{\bar{M}} * f = f$.

In this paragraph we give another interpretation of the space $L_M(K)$.

Definition. Let M be an irreducible unitary representation of K and U any representation of K in a Banach space H.

We say that an element a $\in H$ is transformed by U following M, if a is contained in a finite dimensional invariant subspace F of H such that the restriction of U to F is direct sum representations of the equivalence class of M.

Let $H^U_M = H_M = \{a \mid \in H$, a transformed by U following $M\}$. It is **59**
easy to verify that H_M is a vector space.

Proposition 1. *$L_M(K)$ is exactly the subspace of $L^2(K)$ formed by the elements which are transformed following M (respectively following $\overline{M}$) by the left (respectively right) regular representation of K.*

Proposition 2. *If U is a representation of K in H, then $E_M = U_{r_M \bar{\chi}_M}$ is a continuous projection from $H \to H_M$.*

In order to prove the proposition 1 and 2 prove the following results.

(1) Suppose that φ belongs to $L_M(K)$, then $\varphi = \sum_{i,j} \lambda_{ij} C^{\overline{M}}_{i,j}$. For

$$x \in K, \text{we have} \left(\overset{\sigma}{x} C^{\overline{M}}_{ij}\right)(y) = C^{\overline{M}}_{ij}(x^{-1}y) = \sum_k C^{\overline{M}}_{ij}(x^{-1}) C^{\overline{M}}_{ij}(y)$$
$$= \sum_k (C^M_{ki}(x)) C^{\overline{M}}_{kj}(y).$$

So the space E_j generated by $C_{ij}, \cdots, C_{rj} (r_M = r)$ is invariant by σ and the restriction of σ to E_j is of class M. Therefore $L_M(K)$, which is direct sum of the E_j, is contained in $\overset{\sigma}{(L^2(G))}_M$.

(2) If φ belongs to $L_M(K)$ and a belongs to H, then we show that $U_\varphi a$ belong to H_M.

We have

$$U_x U_\varphi a = U_{\epsilon_x * \varphi^a p} = U_{\underset{x}{\sigma} \circ \varphi^a}$$

where ε_x is the Dirac measure at the point x, and

$$U_{\varepsilon_x} b = \int_K U_y b \, d\varepsilon_x(y) = U_x b.$$

60 This shows that $\varphi \in L_M(K) \to U_\varphi$ a $\in H$ is a morphism of representation σ and U. Hence $U_\varphi a$ is transformed by U following M.

(3) If a belongs to H_M, then $E_M a = a$. Since a belongs to some finite dimensional invariant subspace F of H and the restriction of U to F is the direct sum of representation of class M, we can find a basis (e_{jk}) of F such that $U_x e_{jk} = \sum\limits_K C^M_{ij}(x) e_{ik}$

Let a $= \sum\limits_{i,j} \lambda_{ij} e_{ij}$. Then

$$\begin{aligned} E_M(a) &= r_M \int \sum_{i,j,k} \lambda_{jk} C^M_{jk}(x) e_{ik} \overline{\chi}_M(x) dx \\ &= r_m \sum_{i,k} \Big(\sum_j \lambda_{jk} \int C^M_{ij}(x) \overline{\chi}_M(x) dx \Big) e_{ik} \\ &= \sum_{i,k} \lambda_{ik} e_{ik} = a. \end{aligned}$$

Moreover

$\int r_M C^M_{ij}(x) \chi_M(x^{-1}) dx = r_M \chi_M * C^M_{ij}(e) = \delta_{ij}$

(4) In particular if φ belongs to $L^2(G)$ it is transformed by σ following M, then

$$\sigma_{r_M \chi_M} \varphi = r_M \overline{\chi}_M * \varphi = \varphi$$

Therefore φ belongs to $L_M(K)$.

Clearly the results (1)and (4) imply proposition 1.

$$\text{Since} \qquad E_M \dot{E}_M = U_{r_M \chi_M} U_{r_M \chi_M} U_{r_M^2 \chi_M * \chi_M}$$
$$= U_{r_M \chi_M} = E_M,$$

the proposition (2) is proved by result (3)

Similarly we prove that $E_M \cdot E_{M'} = 0$ for $M \neq M'$. Thus we get a family of projections E_M with $E_M(H) = H_M$. The sum $\sum H_M$ is direct and is dense in H. It is sufficient to prove that if a' is a continuous linear form on H, which is zero on every H_M, then $\langle a, a' \rangle = o$ for every $a \in H$. Let us put $\varphi(x) = \langle U_x a, a' \rangle$. Then 61

$$\langle \varphi, C_{ij}^M \rangle = \int C_{ij}^{\overline{M}}(y) \langle U_y a, a' \rangle dy.$$
$$= \langle U_g a, a' \rangle \text{ with } g = C_{ij}^{\overline{M}}$$

But $U_g a'$ belongs to $H_{\bar{M}}$, therefore we get that φ is orthogonal to all the coefficients C_{ij}^M for any M, so $\varphi = 0$.

In particular if U is unitary (for instance the regular representation in $L^2(K)$), then the E_M are orthogonal projections and H is exactly Hilbertian sum of the closed subspaces H_M.

Let G be a locally compact group, K a compact subgroup of G. Suppose that U is a continuous representation of G in H and M an equivalence class of unitary representation of K. By $H_M^U = H_M$ we shall mean the vector subspace of H consisting of elements which are transformed by the restriction of U to K following M. As in the above case $E_M = U_{r_M \overline{\chi}_M}$ is a projection of H to H_M. Let

$$L_M(G) = \left\{ f \mid f \in L(G), f * r_M \overline{\chi}_M = r_M \overline{\chi}_M * f = f \right\}$$

It is easy to prove that $L_M(G)$ is a subalgebra of $L(G)$ and the mapping $f \to r_M \overline{\chi}_M * \dot{*} r_H \overline{\chi}_M$ is a projection from $L(G)$ to $L_M(G)$.

If f belongs to $L_M(G)$ and a belongs to H, then is in H_M. If b 62 belongs to H'_M, then $U_f(a) = U_{r_M}(a)_{\chi_M * f} = E_M\, U_f a \Rightarrow U_f a$ is in H_M. If b belongs to $H_{M'}$, then

$$U_f b = U_{f * r_M \overline{\chi}_M} \quad E_{M'} b = U_f E_M E_{M'} b = 0$$

This shows that U is a representation of $L_M(G)$ in H_M and $U_f = E_M U_f E_M$. Moreover for $f \in L_M(G)$

$$f(y) = r_M \int\limits_K f(k^{-1}y)\overline{\chi}_M(k)dk.$$

In particular if M is the identity representation, then χ_M is constant and f is in $L_M(G)$ if and only if

$$f(y) = r_M \int\limits_K f(ky)dk = r_M \int\limits_K f(yk)dk$$
$$\Longleftrightarrow f(hyk) = f(fyk) = f(y).$$

Such functions are called spherical function on G with respect to K. They can be considered as functions on G/K which are left invariant, provided we write $G/K = \{K, aK, - - -\}$

2 Irreducible Representations

In this section we study how we can get some information about the representation of a group G by studying the representation of the algebra $L_M(G)$.

Definition 1. A representation U of a group G in a vector space V is said to be *algebraically irreducible* if there exists no proper invariant subspace of V.

63 **Definition 2.** A representation U of a topological group G in a locally convex space E said to be *topologically irreducible* if there exists no proper closed invariant subspaces of E.

Definition 3. A representation U of a topological group G in a Banach space H is said to be completely irreducible if $U(L(G))$ is dense in $Hom(H, H)$ in the topological of simple convergence i.e., given an operator T on H and element $a_1, a_2, \cdots, a_p$ in H, there exists for every $\in > 0$ an element f in $L(G)$ such that

$$\| (U_f - T)a_i \| < \in \qquad \text{for } i = 1, 2, \cdots, p.$$

It is obvious that (1) $\Rightarrow$ (2). To prove that (3) $\Rightarrow$ (2), suppose that F is a proper closed invariant subspace of H. Let $a \neq 0$ be any element of F, then for every b in H there exists a $T \in \mathrm{Hom}(H, H)$ such that $T(a) = b$. But by definition for every $\varepsilon > 0$ there exists an element f in $L(G)$ such that $\| U_f a - T(a) \| < \varepsilon$. This means that F is dense in H which is a contradiction because F was assumed to be a closed proper subspace of H.

The definitions (2) and (3) are equivalent for unitary representation by Von Neumann and all the three representation are equivalent for finite dimension representations. The proof can be found in [9]. The definition (1) implies (3) (for proof see annals of Mathematics, 1954 Godement).

Lemma 1. If U is a completely irreducible representation of G in a Banach space H, then the representation U^M of $L_M(G)$ is $H(M)$ is also completely irreducible.

Proof. Suppose that T belongs to $\mathrm{Hom}(H(M), H(M))$. Extend T to H by setting $\tilde{T} = T$ on $H(M)$ and O on $E_M^{-1}(0)$. Obviously T is continuous on H. ◻

Since U is completely irreducible, $\tilde{T}$ can be approximated by U_f for f in $L(G)$ i.e., $\tilde{T} = \lim U_{f_i}$. Therefore 64

$$\begin{aligned} E_M \tilde{T} E_M &= \lim E_M U_{f_i} E_M \\ &= \lim U_{r_M \overline{\chi}_M * f_i * r_M \overline{\chi}_M} \end{aligned}$$

Hence in H_M, $T = \lim U_{r_M \overline{\chi}_M * f_i * r_M \overline{\chi}_M}$

where $r_M \overline{\chi}_M * f_i * r_M \chi_M$ is in $L_M(G)$. Thus U^M is completely irreducible.

Let U be a unitary irreducible representation of G in a Hilbert space H. *By coefficient of* U we means positive definite function $\langle U_x a, a\rangle$ on G. We state without proof the following theorem about the coefficients of unitary representations.

Theorem 1. *If two irreducible unitary representations have same non-zero coefficient associated to them, they are equivalent.*

We have seen that the representation U can be extended to the space $M(G)$ and the operator $U_{\mu*\tilde{\mu}}$ for any μ in $M(G)$ is Hermitian. In particular if we take $\mu = r_M \overline{\chi}_M dk$, we have $\mu = \tilde{\mu}$. There fore $U_{\mu*\mu} = E_M$ is Hermitian.

Moreover for any f in $L(G)$ and a in H_M

$$\begin{aligned}\langle U_f a, a\rangle &= \langle U_f E_M a, E_M a\rangle = \langle E_M U_f E_M a, a\rangle \\ &= \langle U_{f_0} a, a\rangle\end{aligned}$$

65 where $f_0 = r_M \overline{\chi}_M * f * r_M \overline{\chi}_M$ belongs to $L_M(G)$. Thus if we know nonzero coefficient associated to U^M, we know coefficient associated to U as a representation of $L(G)$, which determines coefficient of U as a representation of G. Thus a unitary irreducible representation of G is completely characterised by its restriction U^M to $L_G(G)$ if U^M is not zero.

Definition. A set Ω of representations of an algebra A in a vector space is said to be complete if for every nonzero f in A there exists $U \in \Omega$ such that $Uf \neq O$.

Proposition 3. *If there exists a complete set Ω of representations of an algebra A which are of dimension $\leq K$ (K a fixed integer), then every completely irreducible representation of A in a Banach space is of dimension $\leq k$.*

We first prove a lemma due to Kaplansky. Let A be any algebra. For $x_1, \cdots, x_p$ in A we define $[x_1, \cdots, x_p] = \sum_{\sigma \in S_p} \varepsilon_\sigma x_{\sigma_1} \ldots x_{\sigma_p}$ where S_p is the set of all permutations σ on $1, 2, \cdots, p$ and ε_σ is the signature of σ. Obviously if dim $A < p$, then $[x_1, \cdots, x_p] = o$ for all $x_1, x_2, \cdots, x_p$ in A.

In particular we take $A = M_n(C)$, algebra of $n \times n$ matrix with coefficient from C, the field of complex numbers, We define

$$r(n) = \inf(p) \text{such that}$$
$$[X_1, \cdots, X_p] = 0, X_i \in M_n(C).$$

Clearly $r(n) \leq n^2 + 1$. We shall prove that $r(n+1) \geq r(n) + 2$.

We have $r(n) - 1$ elements $X_1, X_2, \cdots X_{r-1}$ in $M_n(C)(r = r(n))$ such **66**
that $[X_1, \cdots, X_{r-1}] \neq 0$, Let E_{kh} be the canonical basis of $M_n(C)$. Then

$$[X_1, \cdots, X_{r-1}] = \sum_{k,h=1}^{n} \lambda_{kh} E_{kh}.$$

Since $[X_1, \cdots, X_{r-1}] \neq 0$, there exists k_0 and h_0 such that $\lambda_{k_0 h_0} \neq 0$. Let $\tilde{X}_i$ be the matrix obtained by adding a row and a column of zeros to X_i. Then

$$\begin{aligned}\left[\tilde{X}_1, \cdots, \tilde{X}_{r-1} E_{h_0,n+1} E_{n+1,n+1}\right] &= \left[\tilde{X}_1, \cdots, \tilde{X}_{r-1}\right] E_{h_0,n+1} E_{n+1n+1} \\ &= \sum_{h,k} \lambda_{kh} \tilde{E}_{kh} E_{h_0} n + 1 \\ &= \sum \lambda_{kh_0} E_{k,n+1} \neq 0.\end{aligned}$$

Thus $r(n+1) \geq r(n) + 2$.

Now we prove the proposition. Suppose that $r(k) = r$ and U is a complete irreducible representation of dim $> K$ in a Banach space H. Let F be a subspace of H of dim $k+1$. Since $r(k+1) > r(k)$, there exist operators $[A_1, \ldots, A_r]$ in $\mathrm{Hom}(F, F)$ such that $[A_1, \ldots, A_r] \neq 0$. We extend each A_i to the whole space H by defining A_i to be zero on F', where F' is any closed subspace such that H is the topological direct sum of F and F'. Suppose that $A_1 = \lim U_{f_{i_1}}$, where $f_{i_1} \in A$. We have

$$0 \neq [\tilde{A}_1, \cdots, \tilde{A}_r] = \sum_{\sigma \in \mathcal{S}_r} \tilde{A}_{\sigma_1}, \ldots \tilde{A}_{\sigma_r} = \lim[U_{f_i} \tilde{A}_2, \cdots, \tilde{A}_r].$$

Therefore there exists f_1 in A such that $[U_{f_1} \tilde{A}_2, \cdots, \tilde{A}_r] \neq 0$. Repeating **67**
this process we obtain that there exist elements $f_1, \cdots, f_r$ in A such that

$U_{[f_1,\cdots,f_r]} = [U_{f_1},\cdots,U_{f_r}] \neq 0$. But this is a contradiction because $[f_1,\cdots,f_r] = 0$ if $[f_1,\cdots,f_r] \neq 0$, then there exists a V in Ω such that $V_{[f_1,\cdots,f_r]}(a) \neq 0 \Rightarrow$

$[V_{f_1},\cdots,V_{f_r}](a) \neq 0$. But $r \geq r_k$ and $dimV \leq k$, therefore $[V_{f_1},\cdots, V_{f_r}] = 0$. Hence $\dim U < k$.

Corollary. *Let G be a locally compact group, K a compact subgroup, M a class of irreducible unitary representations of K in a Banach space H. If there exists a system Ω of representations of G in a Banach space such that (i) for every U in Ω, the representation U^M of $L_M(G)$ is of* $\dim \leq p \dim M$. *Equivalently M occurs atmost p times in each U.*

(ii) The representations U^M for U in Ω form a complete system of representation of algebra $L_M(G)$.

Then M occurs atmost p times in any completely irreducible representation of G.

3 Measures on Homogeneous spaces

Let G be a locally compact group, dx the right invariant Haar measure and $\Delta(x)$ the modular function on G i.e., $d(yx) = \Delta(y)dx$. Let Γ be a closed subgroup of G. We shall denote by $\xi,\eta\ldots$ the elements of Γ by $d\xi$ and δ the Haar measure and the modular function on Γ. It is well
68 known that there exists a right invariant Haar measure on G/Γ if and only if $\Delta(\xi) = \delta(\xi)$. In general it is possible to find a quasi-invariant measure on G/Γ. In order to show the existence, one shows that there exists a strictly positive continuous function ρ on G such that $\rho(\xi x) = \dfrac{\delta(\xi)}{\Delta(\xi)}\rho(x)$ for every x in G and ξ in Γ. Then the measure $\rho(x)dx$ gives rise to a measure $d\mu(x)$ on G/Γ such that for any f in $L(G)$ we have

$$\int\limits_G f(x)\rho(x)dx = \int\limits_{G/\Gamma} d\mu(x)\int\limits_{\Gamma} f(\xi x)d\xi \tag{1}$$

It is obvious from (1)that

$$d\mu(\overline{(xy)}) = \frac{\rho(xy)}{\rho(x)}d\mu(x)$$

where $\dfrac{\rho(xy)}{\rho(x)}$ depends only on the cosets of x modulo Γ. Thus $\mu(x)$ is a quasi-invariant measure on G/Γ. The details could be found in [9].

4 Induced Representations

Let L be a representation of Γ in Hilbert space H. We shall define two types of induced representation on G given by L.

(1) Assume that L is unitary. Let H^L be the spaces of functions f on G such that

   (1) f is measurable with values in H.

   (2) $f(\xi x) = [p(\xi)]^{1/2} L_\xi f(x)$, for $\xi \in \Gamma$.

   (3) $\int\limits_{G/\Gamma} (\rho(x))^{-1} \parallel f(x) \parallel^2 dx < \infty$.

Since the function $(\rho(x))^{-1} \parallel f(x) \parallel^2$ is invariant on the left by Γ, it can be considered as a function on G/Γ. Thus we define

$$\parallel f \parallel^2 = \int\limits_{G/\Gamma} (\rho(x))^{-1} \parallel f(x) \parallel^2 d\mu(x)$$

It can be proved that H^L is a Hilbert space with the scalar product **69**

$$\langle f, g >, = \int\limits_{G/\Gamma} (\rho(x))^{-1} \langle f(x), g(x) \rangle d\mu(x).$$

Let U^L be the map from G to H^L such that

$$U^L_x f(y) = f(xy)$$

Obviously U^L is continuous. Since we have

$$\parallel U^L_y f \parallel^2 = \int\limits_{G/\Gamma} (\rho(x))^{-1} \parallel f(xy) \parallel^2 d\mu(x)$$

$$= \int\limits_{G/\Gamma} (\rho(xy^{-1}))^{-1} \parallel f(x) \parallel^2 \frac{\rho(xy^{-1})}{\rho(x)} d\mu(x)$$
$$= \parallel f \parallel^2$$

It follows that U^L is unitary. We say that U^L is the unitary representation induced by L.

(ii) Let L be any representation of Γ. Let us suppose that there exists a compact subgroup K of G such that $G = \Gamma K$. Let C^L be the space of functions f such that

(1) f is continuous with values in H.

(2) $f(\xi x) = (\rho(\xi))^{\frac{1}{2}} L_\xi(f(x))$ for $\xi \in \Gamma$.

We define $\parallel f \parallel = \sup\limits_{x \in K} \parallel f(x) \parallel$. Clearly C^L with this norm is a Banach space. Again right translation by elements of G give rise to a representation of G in G^L. We denote this also by U^L.

Let $f \to$ restriction of f to $K = f_0$ be the map from the C^L to $C(K)$ (the set of continuous functions on K with values in H). The image of
70 C^L by this map is the set of elements $f_0 \in C(K)$ which satisfy condition (2) above for all ξ in $\Gamma \cap K$ and x is K. But $\rho(\xi) = 1$, because ρ is a positive real character of $K \cap \Gamma$, therefore $f_0(\xi x) = f_0(x)$. Through the space C^L is identified with a subspace of $C(K)$ yet the representation U^L cannot be defined on this subspace. However the restriction of U^L to K and the representation induced by the restriction of L to $\Gamma \cap K$ are identical.

If L is unitary then f belongs to H^L if and only if f_0 belongs to $L^2(K)$. We can choose ρ in such a way that $\rho(xk) = \rho(x)$ for $k \in K$. Since the group $K/K \cap \Gamma$ is compact homogeneous space, there exits one and only one invariant Haar measure on it. But $K/K \cap \Gamma$ is isomorphic to G/Γ therefore with the above choice of ρ, the quasiinvariant measure on G/Γ gives rise to the invariant measure on $K/K \cap \Gamma$. We have

$$\int\limits_{G/\Gamma} (\rho(x))^{-1} \parallel f(x) \parallel^2 d\mu(x) = \int\limits_{K/K \cap \Gamma} \parallel f(k) \parallel^2 d\mu(k)$$

$$= \int\limits_K \| f(k) \|^2 \, dk \qquad \text{(A)}$$

Our result is obvious from (A).

5 Semi Simple Lie Groups

Let G be a semi simple Lie group worth a faithful representation. We state here two theorems the proof of which could be found in [19].

Theorem 2. *The group G has a maximal compact subgroup and all the maximal compact subgroup are conjugates.*

Theorem 3. *Suppose that K is maximal compact subgroup of G, then there exists a connected solvable T of G such that $G = TK$.*

We shall prove the following theorem about completely irreducible representation of G. **71**

Theorem 4. *Every irreducible representation M of K is contained atmost* dim (M) *times in every completely irreducible representation of G.*

Proof. (1) The finite dimensional irreducible representations of G is a vector H is a complete system of representations of $L(G)$. Let $x \to \rho_x$ be a representation of G in a vector space H. We call the function $\theta(x) = \langle \rho_x a, a' \rangle$ where a belongs to H and a' belongs to H^* (the conjugate space of H), a coefficient of the representation. Let V denote the vector space generated by all coefficients of all finite dimensional irreducible representations of G. Since every finite dimensional representation of G is completely reducible, V contains all the coefficients of all finite dimensional representations of G. Let ρ^1 and ρ^2 be two finite dimensional irreducible representations of G. Then we have

$$\langle \rho^1_x a_1, a'_1 \rangle \langle \rho^2_x a_2, a'_2 \rangle = \langle \rho^1_x \otimes \rho^2_x \; a_1 \otimes a_2, a'_1 \otimes a'_2 \rangle$$

showing that V is an algebra. Moreover V is a self adjoint algebra, because if $\theta(x) = \langle \rho a, a' \rangle$ is in V, then $\overline{\theta}(x) = \langle \overline{\rho}_x \overline{a}, \overline{a'} \rangle$ is also in V. Since G

has a finite dimensional faithful representation, V separates points i.e., if $\theta(x) = \theta(x')$ for every θ in V, then $x = x'$. Thus Stone- Weierstrass' approximation theorem every continuous function on G can be approximated uniformly on every compact subset by elements of V. Hence if f is a non-zero elements of $L(G)$, then $\int f(x)g(x)dx = 0$ for every element
72 g of $C(G)$ (the set of all continuous functions on G), because

$$\rho_f = \int \rho_x f(x)dx \text{ and } \int < \rho_x a, a' > f(x)dx = 0$$

for every a in H and a' in H^* and ρ. Therefore f must be =0

(2) The representations of G induced by all characters of T form a complete system for $L(G)$

Let ρ be a finite dimensional irreducible representation of G and let $\overset{v}{\rho} = (\overset{t}{\rho})^{-1})$ be the representation contragradient to ρ. By Lie's theorem [19],the restriction of $\overset{v}{\rho}$ to T has an invariant subspace of dimension 1, which implies that there exists a vector $b' \neq 0$ in E^*(the conjugate space of the representation space E of, ρ) such that $\overset{v}{\rho}(t) = b' = \chi(t)b'$ for every $t \in T$. Consider the mapping a $\in E \to \widetilde{a} \varepsilon c^{\chi-1}$, where $\widetilde{a}(x) =< \rho_x a, b' >$. Since

$$\widetilde{a}(tx) =< \rho_{tx} a, b' >=< \rho_x a, \rho_t^{r-1} b' >= \chi^{-1}(t) < \rho_x a, b' >= \chi^{-1}(t)\widetilde{a}(x),$$

$\widetilde{a}(x)$ is covariant by left translation. Obviously the map $a \to \widetilde{a}$ is continuous. Let $U^{\chi-1}$ be the representation of G induced by χ^{-1}. The mapping $a \to \widetilde{a}$ is a morphism of representations ρ and $U^{\chi-1}$, because

$$\widetilde{\rho_y}\, a(x) = \langle \rho_x\, \rho_y a, b' \rangle = \widetilde{a}(xy) = U_y^{\chi-1}(\widetilde{a}).$$

The mapping $a \to \tilde{a}$ is not zero. If $a \neq 0$, then $(\rho_x a)$ generates the whole space E because ρ is irreducible, therefore for atleast on x in $G\langle \rho_x a, b' \rangle \neq 0 \Rightarrow \widetilde{a} \neq 0$. Let f be a non-zero element of $L(G)$. If $U_f^{\chi-1} = 0$. For every χ then $\rho_f = 0$ for every ρ which means the $f = 0$ by (1). This is a contradiction, hence our result is proved.

73 (3) We shall show that if χ is a character of T, then M occurs atmost dim (M) times in U^χ. Clearly U^χ/K(restriction of $U^\chi to K$) $=$

$U^{\chi/K\cap T}$.But the space of this representation is the space of continuous functions f on K such that

$$f(tk) = \chi(t)f(k) \text{ for } t \in K \cap T.$$

Therefore $U^{\chi/K\cap T}$ is a subrepresentation of the right regular representation of K. Hence $(C^{\chi})_M \subset L_M(K)$ which is a space of $(dimM)^2$. Thus M occurs at most dim(M) times in U. Our theorem follows from (2), (3) and proposition 1.3. $\square$

Chapter 4

Classical Linear Groups over p-adic Fields

1 General Definitions

We shall study the following types of classical linear groups over field P or over a division algebra. 74

(I) (a) $\underline{GL_n(P)}$- The group of all non-singular n x n matrices with coefficients from P is called the general linear group

(b) $\underline{PrGL_n(P)}$ Let $CL_n(P)$ be the centre of the group $GL_N(P)$. The group pr $GL_n(P) = GL_n(P)/CL_n(P)$ is called the projective linear group.

(c) $SL_n(P)$-The subgroup of $GL_n(P)$ consisting of all the matrices of determinant 1 is called the special linear group or the unimodular group. It can be proved that $\mathrm{Pr}SL_n(P) = SL_n(P)/C(SL_n(P))$ is a simple group

(II) -Let $E = P^n$ and φ a non-degenerate bilinear form over E

(a) $\underline{Sp_n(P)}$-If φ is an alternating form,then the the set of all matrices in $GL_n(P)$ which leave this bilinear form invariant is a group called the linear symplectic group. We shall denote the by $Sp_n(P)$. This group is independent of the choice of the alternating bilinear form because any two such bilinear forms are equivalent.

(b) If φ is a symmetric non-degenerate bilinear form, then the set of elements in $GL_n(P)$ leaving φ invariant is group called the linear orthogonal group.

(III) Let $\widetilde{P}$ be a separable quadratic extension of P. Let $\xi \to \bar{\xi}$ be the unique nontrivial automorphism of $\widetilde{P}$. If φ is a non-degenerate
75 Hermitian bilinear form over E i.e., $\varphi(y, x) = \varphi\overline{(x, y)}$, then the set $U_n(\varphi, P)$ of elements of $GL_n(P)$ leaving φ invariant is a group called the unitary group.

(IV) Let $\widetilde{P}$ be a division algebra of finite rank over P, such that P is the centre of $\widetilde{P}$. We define $GL_n(P)$ as in I (a). The group $SL_n(P)$ can be defined as the kernel of the map σ(determinant of Dieudonne) from $GL_n(P)$ to $\widetilde{P}^*/C$ where C is the commutator subgroup of P^*.

(V) Let $\widetilde{P}$ be the algebra of quaternions over P. In this case there exists an involution in $\widetilde{P}$ i.e., an anti automorphism of $\widetilde{P}$ of order 2. So we can define as in (3) the group $U_n(\varphi, P)$ which leaves invariant the bilinear form φ over $\widetilde{P}^n$. As in (1) one can define $S0_n(\varphi, P)$ and $SV_n(\varphi, P)$ and prove that their projective groups are in general simple.

Suppose that P is a locally compact p-adic field. All the groups of type (1), (2) and (3) are locally compact, because on $M_n(P)$ (the set of all $n\chi n$ matrices with coefficients from P) we have the topology of P^{n^2} and $GL_n(P)$ is an open subset of $M_n(P)$ and the groups $SL_n(P)$ etc.are closed subgroups of $GL_n(P)$.

Let us assume that the rank of $\widetilde{P}$ over P in (4) is r. Then $M_n(\widetilde{P})$ may be imbedded in $M_{nr}(P)$, as $\widetilde{P}^n$ can be considered as a space of dimension nr over P, since a matrix is inversible in $M_n(\widetilde{P})$ if and only if it is invertible in $M_{nr}(P)$, we have

$$GL_n(\widetilde{P}) = GL_{nr}(P) \cap M_n(\widetilde{P})$$

But $GL_{nr}(P)$ is an open subset of $M_{nr}(P)$, therefore $GL_n(\widetilde{P})$ is an
76 open subset of $M_n(\widetilde{P})$. Since $M_n(\widetilde{P})$ is locally compact, because it has

the same topology as the $\widetilde{P}^{n^2}, GL_n(\widetilde{P})$ is locally compact. $U_n(\varphi, \widetilde{P})$ is locally compact, because it is a closed subgroup of $GL_n(\widetilde{P})$.

2 Study of $GL_n(\widetilde{P})$

By $\widetilde{P}$ we shall mean a division algebra of finite rank over P, which is a locally compact valuated field, contained in the centre of $\widetilde{P}$. Let $\tilde{\mathscr{O}}$ denote the ring of integers of $\widetilde{P}$

As we have already seen that $\tilde{\mathscr{O}}$ is a compact subset of $\widetilde{P}$, therefore $M_n(\tilde{\mathscr{O}})$ which is homeomorphic to $\mathscr{O}^{n2}$ is compact in $M_n(\tilde{\widetilde{P}})$. Let $GL_n(\tilde{\mathscr{O}})$ be the set of elements $M_n(\tilde{\mathscr{O}})$ which are invertible in $M_n(\tilde{\mathscr{O}})$. Obviously$GL_n(\widetilde{P})$ contains $GL_n(\tilde{\mathscr{O}})$. Therefore

$$GL_n(\tilde{\mathscr{O}}) = GL_n(\widetilde{P}) \cap M_n(\tilde{\mathscr{O}}) \cap [GL_n(\widetilde{P}) \cap M_n(\tilde{\mathscr{O}})]^{-1}$$

Since $\tilde{\mathscr{O}}$ is open in $\widetilde{P}, M_n(\tilde{\mathscr{O}})$ is open in $M_N(\tilde{P})$. Therefore $GL_n(\tilde{\mathscr{O}})$ is open in $M_n(\tilde{\mathscr{O}})$. Similarly $GL_n(\tilde{\mathscr{O}})$ is open in $GL_n(\widetilde{P})$. Moreover $GL_n(\tilde{\mathscr{O}})$ is closed in $M_n(\tilde{\mathscr{O}})$. For, let (X_p) be a sequence of elements in $GL_n(\tilde{\mathscr{O}})$ such that X_p tends to $X \in M_n(\tilde{\mathscr{O}})$ as p tends to infinity. Because $M_n(\tilde{\mathscr{O}})$ is compact, we can assume that X_p^{-1} has a limit Z in $M_n(\tilde{\mathscr{O}})$. But then $ZX = XZ = I$, therefore X belongs to $GL_n(\tilde{\mathscr{O}})$. Hence $GL_n(\tilde{\mathscr{O}})$ is compact.

We define in the following some subgroups of $GL_n(\widetilde{P})$, which will be of use later on.

(i)

$$\Gamma = \left\{ \gamma = \begin{pmatrix} a_1 & & * \\ & \ddots & \\ 0 & & a_n \end{pmatrix} | \gamma \in GL_n(\widetilde{P}) \right\}$$

where(*) indicates that there may be some non-zero entries.

(ii)

$$T = \left\{ t = \begin{pmatrix} \widetilde{\pi}^{\alpha} & & * \\ & \ddots & \\ 0 & & \widetilde{\pi}^{\alpha} \end{pmatrix} | t \in GL_n(\widetilde{P}), \alpha_i \in Z \right\}$$

$\widetilde{\pi}$ being a uniformising parameter in $\tilde{P}$ 77

(iii)

$$N = \left\{ \underline{n} = \begin{pmatrix} 1 & & * \\ & \ddots & \\ 1 & & 1 \end{pmatrix} \right\}$$

(iv)

$$D = \left\{ \underline{d} = \begin{pmatrix} a_{11} & & 0 \\ & \ddots & \\ 0 & & a_{1n} \end{pmatrix} \middle| a_{ij} \in \widetilde{P}, a_{ij} \neq 0 \right\}$$

(v)

$$\Delta = \left\{ \begin{pmatrix} \widetilde{\pi}^{\alpha_1} & & 0 \\ & \ddots & \\ 0 & & \widetilde{\pi}^{\alpha_n} \end{pmatrix} \middle| \alpha_i \in Z \right\}$$

We see immediately that $T = \Delta N$ and $\Gamma = DN$. Moreover T is a solvable group, Γ is solvable if $\widetilde{P}$ is commutative and T (respectively Γ) is a semi direct product of Δ and N(respectively D and N).

Proposition 1. *$GL_n(\tilde{P}) = G = TK$, where $K = GL_n(\tilde{\mathscr{O}})$.*

Proof. When $n = 1$, the proposition is trivially true. Suppose that it is true for all $GL_s(\widetilde{P})$ for $s \leq n-1$. We shall prove it for $GL_n(\widetilde{P})$. Let $g = (g_{ij})$ be an element of G. We can find integers $(k_{j1})_{1 \leq j \leq n}$ such that

$$\sum_{j=1}^{n} g_{ij} k_{j1} = 0 \text{ for } 2 \leq i \leq n$$
$$= a_{11} \neq 0 \text{ for } i = 1.$$

78 By multiplying on the right with a suitable element of $\widetilde{P}$ we can take atleast one of k_{j1} to be 1. Let $k = (\gamma_{ij})$ be a matrix, where $\gamma_{i1} = k_{i1}$ for $i = 1, 2, \ldots, n$ with $k_{ji} = 1, \gamma_{jr} = 0$ for $r = 2, \ldots, n$ and the other γ_{ij} are so determined that k belongs to K.

So we get

$$g_k = \begin{pmatrix} a_{11} & * \\ 0 & * \end{pmatrix} = \begin{pmatrix} \widetilde{\pi} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & * \\ 0 & g' \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix}$$

where g' is $n-1 \times n-1$ matrix and $a_{11} = \tilde{\pi}^{\alpha} y, y \in \mathscr{O}^*$. $\square$

But by induction hypothesis $g' = t'k'$ where t' belongs to T' and $k' \in K'$ the subgroups T' and K' defined in $GL_{n-1}(\widetilde{P})$ in the same way as T and K in G Thus we get

$$\begin{pmatrix} 1 & * \\ 0 & g' \end{pmatrix} = \begin{pmatrix} 1 & *k'^{-1} \\ 0 & t' \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & k' \end{pmatrix}$$

This implies that

$$\begin{aligned} gk &= \begin{pmatrix} \widetilde{\pi}^{\alpha} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & *k'^{-1} \\ 0 & t' \end{pmatrix} \begin{pmatrix} 1 & o \\ 0 & k' \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} \\ &= t_1 k_1, t_1 \in T \text{ and } k_1 \in K. \end{aligned}$$

Hence our result follows:

We shall now prove an analogue of Elementary divisors theorem. Let A be a ring with unity (but without any other condition). Let us consider the following assertions(where module signifies left module):

(I a) any finitely generated module is isomorphic to a direct sum $\bigoplus_{i=1}^{i=r} A/\underline{a}_i$, where $\underline{a}_i$ are left ideals with $A \neq a_1 \supset \cdots \supset \underline{a}_r$ **79**

(I b) Such a decomposition, if it exists, is unique.

(II a) if M is a free module of finite type and N a finitely generated submodule of M, there exists a basis $e_1, \ldots, e_r$ and r elements $\alpha_1, \ldots, \alpha_r$ of A such that $\alpha_{i+1} \subset A\alpha_i$ and such that N is the direct sum of submodules $A\alpha_i e_i$.

(II b) if such elements e_i and α_i exist, the ideal $A\alpha_i$ are independent of the choice of the e_i and α_i satisfying (II a).

(III a) if g is a $m \times n$ matrix with coefficients in A, there exists two $m \times m$ and mxn invertible matrices p and q such that $d = pgq$ is a $m \times n$ "diagonal" matrix(i.e., $d_{ij} =$ for $i \neq j$) and $\alpha_i = d_{ii} \in A\alpha_{i+1}$.

(III b) if such matrices p and q exist, the ideals $A\alpha_i$ are independent of the choice of p and q (satisfying(III b)).

It is obvious that (III a) implies (IIa): consider a basis $x_1, \ldots, x_n$ of M and a system of generators $y_1, \ldots, y_m$ of N and define the matrix g by $y_j = \sum g_{ij} x_i$. Then $e_i = \sum (q^{-1})_{ik} x_k$ is basis of M and the $\alpha_i e_i = \sum p_{ik} y_k$ generate N. if a is left Noetherian then (IIa) implies (Ia), for any finitely generated module is a quotient M/N, with M free of finite type and N finitely generated. Conversely,it is obvious that (I a) implies (II b) and (II b) implies (III b).

It is well known that all these six assertions are true if A is a commutative principal ideal ring (without zero divisors)(see for instance Bourbaki, Alg., ch VII, §4). We shall now prove the following extension:

80 **Theorem.** *Let A be a ring with unity (but A may be non-commutative and may have zero divisors),which satisfies the following conditions:*

1) *any left or tight ideal is two sided (equivalently, Ax =xA for any $x \in A$*

2) *the set of the principal ideals is totally ordered by inclusion (hence any finitely generated ideal is principal).*

Then, the assertions (IIIa) and (Ia) *are true (hence also* (IIa)*, and* $(IIIb)$*. If moreover A dis Noetherian (that is if any ideal is principal),then* (Ia) *is also true*

Proof of (III a): the result is obviously true form $n = m = 1$. Assume it is proved for $(m-1) \times (n-1)$ matrices. Let us consider the ideals A g_{ij} : $by(2)$ they are all contained in one of them, and we can assume without loss of generality, that $g_{ji} \in Ag_{11}$ for any indices i,j. Let $g_{i1} = c_i g_{11}$ for $2 \leq i \leq m$. By multiplying g on the left by a $m \times m$ matrix k where

$$k = \begin{pmatrix} i & 0 \cdots 0 \\ -c_2 & 1\, 0 \cdots 0 \\ & \cdots \\ -c_m & o \cdots 1 \end{pmatrix}$$

we get a matrix kg with $(kg)_{11} = g_{11}$ and $(kg)_{i1} = 0$ for $i \geq 2$. Moreover, the matrix k is invertible. Similarly, using the fact that $g_{ij} \in g_{11}A$. We find a $n \times n$ inversible matrix h such that

$$kgh = \begin{pmatrix} g_{11} & 0 & \cdots 0 \\ 0 & & \\ & g' & \\ 0 & & \end{pmatrix}$$

Now, we have just to apply the induction hypothesis to g' (remember **81**
that all the coefficients of g, hence of g' belong to Ag_{11}).

Proof. (Ib): more generally, we shall prove that assumption 1) alone implies (Ib). ◻

Let $M = \sum\limits_{i=1}^{n} A/\underline{a_i} = \sum\limits_{j=1}^{m} A/\underline{b_i}$, with $\underline{a_1} \supset \underline{a_2} \supset \cdots \supset \underline{a_n}$ and $\underline{b_1} \supset \underline{b_2} \supset \cdots \supset \underline{b_m}, \underline{a_i} \neq A$ and $\underline{b_i} \neq A$ for any i. Then $m = n$ and $\underline{a_i} = \underline{b_i}$ for $i = 1, 2, \ldots, n$.

Proof. Let x'_i(respectively y'_j) be the canonical generator of $A/\underline{a_i}$ (respectively $A/\underline{b_j}$) and x_i (respectively $\underline{y_j}$) the canonical image of x'_i (respectively y'_j) in M. Then $y_j = \sum\limits_{i=1}^{n} a_{ij} x_i$, where $a_{ij} \in A$ and is determined completely modulo $\underline{a_i}$ and therefore modulo $\underline{a_i}$. Similarly $x_i = \sum\limits_{k=1}^{m} b_{ki} y_k$, where $b_{ki} \in A$ and is completely determined modulo b_1. Let m be a maximal left ideal containing b_1. We see immediately that m is a two sided ideal and $A/\underline{\text{m}}$ is a division algebra. Since $y_j = \sum\limits_{i=1}^{n} a_{ij} = \sum\limits_{i=1}^{n} b_{ki} y_k$, we have

$$\sum_{i=1}^{n} a_{ij} \equiv \delta_{kj} \pmod{\underline{m}}$$

But this is possible only when $n \geq m$, because if V^m and V^n are two vector spaces over a division ring of dimension m and n respectively such that φ and ψ are two linear transformations from V^m to V^n and V^n to V^m respectively. then $\varphi\psi = I$ implies that ψ is an isomorphism of V^m onto a subspace of V^n. In the same way we get that $m \geq n$. Hence $m = n$. ◻

If possible let us suppose that $\underline{a_i} \neq \underline{b_i}$ for some i. Let us suppose that there exists an element a in $\underline{a_i}$ which does not belong to $\underline{b_i}$. Consider the set aM, it is a submodule of M. Therefore 82

$$aM = \sum_{i=1}^{n} aA/aA \cap \underline{a_i} = \sum_{i=1}^{n} aA/a \cap a_i$$

because every left principal ideal in A is a right principal ideal in A. Let $x \in A \rightarrow \overline{xa} \in Aa$ be a map from A to $Aa/aA \cap \underline{a_i}$, its kernel is the set $\{x|xa \in \underline{a_i}\} = B$. Therefore we get that $Aa/aA \cap \underline{a_i}$ is isomorphic to A/B. Moreover $A/B = (0)$ if and only if a belongs to $\underline{a_i}$. Now rank of aM=number of $\underline{a_i}$ such that a does not belong to $\underline{a_i}$. Since a belongs to a_i, a belongs to $\underline{a_j}$ for $j \leq i$, therefore rank of a $M \leq n - i$. On the other hand rank of aM = number of $\underline{b_j}$, such that a does not belong to $\underline{b_j}$. Since a does not belong to $\underline{b_i}$, rank $aM > n - i$. Hence we arrive at a contradiction. Thus $\underline{a_i} = \underline{b_i}$ and our result is proved.

Remark. It can be shown that the six assertions (I a) to (III b) are true if the ring A satisfies the conditions 1) and:

1) any ideal is principal;

2) A has no zero divisors.

The proof works exactly as in the commutative case (see Bourbaki, loc. cit.)

Obviously, the ring $\tilde{\mathscr{O}}$ of the integers of any valuated non - commutative field satisfies 1)and 2).Moreover we have in this case $d_{ii} = (\tilde{\pi})^{\beta_i}$ with $y_i \in \tilde{\mathscr{O}}^*$ and $1 \leq i \leq r$ and $d_{ii} = 0$ for $i > r$. The diagonal $n \times n$ matrix y defined by $y_{ii} = y_i$ for $1 \leq i \leq r$ and $y_i = 1$ for $i > r$ is invert-
83 ible and multiplying d on the right by y^{-1} and q on the left by y, we get a decomposition $g = p'd'q'$ where p' and q' are invertible and d' is a diagonal matrix whose diagonal coefficients $\tilde{\pi}^{\beta_i}$ are positive powers of the uniformising parameter $\widetilde{\pi}$ with $\beta_1 \leq \cdots \leq \beta_r$, and the β_i are completely determined by these conditions (we used the fact that ideal in $\tilde{\mathscr{O}}$ is generated by one and only one power of $\widetilde{\pi}$).

Now, let us return to the group G. For any n-tuple of rational integers, $\alpha = (\alpha_1, \ldots, \alpha_n)$, let d_α be the diagonal $n \times n$ matrix with diagonal coefficients $\tilde{\pi}^{\alpha_i}$ and let Δ^+ be the subset of the subgroup Δ consisting of the matrices d_α with $\alpha_1 \leq \cdots \leq \alpha_n$.

Proposition 2. *In each double coset KgK modulo K, there exists one and only one element of Δ^+.*

Proof. Let $g = (g_{ij})$ be any element of G. Multiply g by a diagonal matrix (a_{ii}), where $a_{ii} = a^k, a \in P, v(a) > 0$ and k is a sufficiently large integer so chosen that the matrix $g' = g(a_{ii})$belongs to K. Then by the above theorem there exist matrices p' and q' in K such that

$$g(a_{ii}) = g' = p' d\beta q' \quad \text{with} \quad d\beta \in \Delta^+$$

Let us take $\alpha_i = \beta_i - kv(a)$. Then we have $g = pd\alpha q$ with q, p in K and d_α in Δ^+. Conversely if g belongs to $Kd_\alpha K$. then g' belongs to $Kd_\beta K$. But d_β is unique, therefore d_α is unique. ◻

Corollary 1. *K is a maximal compact subgroup of G.*

If possible let $H \supset K$ be a compact subgroup of G. Obviously there exists $\alpha \neq 0$ such that $d\alpha$ belongs to H. Then

$$(d\alpha)^r = \begin{pmatrix} \widetilde{\pi}^{\alpha_1 r} & & 0 \\ & \ddots & \\ 0 & & \widetilde{\pi}^{\alpha_n r} \end{pmatrix}$$

If $\alpha_i \neq 0$, then $v(\pi^{r\alpha_i} \to \pm\infty$ as $r \to \pm\infty$, which is a contradiction as **84**
v is a continuous function form $\widetilde{P}$ to R. Hence $H = K$.

Let E be a vector space over $\widetilde{P}$. Let I be a lattice in E i.e., a finitely generated $\tilde{\mathscr{O}}$ module such that its basis generate E. Since I has no torsion, basis of I is a basis of E. In particular if we take $E = \widetilde{P}^n$ and $I = \widetilde{\mathscr{O}}^n$ and if we identify G with the group of endomorphisms of E, then $g \in K$ and only if g(I)=I. Moreover if we take any lattice L, then the subgroup of G which leaves L invariant is a conjugate subgroup of K.

Let H be a compact subgroup of G. Let $e_1, \ldots, e_n$ be a basis of E. Let J be an $\tilde{\mathscr{O}}$-module generated by the elements $h(e_j), 1 \leq j \leq n$ and $h \in H$. Evidently we have

(1) J is invariant by H

(2) $J \supset I$

(3) The map $h \to h(e_j)$ is a continuous map from H to E.

But H is compact, therefore the image of H in E by the map defined in (3) is compact and hence bounded. Therefore there exists an integer k such that $J \subset \widetilde{\pi}^{-k} I$, which shows that J is finitely generated, but $J \supset I$, therefore J is generated by a finite set of element which generate E. Hence J is a lattice. Thus H is contained in a conjugate subgroup of K namely the subgroup of G which leaves J invariant. Hence we have proved the the following.

Corollary 2. *Any two maximal compact subgroups of G are conjugates and any compact subgroup of G is contained in a maximal compact subgroup of G.*

85 **Remark 3.** Any double coset KxK, $x \in G$, is a finite union of left cosets modulo K, because K is open and compact, therefore every double coset and left coset modulo K is open and compact.

We introduce *a* total ordering in Z^n by the lexicographic order i.e., if $\alpha = (\alpha_1, \cdots, \alpha_n)$ and $\beta = (\beta_1, \cdots, \beta_n)$ are two elements of Z^n, then we say that $\beta > \alpha$ if $\beta_i > \alpha_i$, for the least index i for which $\beta_i \neq \alpha_i$.

Proposition 3. *If $Nd_\beta K \cap Kd_\alpha K \neq \phi$, where $\alpha \cdot \beta$ are in Z^n and $d_\alpha \in \Delta^+$ then $\beta \geq \alpha$ and $Nd_\alpha K \cap Kd_\alpha K = d_\alpha K$.*

Proof. Let nd_β belongs to N d_β $K \cap Kd_\alpha K$, where

$$\underline{n} = \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}, d_\beta = \begin{pmatrix} \tilde{\pi}^{\beta_1} & & 0 \\ & \ddots & \\ 0 & & \tilde{\pi}^{\beta_n} \end{pmatrix}$$

Then nd_β belongs to $Kd_\alpha K$. But $\underline{n}d_\beta$ belongs to $Kd_\alpha K$ if and only if the invariant factors of $\underline{n}d_\beta$ are $\overset{\alpha_1}{\tilde{\pi}}, \cdots \overset{\alpha_n}{\tilde{\pi}}$. Therefore we get that $\tilde{\pi}^{\alpha_1}$ divides $\tilde{\pi}^{\beta_i}$ for $i = 1, 2, \cdots, n$. If $\alpha_1 < \beta_1$, our assertion is proved. If $\alpha_1 = \beta_1$, then we multiply the matrix $\underline{n}d_\beta$ on the right by a matrix δ, where

$$\delta = \begin{pmatrix} 1 & -\tilde{\pi}^{\alpha_1} a_{12} & \cdots & -\tilde{\pi}^{\alpha_1} a_{1n} \\ 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

if

$$\underline{n}d_\beta = \begin{pmatrix} \tilde{\pi}^{\alpha_1} & a_{12} & \cdots a_{1n} \\ 0 & \tilde{\pi}^{\beta_2} & \cdots * \\ & \ddots & \\ 0 & 0 & \tilde{\pi}^{\beta_n} \end{pmatrix}$$

So we get 86

$$\underline{n}d_\beta \delta = \begin{pmatrix} \tilde{\pi}^{\alpha_1} & 0 & \cdots 0 \\ 0 & \tilde{\pi}^{\beta_2} & * \\ & \ddots & \\ 0 & 0 & \tilde{\pi}^{\beta_n} \end{pmatrix} = \begin{pmatrix} \tilde{\pi}^{\alpha_1} & 0 \\ 0 & g' \end{pmatrix}$$

It is obvious that δ belongs to K. Therefore $\underline{n}d_\beta \delta$ is in $Kd_\alpha K$, which means that its invariant factors are $\tilde{\pi}^{\alpha_1}, \cdots, \tilde{\pi}^{\alpha_n}$. Thus $\tilde{\pi}^{\alpha_2}, \cdots \tilde{\pi}^{\alpha_n}$ are the invariant factors for g', which implies that g' belongs to $K_{n-1} d_\alpha - K_{n-1}$ with obvious notations. Our assertion is trivially true for$n = 1$. If we assume that it is true for all groups $GL_r(\tilde{P})$ for $r \leq n-1$, we get $\overline{\alpha} \leq \overline{\beta}$. But $\alpha = \beta$, therefore $\alpha \leq \beta$. We prove the second assertion also by induction on n. For $n = 1$, it is trivially true. Let us assume that the results is true for all groups $GL_r(P)$ for $r \leq n-1$. We have to show that $d_\alpha^{-1} \underline{n} d\alpha$ belongs to K if $\underline{n}d_\alpha$ belongs to $Kd_\alpha K$ Let us suppose that

$$n = \begin{pmatrix} 1 & a_{12} & \cdots a_{1n} \\ 0 & 1 & * \\ & \ddots & \\ 0 & 0 & 0 \end{pmatrix}$$

Since $\underline{n}d_\alpha$ belongs to $Kd_\alpha K \tilde{\pi}^{\alpha_1}$ divides a_{1i} for $i = 2, \cdots, n$. Obviously

$$d_\alpha^{-1}\underline{\mathrm{n}}d_\alpha = \begin{pmatrix} 1 & x_{12} & \cdots x_{1n} \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & X \\ 0 & g' \end{pmatrix}$$

87 where X consists of integers $x_{ij} = \tilde{\pi}^{-\alpha_1} a_{ij}$, and g' is *a* $(n-1 \times n-1)$ mat rix of the form $d_{\alpha^-}^{-1}\underline{\mathrm{n}}' d_{\alpha^-}$ and the invariant factors of $n' d_\alpha -$ are $\tilde{\pi}^{\alpha_2}, \cdots, \tilde{\pi}^{\alpha_n}$. Therefore by induction hypothesis g' belongs to K_{n-1}. This shows that $d_\alpha^{-1}\underline{\mathrm{n}}d_\alpha$ belongs to K. □

3 Study of $O_n(\varphi, P)$

In this section we shall prove some of the results of §2 for the group $G = O_n(\varphi, P)$.The same results can be proved for other such groups of $GL_n(P)$ namely $SL_n(P)$ etc. with obvious modifications. Throughout our discussion P will denote *a* locally compact p-adic field such that $K = \mathscr{O}_P | \mathscr{Y}_P$ has characteristic different from 2.

Definition 1. Let E be *a* vector space of dimension n over P. *A* subspace $F \subset E$ is called *isotropic with respect to* φ (a bilinear form as E) if there exists an element x in F such that $\varphi(x, y) = 0$ for every y in F, in other words the bilinear form when restricted to F is degenerate.

Definition 2. *A* subspace $F \subset E$ is called *totally isotropic with respect to* φ if the restriction of φ to F is zero i.e., $\varphi(x, y) = 0$ for every x, y in F.

It is obvious from the definition that the set of totally isotropic subspaces of E is inductively ordered. Therefore there exist maximal totally
88 isotropic subspaces of E. They are of the same dimension, which we call the index of φ. If index of $\varphi = 0, \varphi$ is called *a* non-isotropic form.

Witt's decomposition. Let E_1, E_2 and E_3 be three subspaces of E such that

(1) $E = E_1 \oplus E_2 \oplus E_3$

(2) E_1 and E_3 are totally isotropic.

(3) $E_1 + E_3$ is not isotropic.

(4) E_2 is orthogonal to $E_1 + E_3$ i.e., for x in $E_2, \varphi(x, y) = o$ for every $y \in E_1 + E_3$.

It can be proved that for the vector space $E = P^n$, there exists *a* Witt decomposition and we can find *a* basis $e_1, e_2, \cdots, e_r$ of $E_1, e_{r+1}, \cdots, e_{r+q}$ of E_2 and $e_{r+q+1}, \cdots, e_n$ of E_3, where $2r + q = n$, in such *a* way that

$\varphi(e_i, e_j) = \delta_{i,n+1-j}$ for $1 \leq i \leq r$ and $r + q < j \leq n.(I)$ and that $r_{r+1}, \cdots, e_{r+q}$ is an orthogonal basis for E_2. Clearly the matrix of the bilinear form φ with respect to this basis of E is

$$\Phi = \begin{pmatrix} O & O & S \\ O & A & O \\ S & O & O \end{pmatrix} \text{ where } S = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

and A is a $q \times q$ matrix, which is the matrix of φ restricted to E_2.

We shall now completely determine the restriction of φ to the non - isotropic part. For simplicity we assume that $r = 0$ and $q = n$. Let $e_1, \cdots, e_q$ be an orthogonal basis of E. If $x = (x_1, \cdots, x_q)$ is *a* point of E with respect to these basis. Then $\varphi(x, x) = \sum\limits_{i=1}^{q} a_i x_i^2$ with $a_i \in P$. If $\dfrac{-a_j}{a_i}$ for $i \neq j$ is in $(P^*)^2$, then the vector $(o, \cdots, a_j, \cdots, a_i, \cdots, o)$ **89**
is an isotropic vector of φ, which is not possible. Therefore $a_i \not\equiv a_j$ (mod P^{*2}), which implies that $q \leq 4$. We shall say that two bilinear forms φ and φ' are equivalent if there exists *a* linear isomorphism of the space of φ onto the space of φ' and *a* constant $c \neq 0$, such that $\varphi' \circ \lambda = \circ\varphi$. Then it can be proved that every non-isotropic bilinear form over E is equivalent to one and only one of the following type:

(1) q=4

(a) $x_1^2 - Cx_2^2 - \pi x_3^2 + C\pi x_4^2$

(2) q=3

(a) $x_1^2 - Cx_2^2 - \pi x_3^2$

(b) $x_1^2 - Cx_2^2 - C\pi x_3^2$

(3) q=2

(a) $x_1^2 - Cx_2^2$

(b) $x_1^2 - \pi x_2^2$

(c) $x_1^2 - C\pi x_2^2$

(4) q=1

(a) x_1^2

(5) q=o

90 (a) The O-form as where $(1, C, \pi, C\,\pi)$ is a set of representatives of P^* modulo $(P^*)^2$ as obtained in Corollary 2 of Hensel's Lemma.

We shall say that *a* basis $e_i, \ldots, e_n$ is a Witt basis for φ if the relations in (I) are satisfied and if the restriction of φ to E_2 has one of the above forms. It is obvious that for φ or for a constant multiple fo φ, we can always find a Witt besides and the matrix of φ with respect to *a* Witt basis is independent of the choice of the Witt basis.

Proposition 4. *If $M = M_q(P)$ is a matrix such that $M'AM$ belongs to $M_q(\mathscr{O})$ (M' denotes the transpose of the matrix M and A denotes the matrix of the restriction of φ to E_2), then M belongs to $M_q(\mathscr{O})$.*

Proof. We prove first that if for $x \in E$, $\varphi(x, x)$ is in $\mathscr{O}$, then the coordinates of x are in $\mathscr{O}$. Let us assume for instance that $q = 4$. If possible let $v(x_1) < 0$ and $v(x_1) \leq \min(v(x_2), v(x_3), v(x_4))$. Suppose that $v(x_1) = \alpha$. Since $v(x_1^2 - cx_2^2 - \pi x_3^2 - c\pi x_4^2) \geq 0$ we have $x_1^2 - Cx_2^2 \equiv o$ (mod $\mathscr{Y}^{2r+1}$), where $r = max(0, \alpha)$. Therefore $(\pi^{-\alpha}x_1)^2 - s(\pi^{-\alpha}x_2)^2 \equiv 0$ (mod $\mathscr{Y}$).

But this is impossible, because $\overline{C}$ is not *a* square in k. Thus our result is established. The other cases can be similarly dealt with. □

Let $M = (m_{ij})$, then $M'AM = (\gamma_{ij})$ where $\gamma_{ij} = \varphi(m_{1i}, \cdots, m_{qi}m_{qj})$, If $M'AM$ belongs to $M_q(\mathscr{O})$ then γ_{ii} belongs to $\mathscr{O}$, which implies that

m_{ri} belongs to $\mathscr{O}$ for $i, r = 1, 2, \cdots, q$. It is obvious that it is sufficient to assume that only the diagonal elements of $M'AM$ are in $\mathscr{O}$.

In the following we shall be dealing with a fixed Witt basis of the 91
space E. We shall adhere to the following notations throughout our discussion.

$$K^o = G \cap K, T^o = G \cap T, N^o = G \cap N, \Delta^o = G \cap \Delta^+ \qquad \text{and}$$

$$d_\alpha^\circ = \begin{pmatrix} \pi^{-\alpha_1} & & & & & & \\ & \ddots & & & & & \\ & & \pi^{-\alpha_r} 0 & & & & \\ & & & 1 \ddots 1 & & & \\ & & & & \pi^{\alpha_r} & & \\ & & & & & \ddots & \\ & & & & & & \pi^{\alpha_1} \end{pmatrix}$$

where $\alpha = (\alpha_1, \cdots, \alpha_r)$

Proposition 5. $G = T^o K^o$

Proof. We have already proved that $GL_n(P) = TK$. Therefore $g \in G$ implies that $g = tk$ where t and K belong to T and K respectively. We know that det $(g) = \pm 1$ and det (k) belongs to $\mathscr{O}^*$. So det (t) belongs to $\mathscr{O}^*$. But det (t) is a power of π, therefore det $(t) = 1$. Now g belongs to G if and only if $g'\Phi g = \Phi$ i.e., $t'\Phi t = k^{-1'}\Phi K^{-1}$. Since $k^{-1'}\Phi k^{-1}$ belongs to $M_n(\mathscr{O}), t'\Phi t$ belongs to $M_n(\mathscr{O})$. ◻

Let us suppose that

$$t = \begin{pmatrix} a_1 & X & Z \\ O & a_2 & Y \\ O & O & a_2 \end{pmatrix}$$

then $$t'\Phi t = \begin{pmatrix} o & O & a_1' S a_3 \\ o & a_2' A a_2 & X' S a_3 + a_2' A Y \\ a_3' S a_1 & Y' A a_2 + a_3 S X & Z' S a_3 + Y' A Y + a_3' S Z. \end{pmatrix}$$

This shows that $a_1' S a_3$ and a_3 and $a_2' A a_2$ belong to $M_n(\mathscr{O})$. More- 92 over, we have $1 = \det t = (\det a_1)(\det a_2)(\det a_3)$ and $(\det a_2)$ and $(\det a_1)$. $(\det a_3)$ belong to $\mathscr{O}$ (for, $a_1' S a_3$ belongs to $M_n(\mathscr{O})$). So det a_2 belongs to $\mathscr{O}^*$ implying a_2 belongs to K. By above proposition we get that the matrix a_2 has coefficients from $\mathscr{O}$. We shall find a matrix δ in $T \cap K$ such that $t\delta$ belongs to G. Then $g = tK = t\delta\delta^{-1}K$ implies that $\delta^{-1}K$ belongs to K^o and our result will be proved. Multiply the matrix t by the matrices h and h' on the right. where

$$h = \begin{pmatrix} b & 0 & 0 \\ 0 & a_2^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad h' = \begin{pmatrix} 1 & \xi & \zeta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

we get
$$t\,h\,h' = \begin{pmatrix} a_1 b & a_1 b + a_2^{-1} X & a_1 b\zeta + z \\ 0 & 1 & Y \\ 0 & 0 & a_3 \end{pmatrix}$$

We shall determine the matrices b, ξ and ζ in such a way that $t\,h\,h'$ belongs to G. Now $t\,h\,h'$belongs to G if and only if

$(t\,h\,h')'\Phi(t\,h\,h') = \Phi$ i.e., if and only if the following conditions are satisfied

$$b' a_1' S a_3 = S \tag{1}$$
$$AY + X' a_2^{-1} S a_3 + \xi' b' a_1' S a_3 = 0 \tag{2}$$
$$a_3' S a_1 b\zeta + a_3' S Z + y' AY + \zeta' b' a_1' S a_3 + Z' s a_3 = 0 \tag{3}$$

Let us take $b' = S(a_1' S a_3)^{-1}$. Then h belongs to $K \cap T$ and the
93 conditions (2) and (3) reduce to

$$AY + X'(a_2^{-1})' S a_3 + \xi' S = 0$$
$$S\zeta + a_3' S Z + Y' AY + \zeta' S + Z' S a_3 = 0$$

So if we take $S\xi' = -AY - X' a_2^{-1} S a_3$ and $s\zeta = -\dfrac{1}{2} V$ where $V = a_3' S Z + Y' AY + Z' S a_3$, we see that the matrix thh' belongs to G. It is obvious that the matrix hh' belongs to $T \cap K$.Hence we get $g = thh'.(hh')^{-1}k = t_\circ k_\circ$, which proves our result completely.

Definition. Let I be a lattice in E. The $\mathscr{O}$ module $\mathfrak{N}(I)$ generated by the set of elements $\varphi(x, y)$ for x, y in I is called the *norm* of the lattice I.

A lattice I is called a maximal lattice if it is maximal among the lattices of norm $\mathfrak{N}(I)$. It is easy to see that any lattice of a given norm is contained in a maximal lattice of the same norm. The lattice I_o generated by the Witt basis $(e_1, \cdots, e_n)$ of E is a maximal lattice of norm $\mathscr{O}_n$. Let I be a lattice of norm $\mathscr{O}$ containing I_o. Let $x = \sum\limits_{i=1}^{n} x_i e_i$ be any element in I. Then $\varphi(x, e_i) = \pm x_{n+1-i}$ for $1 \leq i \leq r$ and $r + q < i \leq n$. let y= $\sum\limits_{i=r+1}^{r+q} x_i e_i$, since $\varphi(y, e_j)$ is an integer for $r + 1 \leq j \leq r + q, x_j$ is an integer for $r + 1 \leq q + r$. Hence x belongs to I_o. Therefore I_o is a maximal lattice.

Theorem 2. *Let I_1 and I_2 be two maximal lattices of norm $\mathscr{O}$, then there exists a Witt basis $(f_1, f_2, \cdots, f_n)$ of E and r integers*
$\alpha_i \geq \cdots \geq \alpha_r \geq 0$, such that ($r$ =index φ)

(1) *I_1 is generated by $(f_1, f_2, \ldots, f_n)$* **94**

(2) *I_2 is generated by*

$$\left(\overset{-\alpha_1}{\pi} f_1, \ldots, \overset{-\alpha_r}{\pi} f_r, f_{r+1}, \ldots, f_{r+q}, \overset{\alpha_r}{\pi} f_{r+q+1}, \ldots, \overset{\alpha_1}{\pi} f_n\right).$$

Proof. We shall prove the theorem by induction on r. When $r = 0$, φ is non-isotropic and there exists only one maximal lattice of norm $\mathscr{O}$ which is generated by any witt basis of E. Let us assume that the theorem is true for all bilinear forms of index $< r$. We first prove the following result. □

If I is a maximal lattice of norm $\mathscr{O}$ and X is an isotropic vector in I such that $\pi^{-1}X$ does not belong to I, then there exists an isotropic vector $X' \in I$ such that $\varphi(X, X') = 1$.

If possible let us suppose that the result is not true. Let us assume that $\varphi(X, Y)$ belongs to $\mathscr{Y}$ for every Y in I. Then $\varphi(\pi^{-1}X, Y)$ belongs to $\mathscr{O}$. Consider $I' = I + \mathscr{O}\pi^{-1}X$. It is a lattice because I' is finitely generated $\mathscr{O}$ module containing I. Moreover

$\varphi(Y + \alpha\pi^{-1}X, Z + \beta\pi^{-1}X) = \varphi(Y, Z) + \alpha\varphi(\pi^{-1}X, Z) + \beta\varphi(\pi^{-1}X, Y)$ is an integer for every α, β in $\mathscr{O}$. Therefore norm of I' is $\mathscr{O}$. But this is a

contradiction because I is *a* maximal lattice of norm $\mathscr{O}$. Therefore there exists *a* vector Y in I such that $\varphi(X, Y)$ belongs to $\mathscr{O}^*$. By multiplying Y by some inversible element of $\mathscr{O}$, we get *a* vector Y' in I such that $\varphi(X, Y') = 1$. Let us take

$X' = Y' - \dfrac{1}{2}\varphi(Y', Y')X$. Obviously $\varphi(X, X') = 1$ and $\varphi(X', X') = O$.

Now we shall prove the theorem. For every isotropic vector $X \in I_1$
95 (respectively I_2) let $t(X)$ (respectively u(X)) denote the smallest integer such that $\overset{t(x)}{\pi} X$ (respectively $\pi^{u(X)}X$) belongs to I_2(respectivelyI_1). Such an integer exists. because I_1 is an $\mathscr{O}$-module of finite type and I_2 generates E, therefore there exists an integer t such that $\pi^t I_1 \subset I_2$. Thus $t(X) \leq t$ always. Let X be an isotropic vector in I_1 such that $\pi^{-1}X$ does not belong to I_1. Then $Y = \pi^{t(X)}X$ belongs to I_2 and $\pi^{-1}Y$ does not belong to I_2. Since $\pi^{-1}X$ does not belong to I_1, it is obvious that $u(Y) = -t(X)$. By the above result there exists *a* vector X' in I_1 such that $\varphi(X, X') = 1$ and $\varphi(X', X') = 0$. This shows that $\pi^{-1}X'$ does not belong to I_1. By the definition of $t(X)$ and $t(X)'$ we get that

$$\varphi\left(\pi^{t(X)}X, \pi^{t(X')}X'\right) = \pi^{t(X)+t(X')}$$

Since $\varphi(\pi^{t(X)}X, \pi^{t(X)}X, \pi^{t(X')}X)$ belongs to $\mho$, we get that

$$t(X) + t(X') \geq 0. \tag{1}$$

Similarly there exists an isotropic vector Y' in I_2 such that

$$\varphi(Y, Y') = 1 \text{and } u(Y) + u(Y') \geq 0.$$

Let $Z = \pi^{u(Y')}Y'$, then $t(Z) = -u(Y')$

Therefore we get

$$t(X) + t(Z) \leq 0 \tag{2}$$

obviously Z is isot ropic and $\pi^1 Z$ does not belong to I_1. Therefore there exists *a* vector Z' in I_1 such that $\varphi(Z, Z') = 1$ and $\varphi(Z', Z') = 0$ and

$$t(Z) + t(Z') \geq 0 \tag{3}$$

Let us suppose that the vector X is so chosen that $t(X)$ is of maximum value, which exists because $t(X) \leq t$ for every X for some integer t.

96 Therefore in particular we get $t(Z') \leq t(X)$. From (2) and (3) it follows that

$$t(X) + t(Z) = 0$$
$$t(X) + t(Z') = 0$$

Thus we have found two vectors X and Z in I_1 such that $\pi^{\alpha_1}X$ and $\pi^{-\alpha_1}Z$ where $\alpha_1 = t(X)$ belong to I_2 and

$$\varphi(Z, X) = \varphi(\pi^{-t(Z)}Y', \pi^{t(X)}Y) = 1.$$

Let F denote the subspace of E orthogonal to the subspace of E generated by the vectors X and Z.Obviously φ restricted to F is non - de- generate and its index is $r-1$. Moreover $I_1 = \mathscr{O}X \oplus \mathscr{O}Z \oplus F \cap I_1$, because for any a in I_1 we have

$a = \lambda X + \mu\, Z + b$, where λ and $\mathscr{O}$ belong to ρ and b belongs to F.

But $\varphi(a, X) = \mu$, therefore it is an integer, similarly λ is an integer. Thus b belongs to I_1 and the assertion is proved. Similarly we have $I_2 = \mathscr{O}\pi^{\alpha_1}X \oplus \mathscr{O}\pi^{-\alpha_1}Z \oplus I_2 \cap F$. It can be easily sen that $I_j \cap F (j = 1, 2)$ is a maximal lattice of norm $\mathscr{O}$. Hence by induction hypothesis there exists a Witt basis $f_2, f_3, \cdots, f_{n-1}$ of F and there exist r-1 integers $\alpha_2 \geq - - \alpha_r \geq o$ such that

(1) $f_1, f_2, \cdots, f_{n-1}$ generate $I_1 \cap F$.

(2) $\overset{-\alpha_2}{\pi} f_2, \ldots, \overset{-\alpha_r}{\pi} f_r, f_{r+1}, \ldots, f_{r+q}, \overset{\alpha_r}{\pi} f_{r+q+1'} \overset{\alpha_2}{\pi} f_{n-1}$ generate $I_2 \cap F$.

If we take $f_1 = Z$, $f_n = X$ and $\alpha_1 = t(X)$ we get a Witt basis $(f_1, \cdots, f_n)$ 97
of E and r integers $\alpha_1, \cdots, \alpha_r$ satisfying the requirements of the theorem because $\alpha_2 = t(f_{n-1)} \leq \alpha_1$.

Corollary 3. *The group G acts transitively on the set of lattices of norm $\mathscr{O}$.*

The mapping g defined by

$$g(f_i) = \pi^{\gamma} f_i, \text{ where}$$
$$\gamma = \alpha_i \text{ for } 1 \leq i \leq r$$

$$= O \text{ for } r+1 \leq i \leq r+q$$
$$= 2r+q-i+1 \text{ for } r+q+1 \leq i \leq 2r+q.$$

leaves Φ invariant. Therefore g belongs to G.

Proposition 6. *In each double coset of G modulo K^o there exists one and only one element d_α of Δ_+^o.*

Proof. Let g be any element of G. We shall denote by g itself the automorphism of E with respect to the initial Witt basis$(e_1, \cdots, e_n)$. The lattice $g(I_o)$ is obviously *a* maximal lattice of norm $\mathscr{O}$. Therefore by the above theorem we get *a* Witt basis $(f_1, \cdots, f_n)$of E such that

(1) I_o is generated by $f_1, \cdots, f_n$,

(2) $g(I_o)$ is generated by $g_1, \cdots, g_n$ where $g_i = \pi^\gamma f_i$ with

γ as defined in the corollary of above theorem. Let $\underline{k_1}$ (respectively $\underline{k_2}$) be the matrix with respect to the basis $e_1, \ldots, e_n$) (respectively $g_!, g_2, \ldots g_n$) of the automorphism k_1 (respectively k_2) defined by $k_1(e_i) = f_i$ (respectively $k_2(g_i) = g(e_i)$) for $i = 1, 2, \cdots, n$. We see immediately that the matrix $\underline{K_1}$ and $\underline{K_2}$ are in K^o. Moreover the matrix of the automorphism $f_i \to g_i$ with respect to the basis f_i is d^o_α where $\alpha = (\alpha_1, \alpha_2, \cdots \alpha_r)$. ◻

98 It is obvious that

$$\begin{aligned} g(e_i) &= \sum_j \underline{(k_2)}_{ji}\, g_j \\ &= \sum_{j,k} \underline{(k_2)}_{ji} (d^o\alpha)_{kj}\ f_k \\ &= \sum_{j,k,l} \underline{(k_2)}_{ji} (d^o\alpha)_{kj}\ \underline{(k_1)}_{lk}\ e_l \end{aligned}$$

Thus we get $g = \underline{k_2}\ d^0_\alpha\ \underline{k_1}$, which means d_α belongs to $K^0 g K^0$.The uniqueness part of the propositional follows from the uniqueness of d^o_α in $K\ x\ K$ for x in $GL_n(P)$.

We introduce a total ordering in Z^n which is inverse of the lexicographic ordering.

Proposition 7. *Let α and β be two elements in Z^r such that $d^0_\alpha \in \triangle^0_+$. If $N^0\, d^0_\beta\, K^0 \cap K^0\, d^0_\alpha\, K^0 \neq \phi$ then $\beta \geq \alpha$. Moreover $N^0\, d^0_\alpha\, K^0 \cap K^0\, d^0_\alpha\, K^0 = d^0_\alpha\, K^0$.*

Proof. Since $N^0\, d^0_\beta\, K^0$ and $K^0\, d^0_\alpha\, K^0$ are contained in $N\, d'_\beta K$ and $K\, d'_\alpha\, K$ respectively with

$$\begin{aligned}
\alpha' &= (-\alpha_1, -\alpha_2, \ldots, -\alpha_r, 0 \cdots 0, \alpha_r, \alpha_{r-1}, \ldots, \alpha_1)\\
\beta' &= (-\beta_1, -\beta_2, \ldots, -\beta_r, 0 \cdots 0, \beta_r, \beta_{r-1}, \ldots, \beta_1)
\end{aligned}$$

we have $N\, d_\beta, K \ \cap\ K\, d_\alpha,\ K \neq \phi$. Therefore $\beta' \geq \alpha'$ for the lexicographic ordering introduced in Z^n before proposition 3 in this chapter. It is obvious that $\beta \geq \alpha$ for the new ordering of Z^r. The other assertion follows trivially from the fact that

$$d^0_\alpha K \cap G = d^0_\alpha K^0. \qquad \square$$

4 Representations of p-adic Groups

We prove here an analogue of the theorem about the representations of semisimple Lie Groups in chapter I of this part. We shall give the proof of the theorem for the general linear group $GL_n(P) = G$, though the same theorem could be proved for other classical linear groups with obvious modifications. We shall adhere to the notations adopted in the earlier chapter. **99**

Let λ denote a character of T which is trivial on N. Since $\triangle$ is isomorphic to $T/N, \lambda$ can be considered as a character of $\triangle$. Let us assume that $U^\lambda_f = 0$ for every λ in $\triangle^*$ (the group of characters of $\triangle$) and $f \in L(G)$ such that $f \neq 0$. We first try to find the condition under which our assumptions are valid. Let φ be an element of C^λ (the space of the induced representation of λ). Then $\varphi(tx) = (\rho(t))^{\frac{1}{2}} \lambda(t)\varphi(x)$ for $x \in G$ and $t \in T$. Moreover

$$U^\lambda_f \varphi(e) = \int_G \varphi(y) f(y) dy = 0, \text{ because } U^\lambda_f = 0 \qquad \text{(I)}$$

Since $\sum$ the support of f is a compact set, it intersect only a finite number of double cosets modulo K. Let

$$S = S(f) = \left[\alpha | d\alpha \in \triangle_+, \sum \cap K\ d_\alpha\ K \neq \phi\right]$$
$$\alpha = \alpha(f) = \min_{\beta}\ \{\beta \in S(f)\}.$$

The set S is a finite non-empty set because $f \neq 0$. Therefore α exists. For any d_α in $\triangle_+$ the coset $K\ d_\alpha\ K$ is a finite union of left cosets modulo K, the representatives for which could be found in T,because $G = TK$. Let I_α be the set of left cosets C modulo K such that $K\ d_\alpha\ K =$
100 $\bigcup\limits_{C \in I_\alpha} C$, where $C = t(C)K, t(C) \in T$. But we know that $T = N\triangle$, therefore $t(C) = n(C)\ d_\gamma(C)$ where $n(C)$ and $d_\gamma(C)$ belong to N and $\triangle$ respectively. Since $n(C)\ d_\gamma(C)$ belongs to $K\ d_\alpha\ K$ proposition 3 implies that $\gamma(C) \geq \alpha$, Thus we get that $K\ d_\alpha\ K = m \bigcup\limits_{C \in\ I_\alpha} n(C)\ K$, $\gamma(C) \geq \alpha$ and if $\gamma(c) = \alpha$, then $C = d_\alpha\ K$ and we can take $t(c) = d_\alpha$. Let us assume that the right invariant Haar measure on G is such that its restriction to K is normalised i.e., $\int_k d_k = 1$. Then for any left coset $C = t(C)K$, we have

$$\int_G f(g) d_g = \triangle(t(C)) \int_K f(t(C)k)\ dk$$

and the equation (I) gives

$$\begin{aligned} 0 = \int_G \varphi(y) f(y)\ dy &= \sum_{\beta \in S} \sum_{C \in I_\beta} \triangle(t(C)) \int_K \varphi(t(C)k) f(t(C)k) dk \\ &= \sum_{\beta} \sum_{C} \sigma(t(C)) \int_K \varphi^0(k)\ f(t(C)k)\ dk \end{aligned}$$

with $\sigma(t) = [\delta(t)\triangle(t)]^{\frac{1}{2}}$ and where φ^0 denotes the restriction of φ to K.

We have shown earlier that $\varphi^0(tx) = \lambda(t)\ \varphi^0(x)$ for $t \in T \cap K = N \cap K$, but $\lambda(N) = 1$, therefore the space C^λ is independent of λ. Moreover there is only one term corresponding to $\beta = \alpha$ in the summation, since for others $\gamma(c) \geq \alpha$. Separating the term for $\beta = \alpha$ we get $U^\lambda_f \varphi(e) =$

$\sigma(d_\alpha)^{\frac{1}{2}}\lambda(d_\alpha)\ \int_K \varphi^o(k)f(d_\alpha\ k)dk + \sum_{\gamma\geq\alpha} Q_\gamma(f,\varphi)\lambda(d\gamma)$ with

$$Q_\gamma(f,\varphi) = \sum_{C\in I_\beta \gamma(C)=\alpha} \sigma(t(C))^{\frac{1}{2}} \int_K \varphi^0(k)f(t(C)k)dk \tag{II}$$

It is obvious that $Q_\gamma(f,\varphi)$ is independent of λ. For every $\gamma\in Z^n$, the mapping $d_\gamma\in\triangle\longrightarrow\chi_\gamma\in\triangle^{**}$ given by $\chi_\gamma(\lambda)=\lambda(d_\gamma)$is an isomorphism of the groups $\triangle$ and $\triangle^{**}$. But the characters of an abelian group are linearly independent, therefore (II) gives us $Q_\gamma(f,\varphi)=0$ for every γ and in particular $Q_\alpha(f,\varphi)=0$. Thus we obtain **101**

$$\int_K \varphi(k)f(d_\alpha k)dk = 0, \text{ for every } \varphi \text{ with } \varphi(nk)=\varphi(k) \text{ for } n\in N\cap K. \tag{III}$$

The equation (III) is true for left and right translations of f by elements of K because $U^\lambda_{\sigma_{xf}} = U^\lambda_{\varepsilon_{xn*f}} = U^\lambda_x U^\lambda_f = 0$ and

$$U^\lambda_{\tau_{xf}} = U^\lambda_{f*\varepsilon_x} = U^\lambda_f\ U^\lambda_x = 0.$$

So if $g(x)=f(k^{-1}x)$ for k in K, we have $U^\lambda_g=0$. Obviously $S(f)=S(g)$ and $\alpha(f)=\alpha(g)$. Let $K'_\alpha = K\cap d_\alpha K\ d_\alpha^{-1}$ and $K_\alpha = K\cap d_\alpha^{-1}\ K\ d_\alpha$ be two subgroups of K. Now

$$\int_K \varphi(k)f(d_\alpha(d_\alpha^{-1}\ hd_\alpha\ k))dk = \int_K \varphi(d_\alpha^{-1}\ hd_\alpha\ k)f(d_\alpha k)dk = 0$$

Thus the function $k\to f(d_\alpha\ k)$ is orthogonal to all the functions φ in $C^\lambda = C$ and their left translates by the elements of K_α, where φ is invariant on the left by the elements of $N\cap K$.

Lemma. *For every $\alpha\in Z^n$ such that $d_\alpha\in\triangle_+$, the subgroup K_α contains $N'\cap K$ where N' is the group consisting of the transpose of elements of N.*

Proof. By definition

$$d_\alpha = \begin{pmatrix} \pi^{\alpha_1} & & 0 \\ & \ddots & \\ 0 & & \pi^{\alpha_n} \end{pmatrix} \text{ with } \alpha_1\leq\alpha_2\leq,\dots,\leq\alpha_n.$$

□

Let $h = (h_{ij})$ be an element of K. Then $(d_\alpha\, h\, d_\alpha^{-1})_{ij} = \pi^{\alpha_i - \alpha_j} h_{ij}$ 102
which shows that the groups K_α consist of matrix h in K such that $\pi^{\alpha_i-\alpha_j} h_{ij}$ is integral. If we take $h \in N' \cap K$, obviously h belongs to K_α. Thus K_α contains $N' \cap K$. This lemma shows that the groups K_α and K'_α are sufficiently big.

In addition to the above assumption about f, let us further assume that f belongs to $L_M(G)$ where M is some irreducible representation of K. Clearly M is a subrepresentation of left regular representation of K in $L^2(K)$. Let $E \subset L^2(K)$ be an invariant subspace of the left regular representation σ of K such that σ when restricted to E is of class M. Therefore $E \subset L_M(K)$. Define $F(k) = f(\underline{d}_\alpha\, k)$. We can assume that $F \neq 0$. Since F is transformed following $\bar{M}$ by the right regular representation of K, F belongs to $L_M(K)$. But F is orthogonal to all the functions φ in C invariant on the left by the elements of $N \cap K$, the left translates of φ by the elements of K and the right translates of φ by the elements of K. Hence if M satisfies the condition (S) i.e. The smallest subspace of E invariant by N' and which contains elements invariant on the left by the elements of $N \cap K$ is E. Then F is orthogonal to $L_M(K)$,
103 because $L_M(K)$ is generated by the right translates of E. But this is a contradiction, because $F \in L_M(K)$. Thus we get the following

Theorem 3. *The representations U^λ for $\lambda \in \triangle^*$ form a complete system of representations of the algebra $L_M(G)$ if the irreducible representation M satisfies the condition (S).*

Corollary 1. *If M satisfies (S) then M occurs atmost $(\dim M)$ times in any completely irreducible representation of G.*

Since U^λ for any λ in $\triangle^*$ when restricted to K is a subrepresentation of the left regular representation of $K, C \subset L_M(K)$ which is a subspace of dimension $(\dim M)^2$, thus M is contained at most $(\dim M)$ times in U^λ. Our result follows from proposition 1.3.

Corollary 2. *The identity representation of K occurs at most once in any completely irreducible representation of G.*

This follows from Corollary 1 as the identity representation satisfies the condition (S).

Corollary 3. *If M is the identity representation of K, then the algebra $L_M(G)$ is commutative.*

The algebra $L_M(G)$ has complete system of representations of dim 1. Therefore if x and y are any two elements of $L_M(G)$, then $U^\lambda(x\,y) = U^\lambda(y\,x)$ for every $\lambda \in \triangle^*$, because U^λ is of dimension 1. Therefore $U^\lambda(xy-yx) = 0$ for every λ in $\triangle^*$. But this is possible only if $xy-yx = 0$ i.e., the algebra $L_M(G)$ is commutative.

Finally we try to find out what are the various representations of K which satisfy the condition (S). It is obvious that a representation which satisfies the condition (S) when restricted to $N \cap K$ contains the identity **104** representation of $N \cap K$. It is not known whether there exist or not representations of K which when restricted to $N \cap K$ contain the identity representation but which do not satisfy the condition (S). However in this connection we have the following result.

Theorem 4. *Every irreducible representation M of K which comes from a representation of $GL_n(\mathscr{O}/\mathscr{Y})$ and the restriction of which to $N \cap K$ contains the identity representation of $N \cap K$ satisfies the condition (S).*

It can be easily proved that $GL_n(\mathscr{O}/\mathscr{Y})$ is isomorphic to K/H, where H is a normal subgroup K consisting of the matrices $(\delta_{ij}+a_{ij})$ where a_{ij} belongs to $\mathscr{Y}$. Therefore a representation of $GL_n(\mathscr{O}/\mathscr{Y})$ gives rise to a representation of K.

Remark. We have proved that in the case of real or complex general linear group the representations induced by the unitary characters of T form a complete system of representations of algebra $L(G)$. But in the case of general linear groups over p-adic fields the representations induced by the characters of $\triangle$ do not form a complete system. In fact the algebra $L(K)$ is a sub-algebra of $L(G)$, because K is open and compact in G. Therefore if the representations U^λ form a complete system for $L(G)$, their restrictions to K will form a complete system of representations of $L(K)$. But the restriction of U^λ to K is a representation of K induced by the unit character of $N \cap K$, therefore by Frobenius reciprocity theorem the irreducible representations of K which occur in

U^λ are precisely those which when restricted to $N \cap K$ contain the identity representation. But there exist representations of K for which this property is not satisfied.

5 Some Problems

I.

105 For any classical group, we have found a maximal compact subgroup K. If G is the general linear group, it is easy to see that:

(i) *any maximal compact subgroup is conjugate to K by an inner automorphism;*

(ii) *any compact subgroup is contained in a maximal compact subgroup*. (For, let H be a compact subgroup of $GL(n, \tilde{P})$ let $e_1, \ldots, e_n$ be the canonical basis of $\tilde{P}^n$. Let I_0 be the $\tilde{O}$-module generated by the e_i and let I be the $\tilde{O}$-module generated by the $h\, e_i$ for $h \in H$: because H is compact, the coordinates of the $h.e_i$ are bounded and there is an integer $n \geq 0$ such that $I \subset \tilde{\pi}^{-n} I_0$. Hence I is a lattice and H is contained in the maximal compact subgroup K_1 formed by the $g \in G$ such that $g.I = I$. Moreover, if $g \in G$ is such that $g.I_o = I$, then $K_1 = gKg^{-1}$.)

But for the other types of classical groups, it is not known if the results (i) and (ii) are true or not. Actually, one cannot hope that (i) is true: already in $SL(n, P)$, we have only:

(i bis) *any maximal compact subgroup is conjugate to K by an (not necessarily inner) automorphism.*

It seems possible that there exist several but a finite number of classes of maximal compact subgroups: for instance, it seems unlikely that the maximal compact subgroup K' of the orthogonal group 0(n,P) which leaves invariant a maximal lattice of norm $\mathscr{P}$ is conjugate to K. But perhaps, any maximal compact subgroup of $0(n, P)$ is conjugate to K or to K'.

It may be noted that (i) and (ii) are not both true in the *projective*
106 group $G = PGL(2, P)$: a maximal compact subgroup K is the canonical image of $GL(2, 0)$ in G; the determinant defines a map d from G to the quotient group $P^*/(P^*)^n$ and the image of any conjugate of K is

contained in the image D of 0^* in $P^*/(P^*)^2$. Now, let u be the image of $\begin{pmatrix} 0 & \pi \\ 1 & 0 \end{pmatrix}$ in G: we have $u^2 = 1$ and $d(u) \notin D$. Hence, u generates a compact subgroup which is *not* contained in any conjugate of K.

II.

It seems very likely that our results about classical groups are valid for any semi-simple algebraic linear group over P(at least if char $P = 0$). The general meaning of the subgroups N, D, T Γ is clear: N is a maximal unipotent, D is a maximal decomposed torus (a decomposed torus is an algebraic group isomorphic to $(P^*)^r$), which normalised N. Then D can be written as $D = \triangle.U$, where $\triangle \approx Z^r$ and $U \approx (0^*)^r$ and we have $T = \triangle.N$. The subgroup Γ is the normaliser of N. It can be proved (A.Borel,unpublished) that D and N exist in any such G (at least if the base field P is perfect) and are unique, upto an inner automorphism. Now the problems are:

(i) define a maximal compact subgroup K;

(ii) prove that $G = T.K$;

(iii) prove that $G = K.\triangle.K$ and define $\triangle_+$ (which is certainly related with the Weyl group and the Weyl chambers);

(iv) prove the key Lemma about the intersection $Nd_\alpha\, K \cap Kd_\beta K$. For (i), the simplest idea is to take a lattice I in the vector space in which G acts, and to put $K = \{g|g \in G, g.I = I\}$. Then we get a compact subgroup. But it is obvious that K will be maximal and satisfy (ii) and (iii) only if I is conveniently chosen. **107**

Assume that char $P = 0$: then we may consider the Lie algebra $\mathscr{G}$ of G and the adjoint representation. Then we can choose a lattice I in $\mathscr{G}$ such that $[I, I] \subset I$ (in other words, I is a Lie algebra over 0);such a lattice always exists: take a basis $\mathscr{G}$ and multiply it by a suitable power of π in such a way that the constants of structure become integral. Now there exist such lattices which are maximal, because $[I, I] \subset I$ implies that I is a lattice of norm $\subset 0$ for the Killing form of $\mathscr{G}$. As this form is non-degenerate, it is impossible to get an indefinitely growing sequence of such lattices. Hence we can choose such a maximal lattice I and put $K = \{g | g \in G, g.I = I\}$.

But let us look at the *compact* case: it can be shown that G is compact if any only if the Lie algebra $\mathscr{G}$ has no nilpotent elements. In this case, we should have $K = G'$. So we are led to the following conjectures:

Conjecture 1. there is a unique lattice in $\mathscr{G}$ which is a maximal Lie subalgebra over 0;

Conjecture 2. the set I if the $X \in \mathscr{G}$ such that the characteristic polynomial of the operator *ad* X has its coefficients in 0, is a Lie subalgebra over 0;

Conjecture 3. (A.Weil): any algebraic simple compact group over a locally compact P-adic field of characteristic zero is (up to finite groups) the quotient of the multiplicative group of a *division algebra* Q over P by its center.

108 It is easy to prove that (3) implies (2): the Lie algebra $\mathscr{G}$ is the quotient of the Lie algebra Q by its center and the $X \in I$ are exactly the images of the integers of Q. It is obvious that (2) implies (1), because any Lie subalgebra over 0 is contained in I. Moreover, (3) is true for the classical groups: we have only for compact groups the groups $PGL_1(\tilde{P}) \approx \tilde{P}^*$ / center and the orthogonal and unitary groups for an anisotropic form; but 0_1 and 0_2 are abelian 0_3 gives the quaternion field, 0_4 is not simple, etc. But one does not know a general proof of (3).

On the other hand, we can look at the "anticompact" case, that is the case of the groups defined by Chevalley in (12). Then the results (i) to (iv) can be proved (for the definition of K and proof of (ii), see Bruhat (10); for (iii) and (iv), my results are not yet published).

Then *if* one can prove one of the above conjectures, one can hope to generalize these results to any semi-simple group by an argument by induction on the dimension of a maximal nilpotent subalgebra of $\mathscr{G}$.

III. Extension to the representations of K which do not satisfy the condition (S).

This problem is related with the construction of other representations of G: we have seen that the representation U^λ do not form a complete system. Hence, by the Gelfand-Raikov theorem, there certainly exist other irreducible unitary representations of G.

We have two indications: first the case of a real semi-simple Lie group G. It seems very likely that to any class of Cartan subgroups H of G, corresponds a series of representations of G, indexed by the characters of H. This has been verified in some particular cases (of.Harish-Chandra and Gelfand-Graev). In particular, assume that there exists a **109**
compact Cartan subgroup H: then in many cases (more precisely in the cases where G/K is a bounded homogeneous domain in the sense of E. Cartan (K is a maximal compact subgroup)), we can get irreducible unitary representations of G in the following way: take a character λ of H. take the unitary induced representations U^λ in the space $\mathscr{H}^\lambda$; this representation is not irreducible. But we have a complex-analytic structure on G/H and we can look at the subspace of $\mathscr{H}^\lambda$ formed by the functions which correspond to *holomorphic* functions on G/H. Then we get an irreducible representation (of (22) or (21). This is in particular true for compact semi-simple Lie groups (after Borel-Well,of (32)).

On the other hand, in the case of classical linear groups over a *finite* field, for instance for the special linear group G with $2, 3$ or 4 variables, one knows all the irreducible representations of G and one sees that to each class of Cartan subgroup H, corresponds a series of representations indexed by the characters of H (of Steinberg (33)). But one does not know how exactly this correspondence works. It seems likely that the representation $U(\lambda)$ associated with character λ of H is a subrepresentation of the induced representation U^λ, and it would be extremely interesting to get a "geometric" definition of $U(\lambda)$.

If one could get such a definition, it would perhaps be possible to generalize it to the algebraic simple linear groups (or at least to the classical groups) over a p-adic field.

IV. Study of the algebra of spherical functions

Let M be the unity representation of K and Let A be the algebra **110**
$L_M(G)$: by our results,this is a *commutative* algebra. It seems possible to determine completely the structure of A. The representations U^λ likely

give all the characters $\hat{\lambda}$ of A. The λ describe a space isomorphic to a space C^r and the map a $\to$ $(\hat{\lambda}(a))$ is probably an isomorphism of A onto the algebra of polynomials on C^r which are invariant by the Weyl group of G. (It seems that a recent work by Satake (unpublished) gives a positive answer).

V. Computation of the "characters" of the U^λ.

The representations U^λ are "in general" irreducible (of (10)). Moreover, if f is a continuous function on G, with carrier contained in K, and if f belongs to some $L_M(K)$, then it is trivial to show that the operator U_f^λ if of *finite rank*, and hence has a *trace*. The same is obviously true if f is a finite linear combination of translates of such functions. But the space of those f is exactly what I called the space of "regular" functions of G (space $D(G)$) and the map $f \to \text{Tr } U_f^\lambda$ is a "distribution" on $G(of(10))$. A problem is to compute more or less explicitly this distribution (which is the "character" of U^λ. It seems likely that, at least on the open subset of the "regular" elements g of G it is a simple function of the proper values of g (by analogy with the case of complex or real semi-simple Lie groups, of works of Harsih-Chandra and Gelfand-Naimark).

Part III

Zeta-Functions

Chapter 5

Analytic Functions over p-adic Fields

Unless otherwise stated K will denote a completed valuated field with 111
a real valuation v. We shall adhere to the notations adopted in part I throughout our discussion.

1 Newton Polygon of a Power-Series

Definition. Let $f(x) = \sum_{i=0}^{\infty} a_i x^i$ be a power-series over K. Let S be the set of points $A_i = (i, v(a_i))$ in the Cartesian plane. The convex hull of S together with the point $y = \infty$ on the ordinate axis is called the *Newton Polygon* of the power series f.

It is obvious that the point $A_i = (i, v(a_i))$ lies on the line $Y + v(x)X = v(a_i x^i)$, where $v(a_i x^i)$ is the intercept cut off by the line on the $Y-axis$. If the series is convergent at the point $x = t$ then intercepts cut off on the axis of Y by the lines through the points A_i with the slope -$v(t)$ tend to infinity as i tends to infinity. Moreover it can be easily proved that if (m_i) is the sequence of slopes of the sides of Newton Polygon of f, then (m_i) is monotonic increasing and $\overline{\lim}_{i\to\infty} m_i = -\liminf_{i\to\infty} \dfrac{v(a_n)}{n} = \rho(f)$ (the order of convergence of f).

2 Zeroes of a power series

Let $f = \sum_{i=0}^{\infty} a_i x^i$ be a power series over K. Let $\rho(f) = - \liminf_{i\to\infty} \dfrac{v(a_i)}{i}$. We
112 have already proved that f is convergent for all points x in K for which $v(x) > \rho(f)$. Let r be a real number greater than $\rho(f)$. We shall try to find the zeroes of f on the circle $v(x) = r$. Let us assume that $a_\circ \neq 0$.

(i) If there exists no side of the Newton Polygon of f with slope-r, then there exists there exists one and only term of minimum valuation in $\sum a_i x^i$. For, if $v(x) = r$ and $a = v(a_i x^i) = v(a_j x^j) = \inf_k v(a_k x^k)$, then all the points A_k are above the line $Y + rX = a$ and $A_i A_j$ is a side of the Newton Polygon of slope-r. This is contrary to the hypothesis. Thus $v(f(x)) = v(a_i x^i)$ for some i and for $v(x) = r$, which implies that there is no zero of f on the circle $v(x) = r$.

(ii) If there exists a side $A_p\, A_q$ of slope-r, then there exist at least two terms of minimum valuation. Therefore there may to be a zero of f on the circle $v(x) = r$. Assume that $p < q$. Let $v(x_\circ) = r$ for some $x_\circ$ in K and $c = v(a_q x_\circ^p) = v(a_q x_\circ^q)$. Consider the power series

$$f_1(y) = a_q^{-1} x_\circ^{-q} f(x_\circ y) = \sum b_i y^i$$

Obviously $v(b_p) = v(b_q) = 0, v(b_i) \geq 0$ for $i \neq p, q$ and $v(y) = 0$ whenever $v(x) = r$. Hence without loss of generality we can take $r = 0, v(a_p) = v(a_q) = 0, v(a_i) > 0$ for $i < o$ and $i < p$ and $i > q$ and $a_q = 1$. Therefore

$$\overline{f(x)} = x^q + \cdots + \overline{a_p} x^p \qquad = x^p (x^{q-p} + \cdots + \overline{a}_p) \text{ where } a_p \neq 0$$

The polynomials x^p and $(x^{q-p} + - - - + \overline{a}_p)$ satisfy the requirements of Hensel's lemma, therefore there exists a monic polynomial g of degree $q - p$ and a power series h, both with coefficients in $\mathscr{O}$, such that

$$\overline{g} = x^{q-p} + \cdots + \overline{a}_p, \overline{h} = x^p, f = gh$$

113 and the radius of convergence of h is equal to the radius of convergence of f. Let us assume that $g = x^{q-p} + \cdots + g_\circ$. Then $\overline{g_0} = \overline{a_p} \neq 0$. Let us further assume that K is an algebraically closed field. Then g has $q - p$

zeroes in K which belong obviously to $\mathscr{O}^*$. Moreover h has no zeroes on the circle $v(x) = 0$. Thus f has exactly $q - p$ zeroes on the circle $v(x) = 0$ where $q - p$ is the length o the projection of the side of the Newton Polygon of f with slope 0. If $\lambda_1, \lambda_2, \ldots, \lambda_{q-p}$ are the zeroes of f, on $v(x) = 0$ then $f = h \cdot \prod_{i=1}^{q-p} (x - \lambda_i)$. We have also proved that if f is a power series and λ is its zero on a circle $v(x) = r > \rho(f)$, then $\dfrac{f(x)}{x - \lambda}$ is also a power series with the same radius of convergence. Regarding the zeroes of f inside the circle $v(x) \geq r$ we prove the following.

Proposition 1. *The power series f has a finite number of zeroes $\lambda_1, \ldots,$ λ_k in the disc $v(x) \geq r > \rho(f)$ and there exists a power series h such that*

$$f(x) =_i \prod_{1=1}^{k} (x - \lambda_i) \cdot h(x) \text{ with } \rho(f) = \rho(h).$$

Proof. We have proved that $f(x)$ has zeroes on the circle $v(x) = r_i > \rho(f)$ if and only if there exists a side of the Newton Polygon of f of slope $-r_i$. But we know that if (m_i) is the sequence of slopes of sides of the Newton Polygon of f, then $\lim\limits_{i \to \infty} m_i = -\rho(f)$. Therefore there exist only a finite number of sides of the Newton Polygon of slope $-r_1 < -r < -\rho(f)$ i.e., there exists only a finite number of r_1 such that $r_1 > r > \rho(f)$ for which there are zeroes of $f(x)$ on $v(x) = r_1$. Hence the theorem follows. ◻

If $f(x) = \sum\limits_{i=0}^{\infty} a_i x^i$ is convergent in a disc $v(x) > r$, then we shall say 114
that f(x) is analytic $v(x) > r$.

Proposition 2. *If $f(x)$ has no zeroes in the disc $v(x) \geq r > \rho(f)$ in particular $f(0) \neq 0$, then the power series $\dfrac{1}{f(x)}$ is analytic for $v(x) > r$.*

Proof. Let us assume that $f(0) = 1$. Since f has no zeroes in $v(x) \geq r$,there exists no side of the Newton Polygon of f of slope $\leq -r$. This implies that $\dfrac{v(a_i)}{i} \geq -r$ for every i. Considering f as a formal power series over K we get

$$\frac{1}{f} = \frac{1}{1+\sum\limits_{i>0} a_i x^i} = \sum_{k=0}^{\infty} (-1)^k \left(\sum_{i=0} a_i x^i \right)^k = \sum_{j=0}^{\infty} b_j x^j$$

where $$b_j = \sum_k (-1)^k \sum_{i_1+i_2+\cdots+i_k=j} a_{i_1} \cdots a_{i_k}$$

Therefore $$v(b_j) \geq \inf_{\substack{k \\ i,+--+i_k=j}} \left(\sum_{l=1}^{k} v(a_{i1}) \right) > -\sum_{l=1}^{k} r_{il} = -r_j$$
$$\Rightarrow \frac{v(b_j)}{j} > -r.$$

Hence $\rho\left(\frac{1}{f}\right) \geq r$. □

Proposition 3. *If f is an entire function(i.e., $\rho(f) = -\infty$) and has no zeroes, then f is a constant.*

Let $f(x) = \sum_{i=0}^{\infty} a_i x^i$. As in the proof of the preceding proposition, we see that:

$$v(a_j) \geq -rj \text{ for any } r.$$

115 *Hence, we have $a_j = 0$ for $j \geq 1$.*

From these propositions, we can deduce the complete structure of entire functions:

Weierstrass' Theorem. Let K be an algebraically closed complete field with a real valuation v. Let f be an everywhere convergent power series over K. Then the zeroes of f different from zero form a sequence $(\lambda_1, \lambda_2, \ldots, \lambda_n, \ldots,)$ such that $v(\lambda_n)$ is a decreasing sequence which tends to $-\infty$ if the sequence (λ_n) is infinite and we have

$$f(x) = a_\circ x^k \prod_{i=1}^{\infty} \left(1 - \frac{x}{\lambda_i}\right) \tag{1}$$

the infinite product being uniformly convergent in each bounded subset of K. Conversely for any sequence (λ_n) such that $v(\lambda_n)$ is a decreasing sequence tending to $-\infty$ as n tends to infinity, the infinite product (1) is uniformly convergent in every bounded subset of K and defines an entire having zeros at the prescribed points λ_n.

Proof. We shall prove the latter part first. Consider

$$\varphi_N(x) = \prod_{N}^{i=1}\left(1 - \frac{x}{\lambda_i}\right) = \sum_{k=0}^{N} a_{kN} x^k,$$

where $$a_{kN} = (-1)^k \sum_{1 \le i_1 < i_2 < --- < i_k \le N} \frac{1}{\lambda_{i_1}\lambda_{i_2}\ldots\lambda_{i_k}}$$

clearly $v(a_{kN}) \geq +\left(v\left(\frac{1}{\lambda_1}\right) + \cdots + v\left(\frac{1}{\lambda_1}\lambda_k\right)\right) = \rho_k$. Since $\lim\limits_{i\to\infty} v(\lambda_i) = -\infty$, $\lim\limits_{k\to\infty} \frac{\rho k}{k} = \infty$. Let

$$\varphi(x) = \prod_{i=1}^{\infty}\left(1 - \frac{x}{\lambda_i}\right) = 1 + \sum_{k=1}^{\infty} a_k x^k, \text{ where}$$
$$a_k = \sum_{1 \le i_1 < i_2 < \cdots < i_k} \frac{1}{\lambda_{i_1}\cdots\lambda_{i_k} + \operatorname*{lt}\limits_{n\to\infty} a_{kn}}$$

(obviously the series giving a_k is convergent and $\frac{v(a_k)}{k} \geq \frac{\rho_k}{k}$). Therefore the series $\varphi(x)$represents an entire function. We have to show that the polynomials φ_N converge to φ uniformly on every bounded subset of K. Given two real numbers M and A there exists an integer q such that $v(a_{kN}x^k) \geq M$ for $k \geq q$, for all x with $v(x) \geq A$and for all N,because $\frac{\rho_k}{k} \to \infty\ as\ k \to \infty$. This implies that for any N **116**

$$v\left(\varphi_N(x) - \sum_{k=0}^{q} a_{k_N} x^k\right) \geq M \text{ for } v(x) \geq A. \tag{2}$$

Similarly we get

$$v\left(\varphi(x) - \sum_{k=0}^{q} a_{k_N} x^k\right) \geq M \text{ for } v(x) \geq A. \tag{3}$$

Since $a_{kN} \to a_K$ as N tends to infinity, combining (2) and (3) we get $v(\varphi(x) - \varphi_N(k)) \geq M$ for N sufficiently large. It can be easily proved that the λ_i are the only zeroes of the function $\varphi(x)$. ◻

Let us denote by f_1 the product given by (1). Take a disc $v(x) \geq r$. In this disc $f(x)$ has only a finite number of zeroes. Let the zeroes of f in $v(x) \geq r$ be 0(k times) and $\lambda_1, \lambda_2, \ldots \lambda_p$. Then

$$f(x) = x^k \prod_{i=1}^{p} \left(1 - \frac{x}{\lambda_1}\right) g(x)$$

where $g(x)$ has no zeroes in the disc $v(x) \geq r$. Therefore $\dfrac{1}{g}$ is analytic in the disc $v(x) > r$. Consider $\dfrac{f_1}{f} = \dfrac{g_1}{g} = \prod_{i=p+1}^{\infty} \left(1 - \frac{x}{\lambda_i}\right) \frac{1}{g}$, where g_1 is analytic and has no zeroes in the disc $v(x) > r$. Therefore $\dfrac{f_1}{f} is$ analytic in the disc $v(x) > r$ and has no zeroes in it. Since it is true for every r, $\dfrac{f_1}{f}$ is a constant function. Hence our theorem is proved.

Form the proposition 2, we can derive some properties of the meromorphic functions:

117 **Definition.** A power series $\varphi = \sum\limits_{i=-m}^{\infty} a_i x^i$ over a field K is said to be a meromorphic function in a disc $v(x) \geq r$ if and only if there exist two functions f and g analytic in the same disc such that $\varphi = \dfrac{f}{g}$.

In any disc $v(x) \geq r' > r, g$ has a finite number of zeroes, therefore $g = Pg'$ where P is a polynomial and g' has no zeroes $v(x) \geq r'$ which means that $\frac{1}{g'}$ is analytic in $v(x) > r'$. Therefore we can can write $\varphi = \dfrac{f'}{P}$, where $f' = f\dfrac{1}{g'}$ is a convergent power series in $v(x) > r'$.

3 Criterion for the Rationality of power-series

Let F be any field and $f = \sum_{k=0}^{\infty} a_k x^k$ an element in $F[[x]]$. It can be easily proved that f is a rational function if and only if there exists a finite sequences $(q_i)_{\circ \leq i \leq h}$ of elements of F at least one of which is non-zero and an integer k such that

$$a_n q_h + a_{n+1} q_{h-1} + \cdots + a_{n+h} q_o = 0$$

for all integers n such that $n + h > k$. Let us denote by A_n^{h+1} the determinant of the matrix $(a_{n+i+j})_{0 \leq i, j \leq h}$.

Lemma 1. The power series f is a rational function if and only if there exists integer h and $n_\circ$ such that $A_n^{h+1} = 0$ for all $v > n_\circ$.

Proof. It is obvious that the condition is necessary. We shall prove that the condition is sufficient by induction on h. When $h = 0$, we have $a_n = 0$ for n sufficiently large. Therefore f is actually a polynomial. Let us assume that $A_n^{h+1} = 0$ for $n > n_\circ$. Moreover we may assume that $A_n^h \neq 0$ for infinitely many n, because if $A_n^h = 0$ for n large then by induction hypothesis we get that f is a rational function. Since $A_n^{h+1} = 0$ **118**
for $n > n_\circ, A_n^h\, A_{n+2}^h = \left(A_{n+1}^h\right)^2$. So it follows that $A_n^h \neq 0$ for $n > n_\circ$. Consider the following system of linear equations

$$E_r = a_{n_\circ + r} x_1 + a_{n_\circ + 1 + r} x_2 + \cdots + a_{n_\circ + h + r} x_{h+1} = 0 \text{ for } r = 0, 1, 2, \ldots$$

For any $q \geq n_\circ$ the system $\sum_q$of the h if h equations $E_q, E_{q+1}, \ldots E_{q+h-1}$ is of rank h (because $A_q^h \neq 0$). So has a unique solution upto a constant factor. But the system $\sum_q'$ of the $h + 1$ equations $E_q, \ldots, E_{q+h}$ is also of rank h (because $A_{q+1}^h \neq 0$ and $A_q^{h+1} = 0$) and therefore $\sum_q'$ and $\sum_{q+1}$ on the hand and $\sum_q'$and $\sum q + 1$ on the other hand have the same solution. Thus any solution of $\sum_q$ is a solution of $\sum_{q+1}$ and any solution of $\sum_{n_o}$ is a solution of E_q for $q \geq n_\circ$. Thus we have found a finite sequence (x_i) such that $a_{n_\circ + r} x_1 + \cdots + a_{n_\circ + h + r} x_{h+1} = 0$ for $r \geq 0$. Hence f is a rational function. □

Theorem 1. *Let $f(x) = \sum a_i x^i$ be a formal power series with coefficients in Z. Let R and r be two real numbers such that*

(1) $Rr > 1$

(2) *f considered as a power series over the field of complex numbers is holomorphic in the disc $|x| < R$.* **119**

(3) *f considered as a power series over Ω_p(the complete algebraic closure of Q_p) is meromorphic in the disc $|x| \leq r'$ with $r' > r$. (where $||_p$) is the absolute value associated to v_p). Then f is a rational function.*

Proof. We can assume that $R \leq 1$, because $R > 1$ implies that f is a polynomial and we have nothing to prove. Moreover $r > 1$, because $Rr > 1$. Since f is meromorphic in $|x|_p \leq r'$, there exist two functions g and h analytic in $|x|_p \leq r$ such that $f = \frac{g}{h}$. If necessary by multiplying f by a suitable power of x we can assume that f has no pole at $x = 0$ and hence that h is polynomial with $h(0) = 1$. Let

$$g \sum_{i=0}^{\infty} g_i x^i \text{ and } h = \sum_{i=0}^{k} h_i x^i$$

$$g_{n+k} = a_n h_k + a_{n+1} h_{k-1} + \cdots a_{n+k-1} h_1 + a_{n+k} \tag{1}$$

By Cauchy's inequality we obtain the following

(1) $|a_s| \leq MR^{-s}$

(2) $|g_s| \leq Nr^{-s}$

By taking R and r smaller if necessary we assume that $|a_s| \leq R^{-s}$ and $|g_s|_p \leq r^{-s}$ for $s > s_\circ$. Let

$$A_n^{m+1} = \begin{vmatrix} a_n & a_{n+1} \cdots & a_{n+k} & a_{n+m} \\ a_{n+1} & a_{n+2} & a_{n+k+1} & a_{n+m+1} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n+m} & a_{n+m+1} & a_{n+m+k} \cdots & a_{n+2m} \end{vmatrix}$$

where $m > k$.

120 The equation (1) gives

$$A_n^{m+1} = \begin{vmatrix} a_n & a_{n+1} \cdots & a_{n+k-1} & g_{n+k} & g_{n+m} \\ a_{n+1} & a_{n+2} & a_{n+k} & a_{n+k+1} & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n+m} & a_{n+m+1} & a_{n+m+k-2} & g_{n+m-k} & r_{2+2m} \end{vmatrix}$$

Obviously for $n > s_o$ we have

$$|A_n^{m+1}| \leq (m+1)!(R^{-(n+2m)})^{m+1}$$

and

$$|A_n^{m+1}|_p \leq (r^{-n})^{m-k+1}$$

because $|a_n|_p \leq 1$ for every n. If $A_n^{m+1} \neq 0$, then

$$1 \leq |A_n^{m+1}||A_n^{m+1}| \leq (m+1)!R^{-2m(m+1)}r^{kn}[Rr]^{-n(m+1)} = k_1[(R\,r)^{m+1}r^{-k}]^{-n}$$

Let m be so chosen that $(Rr)^{m+1}r^{-k} > 1$. Then there exists an integer $n_\circ$ such that for $n > n_\circ$

$$|A_n^{m+1}||A_n^{m+1}| < 1.$$

This is a contradiction. Therefore $A^{m+1} = 0$ for $n > n_\circ$. Hence f is a rational function. □

Corollary. *If f is a power series over Z such that f has a non-zero radius of convergence considered as series over the complex number field is meromorphic in Ω_p, then f is a rational function.*

4 Elementary Functions

We consider the convergence of the exponential logarithmic and binomial series in this section. We assume that the field K is of characteristic 0 and the real valuation v on Q induces a p-adic valuation. **121**

The exponential series $e(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$. Converges in the disc $v(x) > \frac{1}{p-1}$ and in the domain of convergence $v(e(x)-1) = v(x)$. Let $n = a_\circ + a_1 p + \cdots + a_r p^r$ where $p^r \leq n \leq p^{r+1}$ and $0 \leq a_i \leq p-1$. One can easily prove that

$$v(n!) = \left[\frac{n}{p}\right] + - - - + \left[\frac{n}{p^r}\right] = \frac{n - S_n}{p-1}$$

where $S_n = \sum_{i=0}^{r} a_i$ Therefore

$$\therefore \frac{v(\frac{1}{n!})}{n} = \frac{-1}{p-1} + \frac{S_n}{n(p-1)}$$

But $\dfrac{S_n}{p-1} \leq \left(\dfrac{\log\ n}{\log p} + 1\right)$. Therefore $\lim\limits_{n\to\infty} \dfrac{v\left(\frac{1}{n!}\right)}{n} = \dfrac{-1}{p-1}$. Hence the series $e(x)$ converges for $v(x) > \dfrac{1}{p-1}$. If $v(x) = \frac{1}{p-1}$, then $\dfrac{v(x^n)}{n!} = \dfrac{1}{p-1} < \infty$ whenever n is a power of p. Thus the series does not converge for $v(x) = \dfrac{1}{p-1}$. The latter part of the assertion is trivial. We see immediately that $e(x+y) = e(x).e(y)$ and $e(x)$ has no zeroes in the domain of convergence.

We define $\log\,(1+y) = \sum\limits_{k=1}^{\infty}(-1)^{k-1}\dfrac{y^k}{k}$ as a formal power series over
122 K. We shall show that the series $\log(1+y)$ converges for $v(y) > 0$ and $v(\log(1+y)) = v(y)$ for $v(y) > \dfrac{1}{p-1}$ we have

$$v\left(\frac{(-1)^n y^n}{n}\right) = nv(y) - v(n)$$

But $v(n) \leq \dfrac{\log n}{\log p}$ therefore $v\left(\dfrac{(-1)^n y^n}{n}\right)$ tends to infinity as $n \to \infty$ whenever $v(y) > 0$. On the other hand $v(n) = 0$ if $(n,p) = 1$, therefore the series is not convergent for $v(y) \leq 0$. For $n > 1$ and $v(y) > \dfrac{1}{p-1}$, it can easily proved that $v\left(\dfrac{(-1)^{n-1}y^n}{n}\right) > v(y)$, which proves our last assertion. Moreover for $v(x) > \dfrac{1}{p-1}$ we have the equalities

$$e(\log(1+x)) = 1 + x \tag{1}$$
$$\log(e(x)) = x \tag{2}$$

Let

$$G = \left\{x | x \in K, v(x) > \frac{1}{p-1}\right\}$$
$$G = \left\{x + 1 | x \in K, v(x) > \frac{1}{p-1}\right\}$$

be subgroups of K_+ (the additive group of K) and K^* respectively. The mapping $x \to e(x)$ is an isomorphism of G onto G', the inverse of which is the mapping $1 + x \to \log(1 + x)$. In fact the mapping $1 + y \to \log(1+7)$ is a homomorphism of the group $1+\mathscr{Y}_\Omega$(Ω begin the complete algebraic closure of K) into the subgroup of Ω_+, where $v(y) > 0$.It is not an isomorphism because it ζ is a $p{-}th$ root of unity, then $v(\zeta - 1) = \dfrac{1}{p-1}$ and $\log \zeta = 0$.

We define $(1 + Y)^Z = \sum\limits_{m=0}^{\infty} h(m, Z)Y^m = e(Z \log(1 + Y))$ where $h(m, Z) = \dfrac{Z(Z-1)\cdots(Z-m+1)}{m!}$ as a formal power series in the variables Y and Z over K. Since h(m,Z) is a polynomial in Z, we can substitute for Z any element of K to get a power series in the one variable Y.

Proposition 4. *For any element t in K the power function* $(1+x)^t$ *defined above is analytic for* $v(x) > \dfrac{1}{p-1}$ *(respectively for* $v(x) > -v(t) + \dfrac{1}{p-1}$*) if* $v(t) \geq 0$ *(respectively if* $v(t) < 0$*) Moreover if t belongs* Z_p*, then* $(1+x)^t$ *is analytic for* $v(x) > 0$. **123**

Proof. When $v(t) < 0$

$$v(h(m, t)) = m(v(t)) - v(m!) \geq mv(t) - \frac{m-1}{p-1}$$

Therefore $\liminf\limits_{m\to\infty} \dfrac{v(h(m, t))}{m} = v(t) - \dfrac{1}{p-1}$ Hence $(1 + x)^t$ is analytic in $v(x) > \dfrac{1}{p-1} - v(t)$. Similarly one can prove the convergence when $v(t) \geq 0$. □

Let t be in Z_p. Then $h(m, t)$ is a p-adic integer. Suppose that $v(m!) + 1 = \alpha$, then there exists an element k_m in Z such that

$$t \equiv k_m \pmod{p^k}$$

Therefore

$$t(t-1)\ldots(t-m+1) \equiv k_m(k_m - 1)$$

or $$h(m,t) \equiv h(k_m, m) \pmod{p}.$$

But $h(k_m, m)$ is a rational integer, therefore $v(h(m,t)) \geq 0$. From this our assertion follows easily.

5 An Auxiliary Function

Throughout our discussion F_q shall denote a finite field consisting of q elements. Let us consider the infinite product

$$F(Y,T) = (1+Y)^T (1+Y^P)^{\dfrac{T^P - T}{P}} (1+Y^{P^m})^{\dfrac{T^{p^m} - T^{p^{m-1}}}{p^m}} \tag{1}$$

The product is well defined as formal power series in two variables Y and T over Q. Clearly (1) is convergent in $Q\Big[[Y,T]\Big]$. Expressing $F(Y,T)$ as a power series over $Q\Big[[T]\Big]$ and $Q\Big[[Y]\Big]$ we obtain

$$\begin{aligned} F(Y,T) &= \sum_{m=0}^{\infty} B_m(T) Y^m, d(B_m(T)) \leq m \\ &= \sum_{m=0}^{\infty} \alpha_m(Y) T^m, \end{aligned}$$

124 where $\alpha_m(Y)$ is a power series, the terms being of degree $\geq m$.

Lemma 2. The coefficients of $F(T,Y)$ are p-adic integers.

Lemma 3. If F is an element of $Q\Big[[Y,Z]\Big]$ such that $F(0,0) = 1$, then F belongs to $Z_p\Big[[Y,Z]\Big]$ if only if the coefficients of $\dfrac{(F(Y,Z))^p}{F(Y^p, Z^p)}$ are in pZ_p excepts for the first.

Proof of Lemma 3. Let us suppose that $F(Y,Z) = 1 - \sum\limits_{i+j>0} a_{ij} Y^i Z^j$, then

$$G = \frac{(F(Y,Z))^p}{F(Y^p, Z^p)} = F_1 x F_2 \quad \text{where}$$

$$F_1 = 1 - p \sum_{i+j>0} a_{ij} y^i Z^j + \cdots + \binom{p}{r}(-1)^r \left(\sum_{i+j>0} a_{ij} Y^i Z^j \right)^r$$

$$+ \cdots + (-1)^p \left(\sum_{i+j>0} a_{ij} Y^i Z^j \right)^p .$$

$$F_2 = 1 + \sum_{k=1}^{\infty} \left(\sum_{i+j>0} a_{ij} Y^{pi} Z^{pj} \right)^k$$

If $G = 1 + \sum\limits_{i+j>0} b_{ij} Y^i Z^j$, then

$b_{ij} = -pa_{ij}+$ (terms of the form pX polynomials in a with rational integers coefficients with

$$r + s < i + j) + \sum_{k=1}^{\infty} \sum_{\substack{i_1 + \cdots + i_k = i' \\ j_1 + \cdots + j_k = j' \\ i_r + j_r > 0}} a_{i_1} j_1 \ldots a_{ik} j_k$$

$$+(-1)^p \sum_{k=1}^{\infty} a^p_{i_1} j_1 a_{i_2} j_2 \cdots a_{i_k} j_k i_1 + \cdots + i_k = i'$$

$$j_1 + \cdots + j_k = j'$$

$$i_r + j_r > 0$$

where the last two sums appear only if i and j are divisible by p and in **125**
this case $pi' = i, pj' = j$.

Assume that b_{ij} belongs to pZ_p for $i + j > 0$. We shall prove that a_{ij} are in Z_p by induction. Obviously a_{00} is in Z_p. Assume that $a_{rs} \in Z_p$ for $r + s < i + j$; then in the formula giving b_{ij} all the terms except perhaps $-pa_{ij}$. But $a - a^p$ belongs to pZ_p if a belongs to Z_p, therefore pa_{ij} belongs to pZ_p and a_{ij} belongs Z_p. The other part of the assertion is trivial

Proof of Lemma 2.

$$\frac{(F(Y,T))^p}{F(Y^p,T^p)} = \frac{(1+Y)^{pT}\prod\limits_{m=1}^{\infty}(1+Y^{p^m})^{\dfrac{T^{pm}-T^{p^{m-1}}}{p^{m-1}}}}{(1+Y^p)^{T^p}\prod\limits_{m=2}^{\infty}(1+Y^{p^m})^{\dfrac{T^{p^m}-T^{p^{m-1}}}{p^{m-1}}}}$$

$$= \left[\frac{(1+Y)^p}{(1+Y^p)}\right]^T$$

$$= \left[a + p\sum_{k=1}^{\infty} b_k Y^k\right]^T$$

where b_k are p-adic integers.

Moreover

$$\left(1 + p\sum_{k+1}^{\infty} b_k Y^k\right)^T = \sum_{m=0}^{\infty} h(m,T)p^m \left(\sum_{k=1}^{\infty} b_k Y^k\right)^m$$

But $\dfrac{v(p^m)}{m!} \geq m - \dfrac{m-1}{p-1} > 0$, therefore $\dfrac{F(Y,T)}{F(Y^p,T^p)}^{p} - 1$ has its coefficients in pZ_p. Thus by lemma (3) the coefficients of $F(Y,T)$ are p-adic integers.

126 One deduces from lemma (2) that $F(y,t)$ is analytic for $v(t) \geq 0$ and $v(y) > 0$, because if $v(t) \geq 0$, then $v(B_m(t)) \geq 0$ because $B_m(t)$ is a polynomial with coefficients from Z_p. Therefore the series $\sum\limits_{m=0}^{\infty} B_m(t)y^m$ converges for $v(y) > 0$.

6 Factorisation of additive characters of a Finite Fields

Let $\mathscr{R}_s = \left\{x \mid x \in \Omega_p = \Omega, x^{P^s} = x\right\}$. We have the canonical map from $\mathscr{R}_2$ to F_{p^s} namely the restriction on the canonical homomorphism of $\mathscr{O}_\Omega$

onto k_Ω. In order t prove that this map is bijective, it is sufficient to prove that is surjective ; because both $\mathscr{R}_s$ and F_{p^s} have p^s elements. If $\bar{x} \neq 0$ is in F_{p^s}, then $\bar{x}^{p^s-1} - 1 = 0$ and $\bar{x}$ is a simple root of the polynomial $X^{p^s-1} - 1$. Therefore by Hensel's lemma there exists an element α belonging to Ω such that $\bar{\alpha} = \bar{x}$ and $\alpha^{p^s-1} - 1 = 0$, which proves that α is in $\mathscr{R}_2$ and the mapping is onto. Infact the canonical homomorphism of $\mathscr{O}\Omega$ onto k_Ω when restricted to $\mathscr{R} = \bigcup\limits_{s=1}^{\infty} \mathscr{R}_2$ is an isomorphism onto k_Ω. Finally Hensel's lemma shows that R_1 is contained in Q_p.

Let $U_s = Q_p(\mathscr{R}_s)$. Clearly U_s is a Galois extension of Q_p and the Galois group is cyclic generated by the automorphism $\sigma : \rho \to \rho^p$, where ρ is a primitive $p^s - 1$ th root of unity. Moreover U_s is an unramified extension of Q_p, because $[U_s; Q_p] = [F_{p^s}; F_p]$. If we take $U = \bigcup\limits_{s=1}^{\infty} U_s$, then the completion of U is the maximum unramified extension of Q_p in Ω and σ is called the Frobenius automorphism of U. If t' is an elements is $\mathscr{R}_2$, then

$$\operatorname*{Tr}_{U_s/\ Q_p} t' = t' + t'^{p} + \cdots + t'^{p^{s-1}}$$

belongs to Z_p. Thus the function $(1+Y)^{\mathrm{Tr}\, t'}$ is analytic for $v(y) > 0$. **127**
Let t' be the representative of $t \in F_{p^2}$ in $\mathscr{R}_2$. If y belongs y belongs to $\mathscr{Y}_\Omega$ then $(1+y)^{\mathrm{Tr}\, t'}$ belongs to Ω. We shall choose y in such a way that mapping $t \to (1+y)^{\mathrm{Tr}\, t'}$ is a character of the additive group of F_{p^s}. Obviously for any u and v in F_{p^s} we have

$$\begin{aligned} (u+v)' &\equiv u' + v' \pmod{\mathscr{Y}_\Omega} \\ \mathrm{Tr}(u'+v') &\equiv \mathrm{Tr}\, u' + \mathrm{tr}\, v' \pmod{\mathscr{Y}_\Omega} \\ &\equiv \mathrm{Tr}\, u' + \mathrm{Tr}\, v' \pmod{pZ_p} \end{aligned}$$

because $\mathrm{Tr}\, u'$ is a p-adic integer. Therefore

$$(1+y)^{\mathrm{tr}(u+v)'} = (1+y)^{\mathrm{Tr}\, u'}(1+y)^{\mathrm{Tr}\, v'}(1+y)^{a},$$

where a belongs to pZ_p. Let us take $1 + y = \zeta$ where $\zeta^p = 1$ and $\zeta \neq 1$. It follows that $(1+y)^a = 1$. Thus the mapping $u \to \zeta^{\mathrm{Tr}\ u'}$ is a character of F_{P^s}. We shall show that it is a non -trivial character. Firstly, $\zeta^a = 1$ if and only if a belongs to pZ_p proved that a already belongs to Z_p. For by choice of y we have $v(y) = \dfrac{1}{p-1} > 0$ and

$$\zeta^a = (1+y)^a = 1 + ay + \cdots + h(m,a)y^m + \cdots$$

Since a is p-adic integer, $v(h(m,a) \geq 0$ and hence $v(h(m,a)y^m \geq \dfrac{2}{p-1}$ for $m \geq 2, (a+y)^a \neq 1$ if $v(ay) < \dfrac{2}{p-1}$. Therefore $v(ay) \geq \dfrac{2}{p-1}$, which implies that $v(a) \geq \dfrac{1}{p-1} < 0$, thus a belongs to pZ_p. But the canonical image of $\operatorname{Tr} u'$ in F_p is the trace of u as an element of F_{p^s} over F_p, therefore there exists as least one u' such that $\operatorname{Tr} u'$ is not in pZ_p. Hence the mapping $u \to \zeta^{\operatorname{Tr} u'}$ is a non-trivial character of F_{p^s}. By definition of the product $F(Y,T)$ we have

$$F(y,u') = (1+y)^{u'} \cdots (1+y^{p^m})^{\dfrac{u'^{p^m} - u'^{p^{m-1}}}{p^m}}$$

$$F(y,u'^p) = (1+y)^{u'p} \cdots (1+y^{p^m})^{\dfrac{u'^{p^{m+1-}} - u'^{p^m}}{-p^m}}$$

$$F(y,u'^{p^{s-1}}) = (1+y)^{u'^{p^{g-1}}} \cdots (1+y^{p^m})^{\dfrac{u'^{p^{m+s-1}} - u'^{p^{m+s-2}}}{p^m}}$$

128 Since $u'^{p^s} = u'$, by multiplying these identities we get

$$\prod_{r=0}^{s-1} F(y,u'^{p^r}) = (1+y)^{\operatorname{Tr} u'}$$

Thus $\zeta^{\operatorname{Tr} u'} = \prod\limits_{k=0}^{s-1} \varphi(u'^{p^k})$ where $\varphi(T) = F(\zeta-1,T)$, is the splitting of additive characters of F_{p^s} which we shall require later.

Chapter 6

Zeta-functions

1

It is well known that the Riemann zeta function $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$, 129
where p runs over all prime numbers, is absolutely convergent for Re $s >$. We can generalise this definition for any commutative ring with unit element . In the case of ring of integers p is nothing but the generating element of the maximal ideal (p) and it is also equal to the number of elements in the field $Z/(p)$. Motivated by this we define for any commutative ring A with identity

$$\zeta_A(s) = \prod_{\mathcal{M}} (1 - N(\mathcal{M})^{-s})^{-1} \tag{I}$$

where $\mathcal{M}$ runs over the set of all maximal ideals of A and $N(\mathcal{M})$ is the number of elements in the field $A/\mathcal{M}$. But in general $N(\mathcal{M})$ is not finite and even if $N(\mathcal{M})$ is finite the produce (I) is not convergent, therefore we have to put some more restrictions on the ring. In the following we shall prove that if A is finitely generated over Z i.e., if there exist a finite number of elements $x_1, \ldots, x_k$ in A such that the homomorphism from $Z\left[X_1, \ldots, X_k\right]$ to A which sends X_i to x_i is surjective, then $N(\mathcal{M})$ is finite and the infinite product (I) is absolutely convergent fot Re $s > \dim A$, where the dimension of A is defined as follows.

Definition. If A is an integral domain, the dimension of A is the transcendence degree (respectively transcendence degree +1) of the quotient

field of A over $Z/(p)$ (respectively Q) if characteristic of A is p (respec-
130 tively 0). In the general case $\dim A$ is the supremum of the dimension of the rings $A/\mathscr{Y}$ where $\mathscr{Y}$ is any minimal prime ideal.

It can be proved that dimension of A is equal to the supremum of the lengths of strict maximal chains of prime ideals. Before proving the convergence of the zeta function we give some examples of finitely generated rings of over Z.

1. The ring Z is finitely generated over itself.

2. Any finite field F_q.

3. The ring of polynomials in a finite number of variables over F_q i,e., the ring $F_q[X_1, \ldots, X_k]$

4. The ring $F_q[X_1, \ldots, X_r]/\mathscr{U}$, where $\mathscr{U}$ is any prime ideal of $F_q[X_1, \ldots, X_r]$. This is the set of regular functions defined over F_q on the variety V defined by the ideal $\mathscr{U}$ affine space.

5. Let K be any algebraic number field. The ring of integers A in K is finitely generated over Z.

6. Let V be an affine variety defined over the algebraic number field K and let $\mathscr{O} \subset K[X_1, \ldots, X_r]$ be the ideal of V. Then the ring of regular functions on V i.e., $K[X_1, \ldots, X_r]/\mathscr{O}$ is not finitely generated over Z. But the ideal $\mathscr{O}$ is generated by the ideal $\mathscr{O}_0 = \mathscr{O} \cap A[X_1, \ldots, X_r]$ of the ring $A[X_1, \ldots, X_r]$ and we can associate to V the quotient ring $A[X_1, \ldots, X_r]/\mathscr{O}$ which is obviously finitely generated over Z. It is to be noted that this ring is not intrinsic and depends on the choice of the coordinates in K^r

2 Fields of finite type over Z

We shall require the following lemma in the course of our discussion.
131 **Normalisation lemma of Noether.** Let K be a field. Let R and S be subrings of K containing a unit elements such that S is finitely generated

over R. Then there exists an elements $a \neq 0$ in R and a finite number pf element $X_1, \ldots, X_r$ in S such that

1. $X_1, \ldots, X_r$ are algebraically independent over the quotient fields of R.

2. Any elements of S is integer over $R[a^{-1}, X_1, \ldots, X_r]$.

Proposition 1. *Let K be a field. Let R be a subring of K and L the quotient field of R. If K as a ring is finitely generated over R, then $(K : L)$ is finite and there exists an element a in R such that $L = R[a^{-1}]$.*

We first prove the following: If a field K is integral over a subring R then R is a field.

Let x be any element of R, then x^{-1} belongs to K and therefore satisfies an equation

$$X^n + a_1 X^{n-1} + \cdots + a_n = 0, a_i \in R$$

This implies that x^{-1} is a polynomial in x over R. But $R[x] = R$, therefore x^{-1} belongs to R. Hence R. Hence R is a field

Proof of proposition 1. Since K is finitely generated over R, by the normalisation lemma, there exists an element $a \neq 0$ in R and a finite family $(x_1, \ldots, x_r)$ in K algebraically independent over L such that K is integral over $R[a^{-1}, x_1, \ldots, x_r]$. By the remark above it follows that $R[a^{-1}, x_1, \ldots, x_r]$ is a field. But $x_1, \ldots, x_r$ are algebraically independent over L, therefore $r = 0$ and $L = R[a^{-1}]$. Since K is finitely generated and integral over $L, (K : L)$ is finite.

Proposition 2. *If a commutative ring A is finitely generated over Z, then $W\mathfrak{N}(\mathfrak{M})$ is finite for any maximal ideal $\mathfrak{M}$ of A.*

Proof. Since A is finitely generated over Z, the field $K = A/\mathfrak{M}$ is finitely **132**
generated over Z. If characteristic of K is zero then K contains Z. Therefore by proposition (1) $Q = Z(a^{-1})$ for some $a \neq 0$ and a in Z, which is impossible. Thus characteristic of K is p and by proposition (1) K is a finite extension of F_p, hence K is a finite field. □

3 Convergence of the product

Proposition 3. *The infinite product $\zeta_A(s)$ is a absolutely convergent for Re $s > \dim A$ and uniformly convergent for Re $s > \dim A + \varepsilon$ for every $\varepsilon > 0$.*

Proof. We shall prove the result by induction on $r = \dim A$. If $r = 0$ then A is a finite field. Let us assume that $A = F_q$. Then

$$\zeta_A(s) = \frac{1}{1 - q^{-s}}$$

is a meromorphic function in the plane with a simple pole at $s = 0$. Let us assume that the result is true for all those rings which are finitely generated over Z and dimension of which are less than r. Before proving the result for rings of dimension r we prove the following result. □

Let A be a finitely generated ring over Z and $B = A[X]$, the ring of polynomials in one variable over A, then $\zeta_B(s) = \zeta_A(s-1)$ in a suitable domain of convergence. In fact if $\zeta_A(s)$ is convergent for Re $s > x$, then $\zeta_B(s)$ is convergent for Re $s > x + 1$.

If dim $A = 0$, then $A = F_q$ for some q and $B = F_q[X]$. Since he maximal ideals in B are generated by irreducible polynomials, which can be assumed to be monic, we get

$$\zeta_B(s) = \prod_P (1 - q^{sd(p)})^{-1}$$

133 where P runs over the set of monic irreducible polynomials over A. In order to prove the absolute convergence of $\zeta_B(s)$, it is sufficient to prove the convergence of the infinite series

$$S = \sum_P \left| q^{-d(P)} \right|^{\sigma} \text{ where } s = \sigma + it$$

Since the number of monic polynomials of degree r is q^r, we have

$$S = \sum_P |q^{-d(P)}|^{\sigma} \leq \sum_{r=1}^{\infty} q^r |q^{-r}|^{\sigma}$$

$$= \sum_{r=1}^{\infty} q(1-\sigma)r$$

Obviously the series S is convergent if $1-\sigma < 0$ i.e., $\sigma > 1$. Moreover in this domain

$$\zeta_B(s) = \sum_{Q} \frac{1}{q^{sd(Q)}} \text{ (}Q\text{ a monic polynomial in}B\text{)}$$
$$= \sum_{k=0}^{\infty} \frac{q^k}{q^{sk}} = \sum_{k=0}^{\infty} \frac{1}{q^{k(s-1)}} = \frac{1}{1-q^{1-s}}$$

Hence

$$\zeta_B(s) = \zeta_A(s-1).$$

Now let the dimension of A be arbitrary and $B = A[X]$.

We shall denote by $\mathrm{Spm}(B)$ the set of maximal ideals of B. For any $\mathfrak{M}$ in $\mathrm{Spm}(B), \mathfrak{M} \cap A$ is in $\mathrm{Spm}(A)$, because $A/\mathfrak{M} \cap A$, being a subring of the finite field $B/\mathfrak{M}$, is a field. Let π denote the mapping $\mathfrak{M} \in \mathrm{Spm}(B) \longrightarrow \mathfrak{M} \cap A \in \mathrm{Spm}(A)$. It can be easily proved that the set $\pi^{-1}\mathfrak{N}$ and $\mathrm{Spm}(A/\mathfrak{N}[X])$ are isomorphic, where $\mathfrak{N}$ is any maximal ideal of A. Therefore

$$\zeta_B(s) = \prod_{\mathfrak{M} \in \mathrm{Spm}(B)} [1-(N(\mathfrak{M}))^{-s}]^{-1}$$
$$= \prod_{\mathfrak{N} \in \mathrm{Spm}(A)} \prod_{\mathfrak{M} \in \pi^{-1}(\mathfrak{N})} (1-N(\mathfrak{M})^{-s})^{-1}$$
$$= \prod_{\mathfrak{N} \in \mathrm{Spm}(A)} \zeta_{A/\mathfrak{M}}[X]^{(s)}$$

134

But $A/\mathfrak{N}$ is a finite field, therefore $\zeta_{A/\mathfrak{N}[X]^{(s)}} = \zeta_{A/\mathfrak{N}}(s-1)$
So we get

$$\zeta_B(s) = \prod_{\mathfrak{N} \in \mathrm{Spm}(A)} (\zeta_{A/\mathfrak{N}}(s-1))$$
$$= \prod_{\mathfrak{N} \in \mathrm{Spm}(A)} (1-N(\mathfrak{N})^{1-s})^{-1}$$

$$= \zeta_A(s-1).$$

It follows that $\zeta_{F_q}(s)_{[X_1,\ldots,X_k]} = \dfrac{1}{1-q^{k-s}}$ and $\zeta_{Z[X_1,\ldots,X_K]} = \zeta_Z(k-s)$ where ζ_Z is nothing but the Riemann zeta function.

Now we shall prove our main proposition. Assume that A is an integral domain.

Let K be the quotient field and R the prime ring of A.

Since A is finitely generated over R, by the normalisation lemma we have the following:

(1) If characteristic $A = p \neq 0$, then there exist r elements $x_1, x_2, \ldots,$
135 x_r in A such that A is integral over $R[x_1, \ldots, x_r]$, where $x_1, \ldots, x_r$ are algebraically independent over $R = F_p$. (ii)- If characteristic $A = 0$, then there exits an element a in $R = Z$ and $r-1$ elements $x_1, \ldots, x_{r-1}$ in A such that every element of A is integral over $Z[a^{-1}, x_1, \ldots x_{r-1}]$ and the elements $x_1, \ldots, x_{r-1}$ are algebraically independent over Q.

We get r elements in the first case and $r-1$ elements in the second case because r is the dimension of A which is equal to the transcendence degree of K over F_p or transcendence degree of K over $Q+1$ according as the characteristic of A is non-zero or not. It can be proved that A (respectively $A' = A(a^{-1})$) is a finite module over $B = F_p[x_1, \ldots, x_r]$ (respectively $B' = Z[a^{-1}, x_1, \ldots, x_{r-1}]$) and the mapping π from $\mathrm{Spm}(A) \to \mathrm{Spm}(B)$ (respectively from $\mathrm{Spm}(A') \to \mathrm{Spm}(B')$) is onto. Let A (respectively A') be generated by k elements as a B (respectively B') module. We shall prove that $\pi^{-1}(\mathfrak{N})$ for any $\mathfrak{N}$ in $\mathrm{Spm}(B)$ (respectively in $\mathrm{Spm}(B')$) has at most k elements. Let $C = A/A\mathfrak{N}$. It is an algebra of rank $t \leq k$ over $B/\mathfrak{N}$. Since $\pi^{-1}(\mathcal{M})$ is isomorphic to $\mathrm{Spm}(A/A\mathfrak{N})$ it is sufficient to prove that C has at most k maximal ideals. This will follow from the following.

Lemma II. *Let A be any commutative ring with identity and $(\mathcal{U}_{i_{1\leq i\leq m}}$ a finite set of prime ideals in A such that*

$$A = \mathcal{U}_i + \mathcal{U}_j \text{ for } i \neq j$$

Then the mapping $\theta : A \to P =_i \prod_{i=1}^{m} A\mathcal{U}_i$ is surjective

Proof. It is sufficient to prove that $1 = \sum_{i=1}^{m} a_i$ where a_i belongs to $\mathcal{U}_j$ for **136**
$j \neq i$ because if $(t_1, \ldots, t_m)$ is any element of P, then

$\theta\left(\sum_{i=1}^{m} t_i' a_i\right) = (t_1, \ldots, t_m)$, where t_i' is a representative of t_i in A.

If $m = 2$, the result is obvious i.e., $1 = a_1 + a_2$ where a_1 is in $\mathscr{O}_2$ and a_2 is in $\mathscr{O}_1$. Let us assume that it is true for less than m ideals.

Then $1 = \sum_{i=1}^{m-1} v_i$ where $v_i \in \mathscr{O}_j$ for $1 \leq j \leq m-1$ and $j \neq i$. Since $A = \mathscr{O}_i + \mathscr{O}_m$, we have $1 = x_i + y_i$ for $1 \leq i \leq m-1$ with $x_i \in \mathscr{O}_m$ and $\mathscr{Y}_i \in \mathscr{O}_i$. Clearly $\sum_{i=1}^{m-1} x_i v_i + \sum_{i=1}^{m-1} v_i y_i = 1$.

Let us take $u_i = v_i x_i$ for $i \leq i \leq m-1$ and $u_m = \sum_{i\ 1}^{m-1} y_i v_i$, then $\sum_{i=1}^{m} u_i = 1$ and $u_i \in \mathscr{O}_j$ for $j \neq i$. □

Let $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_t$ be any finite set of distinct maximal ideals of C. Then by lemma (1) $C/_i \bigcap_{i=1}^{t} \mathfrak{M}_i$ is isomorphic to $\bigoplus_{i=1}^{t} C/\mathfrak{M}_i$($\oplus$ indicates the direct sum). Thus $t \leq k$.

Assume that the characteristic of A is 0. Let $\mathfrak{M}$ be any maximal ideals of A. If a does not belong to $\mathfrak{M}$, then $\mathfrak{M}A[a^{-1}]$ is a maximal ideal in $A[a^{-1}]$, because $A[a^{-1}]/\mathfrak{M}A[a^{-1}]$ is isomorphic to $A/\mathfrak{M}$. If a belongs to $\mathfrak{M}$, then $\mathfrak{M}$ contains one and only one prime P_i occurring in the unique factorisation of a and the set of maximal ideals which contains p_i. is isomorphic to $\operatorname{Spm}(A/p_iA)$. Therefore if $a = p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$, then

$$\zeta_A(s) = \zeta_{A[a^{-1}]}(s) \prod_{i=1}^{t} \zeta_{A/p_iA}(s)$$

But $\dim A/p_iA < \dim A$, therefore inorder to prove the convergence **137**
of $\zeta_A(s)$ it is sufficient to consider $\zeta_{A[a^{-1}]}(s)$. We have

$$\zeta_{A[a^{-1}]}(s) = \prod_{\mathfrak{N}\ \operatorname{Spm}(B')} \prod_{\mathfrak{N} \in^{-1} \pi(\mathfrak{N})} (1 - (N\mathfrak{M})^{-s})^{-1}$$

Since $N(\mathcal{M}) \geq N(\mathcal{M})$, we get

$$\sum_{\mathfrak{N} \in \operatorname{Spm}(B)} \sum_{\mathfrak{N} \in \pi^{-1}(\mathcal{M})} |N\mathcal{M}|^{-\sigma} \leq k \sum_{\mathfrak{N} \in \operatorname{Spm}(B')} |N\mathfrak{N}|^{-\sigma} \leq k\zeta_z(r - \sigma - 1)$$

Therefore $\zeta_{A[a^{-1}]}(s)$ is convergent for $\mathfrak{R}s > \dim A$.

If characteristic $A = p$, then we get

$$\sum_{\mathfrak{N} \in \operatorname{Spm}(B)} \sum_{\mathfrak{M} \in \pi^{-1}(\mathfrak{N})} |N\mathcal{M}|^{-\sigma} \leq k \sum_{\mathfrak{N} \in \operatorname{Spm}(B')} |N\mathfrak{N}|^{-\sigma} \leq k\zeta_{F_p}(r - s)$$

which gives the same result as above, Now we have to prove our theorem in the general case(A is not an integral domain). But we shall prove in the next § a more general result.

4 Zeta Function of a Prescheme

Let A be a commutative ring with unity. We shall denote by $\operatorname{Sp}(A)$ the set of all prime ideals of A. On $\operatorname{Sp}(A)$ we define a topology by classifying the sets $F(\mathscr{O})$ as closed sets, where

$$F(\mathscr{O}) = \{\mathscr{Y} | \mathscr{Y} \supset \mathscr{O}, \mathscr{Y} \in \operatorname{Sp}(A)\}.$$

and $\mathscr{O}$ is any ideal in A. This topology is referred to as the Jacobson Zariski topology. It is obvious that in this topology a point is closed if and only if it is a maximal ideal of A. We associate with every point $\mathscr{Y}$ of $\operatorname{Sp}(A)$ a local ring A namely the ring of quotient of A with respect to
138 the multiplicatively closed set $A - \mathscr{Y}$. On $\mathscr{O}$ the sum of all these local rings we define a sheaf structure by giving“sufficiently many” sections. For any $a, b, \in, A$ we consider the open subset

$$V(b) = \{\mathscr{Y} | \mathscr{Y} \in \operatorname{Sp}(A), \mathscr{Y} \not\ni b\}.$$

For any $\mathscr{Y} \in v(b), \left(\dfrac{a}{b}\right)_{\mathscr{Y}}$ the, fraction $\dfrac{a}{b}$, is an element of $A_{\mathscr{Y}}$. Then the mapping $\mathscr{Y} \to \left(\dfrac{a}{b}\right)_{\mathscr{Y}}$ gives a section $S(a, b)$ of $\mathscr{O}$. The pair $(X, \mathscr{O})$ together with the sheaf of local rings $\mathscr{O}$ is called an *affine scheme*, where $X = \operatorname{Sp}(A)$.

Definition. Let $(X, \mathscr{O})$ be a ringed space. We say that X is a prescheme if every point has an open neighbourhood which is isomorphic as a ringed space to $\mathrm{Sp}(A)$ for some ring A. Such a neighbourhood is called an affine neighbourhood.

We shall assume that the pre-scheme X satisfies the ascending chain condition for open sets, then X is quasi-compact and it can be written as the union of a finite number of affine open sets X_i. We shall denote by A_i the ring such that X_i is isomorphic to $\mathrm{Sp}(A_i)$. Then the ring A_i is Noetherian and has a finite number of minimal prime ideals $\mathscr{Y}_{ij}$. Each prime ideal of A_i contains a $\mathscr{Y}_{ij}$ and $X_i = \mathrm{Sp}(A_i)$ is the union of the $s_{ij} = \mathrm{Sp}(A_{ij})$ (with $A_{ij}) = A_i/\mathscr{Y}_{ij})$, each S_{ij} being a closed subset of X_i and the A_{ij} being integral domains. Moreover the residue field of the local ring associated to a point $x \in S_{ij}$ is the same for the sheaf of the scheme X and for the sheaf of the scheme $\mathrm{Sp}(A_{ij})$

We define the dimension of X as the maximum of the dimensions of the rings A_i(or of the rings A_{ij}). It can be proved that if X is irreducible (i.e. if X cannot be represented as union of two proper closed subsets). then $A_i = \dim A_j$ for $i \neq j$.

A prescheme S is a finite type over Z if there exists a decomposition of S into a union of a finite number of open affine sets X_i such that each 139
A_i, the ring associated to X_i, is finitely generated over Z. It can be proved that the same is true for any decomposition into a finite number of affine open sets. In particular, a ring A is finitely generated over Z if and only if the scheme $\mathrm{Sp}(A)$ is of finite tyte over Z and an open prescheme of S is also of finite type over Z.

Let S be a prescheme of finite type over Z. A point $x \in S$ is *closed* if and only if the residue field of the local ring of x is *finite* (we shall denote by $N(x)$) the number of elements of this field). In particular, if $S = UX'_i$, then a point $x \in X_i$ is closed in S if and only if it is closed in X_i Now we define the ζ-function of S by:

$$\zeta_S(s) = \prod (1 - (N(x))^{-s})^{-1}$$

where x runs over the set of closed points of S. It is clear that if $S = S_P(A)$, then $\zeta_S = \zeta_A$. As above, we can write S as a union of a finite number of subsets S_i, each S_i being affine open subset, with

$S_i = \mathrm{Sp}(A_i)$, where A_i is an integral domain finitely generated over Z. Then it is obvious that:

$$\zeta_S = \frac{\left(\prod_{\pi} \zeta_{S_i}\right)\left(\prod_{i<j<k} \zeta_{s_i \cap S_j \cap S_k}\right)\cdots)}{\left(\prod_{i<j} \zeta_{S_i \cap S_j}\right)\cdots} \tag{I}$$

Now we shall prove the following generalisation of the Theorem 1 bis:- *The ζ function of a prescheme S of finite type over Z is convergent for Re $s > \dim S$.*

Of course, theorem 1 bis implies theorem 1. Assume we have proved the theorem 1 bis for prescheme of dimension $< \dim S$. Then we get as in the preceding § the convergence of ζ_A for any integral domain A finitely generated over Z of dimension $\leq \dim S$, and in particular the
140 convergence of the $\mathcal{Z}_{S_i}$. After (I), we have just to prove this: if U (resp. F) is an open (resp. closed) subset of $X = \mathrm{Sp}(A)$ (with $\dim A \leq \dim S$), then $\zeta_{U \cap F}$ is convergent for $\mathrm{Re}(s) > \dim S$. But let $G = X - U$; we have:

$$\zeta_{\cup \cap F} = \zeta_F / \zeta_{F \cap G}$$

and $F \cap G$ is closed in X. Hence we have just to prove the convergence of ζ_F. But F is defined by an ideal of A and $F = \mathrm{Sp}(A/\mathscr{O})$ and $\zeta_F = \zeta_{A/\mathscr{O}}$. If $\mathscr{O} = \{0\}$, we have $\zeta_F = \zeta_A$ and if $\mathscr{O} \neq \{0\}$ then the minimal prime ideals of $A/\mathscr{O}$ give non trivial prime ideals of A and we have $\dim A/\mathscr{O} < \dim S$: the induction hypothesis ensures the convergence of ζ_F. Hence we have completely proved the theorems 1 and 1 bis

5 Zeta Function of a Prescheme over F_P

Let S be a prescheme over Z of finite type. We have a canonical map from a prescheme S to $\mathrm{Sp}(Z)$ given by $\pi(x)$ = characteristics of the residue field of local ring of x for any x in S. Suppose that $\pi(x) = p$ for every x in S. In this case each A_i is of characteristic p and the canonical map from Z into A_i can be factored through F_P. In this case we say that the prescheme S is over F_P.

Let S be a prescheme of finite type over F_P. Then the residue field $k(x)$ of the local ring associated to a closed point x is of characteristic P for every x in S. Therefore $k(x) = F_{P^{d(x)}}$ where $d(x)$ is a strictly positive integer. thus

$$\zeta_S(s) = \prod_{\overline{x}=x\in S} \left(1 - p^{-sd(x)^{-1}}\right)$$

Let us take $t = p^{-s}$. Then

$$\zeta_S(s) = \prod_{\overline{x}=x\in S} \left(1 - t^{d(x)^{-1}}\right) = \overline{\zeta}_S(t).$$

The function $\tilde{\zeta}_s(t)$ is also called a zeta function on S. It is absolutely convergent in the disc $|t| < P^{-\dim(s)}$. we have **141**

$$\tilde{\zeta}_s(t) = \prod_{\overline{x}=x\in S} \sum_{k=0}^{\infty} t^{kd(x)} = \sum_{h=0}^{\infty} a_h t^h$$

with $a_0 = 1$ and $a_n \in Z$. The end of these lectures will be devoted to the proof of the following theorem (Dwork's theorem):

Theorem 1. *The function $\tilde{\zeta}_S(t)$ of a prescheme S of finite type over F_P is a rational function of t.*

6 Zeta Function of a Prescheme over F_q

In order to prove Dwork's theorem it is sufficient to prove it for an affine scheme and open sets of an affine scheme because of the equation (1). Then we have to look at thezeta function of a ring A finitely generated over F_P. Such a ring can be considered as the quotient of $F_P[X_1, \ldots, X_k]$ by some ideal $\mathscr{O}$ and we can associate to A the variety V defined by $\mathscr{O}$ in K^k where K is the algebraic closure of F_P. It may be noted that V is not necessary irreducible. We shall call ζ_A the zeta function of the variety V.

More generally we consider a variety V over F_q, where $q = p^f$. The variety V is completely determined by the ring

$A = F_q[X_1, \ldots X_n]/\mathscr{O} \cap F_q[X_1, \ldots, X_n]$ where $\mathscr{O}$ is an ideal in $K[X_1, \ldots, X_n]$ generated by $\mathscr{O}_0 = F_q[X_1, \ldots, X_n] \cap \mathscr{O}$ K being the algebraic closure of F_q. We define

$$\zeta_v = \zeta_A \text{ and } \tilde{\zeta}_v = \tilde{\zeta}_A.$$

142 For every maximal ideal $\mathfrak{M}$ of $F_q[X_1, \ldots X_n]$ there exists a maximal ideal $\mathfrak{M}$ in $K[X_1, \ldots, X_n]$ such that $F_q[X_1, \ldots, X_n] \cap \mathfrak{M}' = \mathfrak{M}$. But $\mathrm{Spm}(K[X_1, \ldots .X_n])$ is isomorphic to K^n, therefore a maximal ideal $\mathfrak{M}$ of $F_q[X_1, \ldots, X_n]$ is determined by one point x of K^n. Moreover this point x belongs to V if and only if $\mathfrak{M} \supset \mathscr{O}$ However this correspondence between the maximal ideals of $F_q[X]$ and the points of K^n is not one-one. So we want to find the condition when two points x and y of K^n correspond to the same maximal ideal of $F_q[X_1, \ldots, X_n] = F_q[X]$. Let $\mathfrak{M}_x$ and $\mathfrak{M}_y$ be the maximal ideals of $K[X]$ corresponding to $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ respectively such that $\mathfrak{M}_x \cap F_q[x] = \mathfrak{M}_y \cap F_q[x]$. It is obvious that $F_q[X]/\mathfrak{M}_x \cap F_q[x] = F[x]/\mathfrak{M}_y \cap F_q[x]$ is isomorphic to $F_q[x_1, \ldots, x_n] = F_{q^f}$ for some $f > 0$. We shall show that the necessary and sufficient condition that

$\mathfrak{M}_x \cap F_q[X] = \mathfrak{M}_y \cap F_q[X]$ is that there exists an element σ in $G(F_{q^f}/F_q)$ such that $\sigma(x) = y$. For $n = 1$ the existence of σ is trivial. Let us assume that there exists a σ in $G(F_q f/F_q)$ such that $\sigma(x_i) = y_i$ for $i = 1, 2, \ldots, r-1$ for $\leq n$. Let $\sigma(x_j) = z_j$ for $j \geq r$. Let $P(x)$ be the polynomial of z_r over $F_q(y_1, \ldots, y_{r-1})$. Then $P(y_1, \ldots, y_{r-1} z_r) = 0$, which gives on applying σ the equation $P(x_1, \ldots, x_{r-1}, y_r) = 0$. Therefore P is in $\mathfrak{M}_y \cap F_q[X]$ i.e., $P(y_1, \ldots y_{r-1}, y_r) = 0$. Thus y_r and z_r are conjugate over $F_q(y_1, \ldots, y_{r-1})$. Let τ be the automorphism of K over $F_q(y_1, \ldots, y_{r-1})$ such that $\tau(a_r) = y_r$. Then $\tau o \sigma$ is an element of $G(F_{q^f}/F_q)$ such that $\tau o \sigma(x_i) = y_i$ for $i = 1, 2, \ldots, r$. Our result fol-
143 lows by induction. The converse is trivial. Hence we see that if $\mathfrak{M}$ is a maximal ideal of $F_q[X]$ containing $\mathscr{O}$ with $N(\mathfrak{M}) = q^f$, then there exist exactly f points conjugate over F_q, in $K^n \cap V$ and $f = (F_q(x) : F_q)$ if and only if f is the smallest integer such that x belongs to $(F_{q^f})^n$. Let

$$N_f = \text{ number of points in } V \cap (F_{q^f})^n$$
$$J_f = \text{ number of points in } V \cap (F_{q^f q^f})^n - \underset{f' < f}{U} (V \cap (F_{q^f})^n)$$

$I_f =$ number of maximal ideals of A of norm q^f.

We have proved that $J_f = fI_f$. By definition of the ζ- function of V we have

$$\begin{aligned}\zeta_V(s) = \zeta_A(s) &= \prod_{\mathfrak{M}\in \mathrm{Spm}(A)} (1-(n\mathfrak{M})^{-s})^{-1} \\ &= \prod_{\mathfrak{M}\in \mathrm{Spm}(A)} (1-q^{-s}f(\mathfrak{M}))^{-1}\end{aligned}$$

where $f(\mathfrak{M})$ is defined by the equation $N(\mathfrak{M}) = q^{f(\mathfrak{M})}$ So we see that we can substitute $t = q^{-s}$ in the zeta function (and not only $t = p^{-s}$ as in the general case) and get a new zeta function.

$$\zeta_V(s) = \prod_{\mathfrak{M}\in \mathrm{Spm}(A)} (1-t^{f(\mathfrak{M})})^{-1} = \prod_{f=1}^{\infty}(1-t^f)^{-I_f} = \tilde{\zeta}_{v,q}(t)$$

Therefore

$$\begin{aligned}\mathrm{Log}\quad \tilde{\zeta}_{v,q}(t) &= \sum_{f=1}^{\infty} -I_f \log(1-t^f) \\ &= \sum_{f=q}^{\infty}\sum_{k=1}^{\infty} I_f \frac{t^{kf}}{k} \\ &= \sum_{f}\sum_{k} \frac{J_f}{f}\frac{t^{kf}}{k} \\ &= \sum_{n=1}^{\infty}\left(\sum_{f/n} J_f\right)\frac{t^n}{n} \\ &= \sum_{n=1}^{\infty} N_n \frac{t^n}{n}\end{aligned}$$

144

Thus $\tilde{\zeta}_{v,q}(t) \exp\left(\sum\limits_{n=1}^{\infty} N_n \frac{t^n}{n}\right)$, where N_n is the number of points of V in F_q^n. We have already seen that this is a power series with integral coefficients.

Theorem $1'$**.** $\tilde{\zeta}_{V,q}(t)$ *is a rational function of t.*

We shall show that in order to prove the rationality of $\tilde{\zeta}_A(t)$ where $t = q^{-s}$, it is sufficient to prove the rationality of $\tilde{\zeta}_A(t)$ where $t = p^{-s}$. Since $\tilde{\zeta}_{v,q}(t)$ and $\tilde{\zeta}_v(t)$ are both convergent in a neighbourhood of the origin, we have

$$\tilde{\zeta}_{v,q}(t^f) = \tilde{\zeta}_v(t) \text{ with } q = p^f.$$

Let μ be any f-th root of unity. Then

$$\tilde{\zeta}_v(\mu t) = \tilde{\zeta}_{v,q}(\mu^f t^f) = \tilde{\zeta}_{v,q}(t^f) = \tilde{\zeta}_v(t)$$

If we have

$$\tilde{\zeta}_v(t) = \frac{\sum_{k=0}^n b_k t^k}{\sum_{k=0}^n C_k t^k}$$

then also

$$\begin{aligned}\tilde{\zeta}_v(t) &= \frac{\sum_\mu (\sum_{k=0}^n b_k \mu^k t^k}{\sum_\mu \sum_{k=0}^n C_k \mu^k t^k}\\ &= \frac{\sum_{k=0}^n b_k (\sum_\mu \mu^k) t^k}{\sum_{k=0}^n C_k (\sum_\mu \mu^k) t^k}\\ &= \frac{\sum_{0\le k\le [n/f]} b_{kf} t^{kf}}{\sum_{0\le k\le [n/f]} C_{kf} t^{kf}}\end{aligned}$$

145 because $\sum\limits_\mu \mu^k = 0$ if $k \not\equiv 0 \pmod f$

Thus we get

$$\tilde{\zeta}_v(t) = \frac{\sum\limits_{0\le k\le [n/f]} b_{kf} t^{kf}}{\sum\limits_{0\le k\le [n/f]} C_k f t^{kf}} = \tilde{\zeta}_{v,q}(t^f)$$

i.e.,

$$\tilde{\zeta}_{V,q}(t) = \frac{\sum\limits_{0\le k\le [n/f]} b_{kf} t^k}{\sum\limits_{0\le k\le [n/f]} C_{kf} t^k}$$

Hence $\tilde{\zeta}_{V,q}(t)$ is a rational function of t.

7 Reduction to a Hyper-Surface

We shall show that to prove our theorem it is sufficient to consider the zeta function of a hypersurface V defined by a polynomial $P(X_1, \ldots, X_n)$ in $F_P[X_1, \ldots, X_n]$. We know that we can write $V = \bigcap\limits_{i=1}^{r} V_i$ where each V_i is a hyper surface. Let E be any subset of $\{1, 2. \ldots, r\}$ and $V_E = \bigcap\limits_{i \epsilon E}^{i} V_i$. Let N_V(respectively N_{V_E}) be the number of points of V(respectively V_E) in any field F_{P^n}. We now prove that

$$N_V = \sum_E (-1)^1 + n(E) N_{V_E} \tag{I}$$

where $n(E)$ is the number of elements in E.

Let any point x in V belong to k hypersurface V_i where $1 \leq k \leq r$. Then x appears l times in the right hand side of equation (I), where

$$\begin{aligned} I &= {}^{r-k}C_0{}^kC_1 - \left({}^{r-k}C_0{}^kC_2 + {}^{r-k}C_1\right) + \cdots + (-1)^{s+1} \\ &\qquad \left({}^kC_s + {}^{r-k}C_1{}^kC_{s-1} + \cdots + {}^kC_h{}^{r-k}C_{s-h} + \cdots\right) + \cdots \\ &= \sum_{t=0}^{\infty} r - k_{C_t} \left[\sum_{h=1}^{\infty} (-1)^{h+t-1} C_h^k\right] \\ &= \sum_{t=0}^{\infty} (-1)^{t-1} \, {}^{r-k}C_t \end{aligned}$$

146

Thus $I = 0$ or 1 according as $r < k$ or $r = k$. Hence the equality (I) is established. This proves that

$$\tilde{\zeta}_V(t) = \prod_E [\tilde{\zeta}_{V_E}(t)]^{(-1)^{1+n(E)}} \tag{2}$$

This proves that it is enough to prove theorem 1 for a hypersurface.

Let V be a hypersurface defined by the polynomial $P(X_1, X_2, \ldots X_n)$ in $F_P[X_1, \ldots X_n]$. Let B be any subset of $\{1, 2, \ldots, n\}$. Let

$$W_B = \{x | x \in V, x_i = 0 \text{ for } i \text{ not in } B\}$$

$$U_B = \left\{ x | x \in W_B, \prod_{i \in B} x_i = 0 \right\}$$

It is obvious that V is union of disjoint subsets $W_B - U_B$ where B runs over all the subsets of $\{1, 2, \ldots, n\}$. Hence the zeta function of V is the product of the zeta functions of the varieties $(W_B - U_B)$ and the theorem 1 will be a consequences of the following lemma.

Lemma 2. Let P be a polynomial in $F_P[X_1, \ldots, X_n]$. then the zeta function of the open subset defined by $\prod_{i=1}^{n} x_i = 0$ in the hyper surface W defined by P is a rational function.

8 Computation of N_r

147 We shall adhere to the following notation throughout our discussion.

$$\begin{aligned} x &= (x_1 \ldots, x_{n+1}), x_i \in F_{P^r}. \\ \alpha &= (\alpha_1, \ldots, \alpha_{n+1}), \alpha_i \in Z. \\ x^\alpha &= x_1^{\alpha_1} \cdots x_{n+1}^{\alpha_{n+1}} \\ |\alpha| &= \alpha_1 + \alpha_2 + \cdots + \alpha_{n+1}. \end{aligned}$$

Let $\mathscr{X}$ be any additive character of F_{p^r}. Then we have

$$\begin{aligned} \sum_{U \in F_{Pr}} \mathscr{X}(UP(X_1, \ldots, X_n)) &= 0 \text{ if } P(x_1, \ldots, x_n) \neq 0 \\ &= p^r \text{ if } P(x_1, \ldots, x_n) = 0 \end{aligned}$$

Therefore

$$\sum_{x_1 \in F^*_{p^r}} \sum_{U \in F_{p^r}} \mathscr{X}(UP(x_1, \ldots, X_n)) = p^r N_r$$

where $$p^r N_r = (p^r - 1)^n + \sum_{x \in (F^*_{pr})} n + 1 \mathscr{X}(x_{n+1} P(x_1, \ldots, x_n))$$

Let

$$x_{n+1}P(x_1,\ldots,x_n)=\sum_\alpha a_\alpha x^\alpha$$

where only a finite number of a_α are nonzero. Then

$$\mathscr{X}(x_{n+1}P)=\prod_\alpha \mathscr{X}(a_\alpha x^\alpha).$$

Therefore $$p^rN_r=(p^r-1)^n+\sum_{x\in(F^*_{p^r})^{n+1}}\prod_\alpha \mathscr{X}(a_\alpha,\ldots,x^\alpha)$$

We take the character $\mathscr{X}$ defined by $\mathscr{X}(t)=\prod_{k=0}^{r-1}\varphi(t'^{p^k})$. where 148
$t'\in R_r$ such that $\overline{t'}=t$ and $\varphi(y)=F(\zeta-1,y),\zeta$ being a primitive p-th root of unity. Thus from equation (1) we get

$$p^rN_r=(p^r-1)^n+\sum_{x\in(F^*_{p^r})^{n+1}}\prod_\alpha\prod_{k=0}^{r-1}\varphi(b_\alpha\xi^\alpha)^{p^k}$$

where $\overline{\xi_i}=x_i,\xi_i\in\mathscr{R}^*_r,\overline{b}_\alpha=a_\alpha$ and b_α belongs to $\mathscr{R}_1$. Let

$$G(\S)=\prod\varphi(b_\alpha\S^\alpha)\text{ and }G_r(\S)=\prod_{k\quad 0}^{r-1}G(\xi^{p^k}).$$

Then

$$p^rN_r=(p^r-1)^n+\sum_{\xi\in(\mathscr{R}^*_r)^{n+1}}G_r(\xi)$$

We have already proved that $G(\xi)$ is analytic for ξ integral. Therefore

$$G_r(\xi)=\sum_{\alpha\in Z^{n+1}}g_{r\alpha}\xi^\alpha$$

Then

$$\begin{aligned}p^rN_r&=(p^r-1)^n+\sum_{\xi\in(\mathscr{R}^*_r)^{n+1}}G(\xi)\\&=(p^r-1)^n+\sum_{\alpha\in Z^{n+1}}g_{r\alpha}\sum_{\xi\in(\mathscr{R}^*_r)^{n+1}}\xi^\alpha\end{aligned}$$

$$= (p^r - 1)^n + \sum_{\alpha \in Z^{n+1}} g_{r_\alpha} \prod_{i=1}^{n+1} \left(\sum_i \xi_i^{\alpha_i} \right)$$

But $\sum_i \xi_i^{\alpha_i} = 0$ if $\alpha_i \not\equiv 0 \pmod{p^r - 1}$

$$= p^r - 1 \text{ if } \alpha_i \equiv 0 \pmod{p^r - 1}$$

Therefore

$$p^r N_r = (p^r - 1)^n + \sum_{\alpha = (p^r - 1)} g_{r_\alpha} (p^r - 1)^{n+1}$$

$$= (p^r - 1)^n + \sum_\alpha g_{p^r\alpha - \alpha} (p^r - 1)^{n+1} \tag{I}$$

149

9 Trace and Determinant of certain Infinite Matrices

Let K be any field and $A = K\Big[[X_1, \ldots, X_{n+1}]\Big]$ be the ring of formal power series in $n+1$ variables over K. Let $H = \sum_\alpha h_\alpha X^\alpha$ by any element of A. We define an operator T_H on A as follows

$$T_H(H') = HH' \text{ for every } H' inA.$$

For any integer r we define an operator λ_r Such that

$$\lambda_r \left(\sum_\alpha a_\alpha X^\alpha \right) = \sum_\alpha a_{r\alpha} X^\alpha.$$

It can be easily proved that these two operators are continuous for the topology given by the valuation on A defined earlier. Let us set $\Gamma_{H,r} = \lambda_r \circ T_H$. It is obvious that the monomials constitute a topological basis of A and the operator $\Gamma_{H,r}$ has a matrix $(\gamma_{\alpha\beta})$ with respect to this basis, where $\gamma_{\alpha\beta} = h_{r\alpha - \beta}$. It is trivial to see that $T_{HH'} = T_H \circ T'_H$ for any two elements H' and H' of A and $\lambda_{rr'} = \lambda_r \circ \lambda'_r$ for any two integers r and r'. Moreover we have

$$\Gamma^s_{H,r} = \lambda_{r^S} \circ T_{H \cdot H^{(r)} \ldots . H^{r^{S-1}}}$$

where $H^{(r)}(X) = H(X^r)$.

In order to prove the above identity it is sufficient to prove that the action of the two sides is the same on the monomials. We have

$T_H 0 \lambda_r(X^\beta) = 0$ if β is not a multiple of r

$$\begin{aligned} T_H \circ \lambda_r(X^\beta) &= T_H(X^{\frac{\beta}{r}}) \text{ if } \beta \text{ is a multiple of } r \\ &= \sum h_\alpha X^{\alpha + \frac{\beta}{r}} = \sum h_\alpha X^{\frac{r\alpha + \beta}{r}} \end{aligned}$$

with the convention that coefficient of $X^{\frac{r\alpha+\beta}{r}} = 0$ if r does not divide β. 150

Therefore

$$\begin{aligned} T_H \circ \lambda_r(X^\beta) &= \lambda_r \left(\sum_\alpha h_\alpha X^{r\alpha} \right) X^\beta) \\ &= \lambda_r \circ T^{(r)}_H \end{aligned}$$

Thus

$$\begin{aligned} \Gamma^2_{H,r} &= \lambda_r \circ T_H \circ \lambda_r \circ T_H \\ &= \lambda_r \circ \lambda_r \circ T_{H^{(r)}} \circ T_H \\ &= \lambda_{r^2} \circ T_{H,H^{(r)}} \end{aligned}$$

Let us assume that we have proved that

$$\Gamma^s_{H,r} = \lambda_{r^S} \circ T_{H \circ H^{(r)} \circ \ldots \circ H^{(r^{s-1})}}$$

Then

$$\begin{aligned} \Gamma^{s+1}_{H,r} &= \Gamma^s_{H,r} \circ \Gamma_{H,r} = \lambda_{r^S} T_{H \circ H^{(2)}} \cdots \circ H^{r^{S-1}} \circ \lambda^\circ_r T_H \\ &= \lambda_{r^S} T_{H \circ} T_{H^{(2)}} T_{H(r^{S-1})} \circ \lambda_r \circ T_H \end{aligned}$$

$$= \lambda_{r^{S+1}} T_H \circ T_{H^{(r)}} \circ \cdots \circ T_{H^{(rs)}}$$

We see immediately that $\Gamma^s_{H,r}$ is an operator of the same type as $\Gamma_{H,r}$ namely $\Gamma^s_{H,r} = \Gamma^s_{H' \circ r'}$ where $r' = r^s$ and $H' = H\, H^{(r)} \ldots H^{(r^{S-1})}$.

151 **Lemma 3.** Let us assume that $K = \Omega$ the complete algebraic closure of Q_P and $r = p^f$. Let us further assume that the coefficients h_α tend to 0 as $|\alpha|$ tends to infinity. Then the series $\mathrm{Tr}(\Gamma^s_{H,r}) = \sum\limits_\alpha (\Gamma^s_{H,r})_{\alpha\alpha}$ giving the trace of $\Gamma^s_{H,r}$ with respect to the basis (X^α) is convergent and we have

$$\mathrm{Tr}(\Gamma^s_{H,r}) = \frac{1}{(r^s-1)^{n+1}} = \sum_{\xi\in(\mathscr{R}^*_{fs})^{n+1}} H(\xi) \ldots\ldots\ldots H\left(\xi^{r^{S-1}}\right)$$

Proof. For any monomial X^β in $K[[X_1, \ldots, X_{n+1}]]$

$$\begin{aligned}\Gamma_{H,r}(X^\beta) &= \lambda_r \circ \sum_\alpha h_\alpha X^{\alpha+\beta}\\ &= \sum_\alpha h_{\alpha r} X^{\alpha+\beta}\end{aligned}$$

Therefore the matrix of the operator $\Gamma_{H,r}$ with respect to the basis (X^β) is $(\gamma_{\alpha\beta})$ with $\gamma_{\alpha\beta} = h_{r\alpha-\beta}$ and $T_r(\Gamma_{H,r}) = \sum\limits_\alpha h_{r\alpha-\alpha}$. But h_α tends to 0 as $|\ \alpha\ |$ tends to infinity, therefore the series $\sum\limits_\alpha h_{r\alpha-\alpha}$ is convergent in K. We have already proved that

$$\sum_{\substack{r-1\\ \rho=1}} H(\rho) = (r-1)^{n+1} \sum_{\alpha\geq 0} h_{r\alpha-\alpha}$$

Therefore

$$T_r(\Gamma_{H,r}) = \frac{1}{(r-1)^{n+1}} \sum_{\rho^{r-1}=1} H(\rho)$$

Hence our lemma is proved for $s = 1$ for $s > 1$, $\Gamma^s_{H,r}$ is of the same type as $\Gamma_{H,r}$.Thus our lemma is completely established. □

152 **Corollary.** *$p^s N_s = (p^s-1)^n + (p^s-1)^{n+1}\operatorname{Tr}\Gamma^s$ where $\Gamma = \Gamma_{G,p}$ we have already proved that*

$$p^s N_s = (p^s-1)^n + \sum_{\xi\in(R_s^*)^{n+1}} \prod_{k=0}^{s-1} G(\xi^{p^k})$$

Therefore the corollary follows from the lemma.

10 Meromorphic character of $\xi_V(t)$ *in* Ω

We have seen that

$$\tilde{\zeta}_V(t) = \exp\left(\sum_{s=1}^{\infty} N_s \frac{t^s}{s}\right), \qquad \text{where}$$

$$N_s = \sum_{i=0}^{n} \binom{n}{i}(-1)^{n-i} p^{s(i-1)} + \sum_{i=0}^{n+1}\binom{n+1}{i}(-1)^{n+1-i} p^{s(i-1)}\operatorname{Tr}\Gamma^s$$

Therefore

$$\begin{aligned}
\sum_{s=1}^{\infty}\frac{N_s t^s}{s} &= \sum_{s=1}^{\infty}\sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}\frac{(p^{i-1}t)^s}{s}\\
&= \sum_{s=1}^{\infty}\sum_{i=0}^{n+1}(-1)^{n+1-i}\binom{n+1}{i}\frac{(p^{i-1}t)^s}{s}\operatorname{Tr}\Gamma^s\\
\exp\left(\sum_{s=1}^{\infty}\frac{N_s t^s}{s}\right) &= \prod_{i=0}^{n}\exp\left(\sum_{s=1}^{\infty}\left[\frac{(p^{i-1}t)^s}{s}\right]\right)(-1)^{n+1-i}\binom{n+1}{i}\\
&= \prod_{i=0}^{n+1}\exp\sum_{s=1}^{\infty}\left[\frac{(p^{i-1}t)^s}{s}\operatorname{Tr}\Gamma^s\right]^{(-1)^{n+1-i}}\binom{n+1}{i}\\
&= \prod_{i=0}^{n}(1-p^{i-1}t)^{(-1)^{n-i}\binom{n}{i}})\prod_{i=0}^{n+1}\Delta(p^{i-1}t)^{(-1)^{n-i}\binom{n+1}{i}})
\end{aligned}$$

where $\Delta(t) = \exp\left(-\sum\limits_{s=1}^{\infty}\dfrac{t^s}{s}\operatorname{Tr}\Gamma^s\right)$

So in order to prove that $\tilde{\zeta}_v(t)$ is meromorphic in Ω, it is sufficient to prove that $\Delta(t)$ is every where convergent in Ω. 153

If Γ were a finite matrix, then its trace is well defined. If the order of the matrix is N, then

$$\operatorname{Tr}\Gamma^s = \sum_{i=1}^{N} \lambda_i^s \text{are the eigen values of } \Gamma.$$

Moreover

$$\begin{aligned}\Delta(t) &= \exp\left(-\sum_{i=1}^{N}\sum_{s=1}^{\infty}\frac{t^s}{s}\lambda_i^s\right) = \prod_{i=1}^{N}(1-t\lambda_i)\\ &= \det(I-t\Gamma)\end{aligned}$$

If Γ is an infinite matrix, we define $\det(I-t\Gamma) = \sum\limits_{m=0}^{\infty} d_m t^m$, where

$$d_m = (-1)^m \sum_{1\le i_1<<i_m} \sum_{\sigma} \varepsilon_\sigma \gamma_{i_1}\gamma_{i_{\sigma(1)}} \ldots \gamma_{i_m} i_{\sigma(m)}$$

ε_σ being the signature of any permutation σ in s_m.

Then for $\Gamma = \Gamma_{G,p}$ we get

$$d_m = (-1)^m \sum_{\alpha_i}{}' \sum_{1\le i\le m} \sum_{\sigma\in s_m} \varepsilon_\sigma \gamma_{\alpha_1\alpha_{\sigma(1)}} \ldots \gamma_{\alpha_m\alpha_{\sigma(m)}} \alpha_i \text{ being distinct.}$$

Let us assume that there exists a constant M such that $v(g_\alpha) \ge M \mid \alpha \mid$. Then

$$\begin{aligned}v(\gamma_{\alpha\beta}) = v(g_{p\alpha-\beta}) &\ge M \mid p\alpha - \beta \mid\\ &\ge M(p\mid \alpha \mid - \mid \beta \mid)\end{aligned}$$

We consider one term of the series giving d_m

$$v\left(\prod_{j=1}^{m} \gamma_{\alpha_j}\gamma_{\sigma(j)}\right) = \sum_{j=1}^{m} v(\gamma_{\alpha_j}\alpha_{\sigma(j)})$$

$$\geq M \sum_j p \mid \alpha_j \mid - \mid \alpha_{\sigma(j)} \mid$$
$$\geq M(p-1) \sum_j \alpha_j$$

154

Now there exist only a finite number of indices α_i such that their length $\mid \alpha \mid$ is less than some constant, therefore the series d_m converges. Moreover we get $v(d_m) \geq M(p-1) \inf \sum\limits_{j=1}^{m} \alpha_j$ where infimum is taken over all the sequence $\alpha_1, \ldots, \alpha_m$. Let $\rho_m = \inf \sum\limits_{j=1}^{m} \mid \alpha_j \mid$. Now let us order the sequence of indices $\alpha \in Z_+^{n+1}$ in such a way that $\mid \alpha_i \mid < \mid \alpha_{i+1} \mid$, then we have $\rho_m = \sum\limits_{i=1}^{m} \mid \alpha_i \mid$ and we see immediately that

$$\lim_{m \to \infty} \frac{\rho_m}{m} = \sum_{\frac{i=1}{m}}^{m} \alpha_i = \infty$$

Therefore $\dfrac{v(d_m)}{m}$ tends to infinity as m tends to infinity. Hence we get the following lemma.

Lemma 4. If an element $G = \sum\limits_{\alpha \in Z_+^{n+1}} g_\alpha X^\alpha$ satisfies the condition

$$(C)\ v(g_\alpha) \geq M \mid \alpha \mid$$

then the series $\det(I - t\Gamma)$ with $\Gamma = \Gamma_G$ is well defined as an element of $\Omega[[t.]]$ and is an every where convergent power series in Ω.

It is evident from the above discussion that if we prove that

(i) The function G defined by $= \pi\varphi(a_\alpha \xi^\alpha)$ satisfies the condition (C) 155

(ii) The formal power series $\exp\left(-\sum\limits_{s=1}^{\infty} \dfrac{t^s \operatorname{Tr} \Gamma^s}{s}\right)$ and $\det(I - t\Gamma)$ are identical.

Then $\Delta(t)$ is every where convergent in Ω which implies that $\tilde{\zeta}_v(t)$ is meromorphic in Ω.

We have already proved the result (ii) when Γ is a finite matrix. Let Γ_h denote the matrix of first h rows and columns of Γ.

Then

$$\begin{aligned}\det(I - t\Gamma_h) &= \exp - \sum_{s=1}^{\infty} \frac{t^s Tr \Gamma_h^s}{s}\\ &= \sum_{m=0}^{\infty} d_m^h t^m\end{aligned}$$

where $d_m^h = (-1)^m \sum\limits_{\leq i_1 \leq i_2 < \ldots < i_m \leq h} \gamma_{i_1 i_{\sigma(1)}} \cdots \gamma_{i_m i_{\sigma(m)}}$ being an element of S_m.

Therefore

$$\log\left(\sum_{m=0}^{\infty} d_m^h t^m\right) = - \sum_{s=1}^{\infty} t^s \frac{\operatorname{Tr}\Gamma_h^s}{s}$$

We shall show that d_m^h converges to d_m and $\operatorname{Tr}\Gamma_h^s$ tends to $\operatorname{Tr}\Gamma^s$ as h tends to infinity. We have

$$\begin{aligned}d_m - d_m^h = (-1)^m \sum_{\alpha_1,\ldots,\alpha_m} \sum_{\sigma \in S_m} \gamma_{\alpha_1} \alpha_{\sigma(1)} \cdots \gamma_{\alpha_m \alpha_{\sigma(m)}}\\ - (-1)^m \sum_{\alpha_i \leq h} \sum_{\sigma \in S_m} \gamma_{\alpha_1} \alpha_{\sigma(1)} \cdots \gamma_{\alpha_m \alpha_{\sigma(*)}}\end{aligned}$$

156 Obviously $v(d_m - d_m^h)$ tends to infinity as h tends to infinity. Similarly one can prove that

$$\begin{aligned}v\left(\operatorname{Tr}\ \Gamma^s - \operatorname{Tr}\ \Gamma_h^s\right) = v\left[\sum_{\alpha_1 \ldots \alpha_s} g_{p\alpha_1 - \alpha_2} \cdots g_{p\alpha_s - \alpha_1}\right.\\ \left. - \left(\sum_{\alpha_1 \ldots \alpha_s\ \leq h} g_{p\alpha_1 - \alpha_2} \cdots g_{p\alpha_s - \alpha_1}\right)\right]\end{aligned}$$

tends to infinity as h tends to infinity. In order to prove that the function G satisfies (1) it is sufficient to prove that each term $\varphi(a_\alpha \xi^\alpha)$ of the product satisfies (1). We have

$$\varphi(t) = F(\zeta - 1, t)$$

But $F(Y, t) = \sum\limits_{m=o}^{\infty} A_m(Y)t^m$ with $A_m(Y) = Y^m B_m(Y)$ and $B_m(Y)$ belongs to $\mathscr{O}[[Y]]$. Therefore

$$\begin{aligned}\varphi(a_\alpha \xi^\alpha) &= \sum_{m=0}^{\alpha} (\zeta - 1)^m B_m(\zeta - 1)(a_\alpha \xi^\alpha)^m \\ &= \sum_{\beta=0}^{\alpha} h_\beta \xi^\beta.\end{aligned}$$

Thus $h_\beta = 0$ if $\beta \neq \alpha_m$

$$= (\zeta - 1)^{\frac{\beta}{\alpha}} B_{\beta_{/\alpha}}(\zeta - 1) a_\alpha^{\frac{\beta}{\alpha}}.$$

which shows that

$$v(h_\beta) \geq \frac{|\beta|}{|\alpha|} \; \frac{1}{p-1} = \left(\frac{1}{p-1} \; \frac{1}{|\alpha|}\right)|\beta|$$

because $B_{\beta_{/\alpha}}(\zeta - 1)a_\alpha^{\beta_{/\alpha}}$ is of positive valuation. Hence G satisfies (I).

We have proved that $\tilde{\zeta}_v(t)$ is convergent in a disc $|t| < \delta < 1$ as **157**
a series of complex numbers and is meromorphic in the whole of Ω, therefore by the Criterion of rationality proved earlier we obtain that $\tilde{\zeta}_v(t)$ is a rational function of t. Hence the lemma 2 of §7 is completely proved and also the theorem 1.

Bibliography

[1] E. Artin Algebraic Theory of Numbers, Gottingen 1960. **158**

[2] E. Artin Geometric Algebra.

[3] A. Borel *Groupes linearies algebriques,* Annals of Math., 64 1956, p.20-82.

[4] N. Bourbaki Algebre Ch.. VII

[5] N. Bourbaki Algebre Ch.. VIII

[6] N. Bourbaki Algebre Ch.. IX

[7] N. Bourbaki Algebre commutative, Ch. I-VI (to appear).

[8] F. Bruhat Sur les representations induties des groupes de Lie, Bull. Soc. Math. Fr., 84, 1956, p.97-205.

[9] F. Bruhat Lecture on Lie groups and representations of locally compact groups, Tata Institute 1958.

[10] F. Bruhat Distributions sur, les groupes localement compacts et applications aux representations des groupes p-adiques, Bull. Soc. Math. Fr., 89, 1961, p.43-76.

[11] F. Bruhat Sur les representations des groupes classiques p-adiques, Amer. Journal of Math., 84, 1961.

[12] C. Chevalley Sur certains groupes simples, Tohoku Math. JOur. 7, 1955, p.14-66.

[13] J. Dieudonne Sur les groupes classiques, Hermann 1948.

[14] J. Dieudonne La geometrie des groupes classiques, Springer 1955.

[15] B. Dwork Norm residue symbol in local number fields, Abh. Math. Sem. Hamburg, 22, 1958, p.180-190.

[16] B. Dwork On the retionality of zeta function of an algebraic variety, Amer. Jour. of Math., 82, 1960, p.631-648.

[17] M. Eichler Quadratische Formen and orthogonale Gruppen, Berlin 1952.

[18] I. Gelfand and M. Naimark Unitare Darstellungen der klassische Gruppen, Berlin 1957.

[19] R. Godement A theory of spherical functions, Trans. A.M.S., 73, 1952, p.496-556.

[20] A. Grothendieck et J. Dieudonne Elements de geometrique Algebrique, I, Publications Mathematiques de 1'I. H.E.S. no4, Paris
159 1960.

[21] Harishchandra Travaux de Harishchandra Seminaire Bourbaki February 1957.

[22] Harishchandra Representations of Semi-simple Lie Groups V Amer. Jour. of Math., 78, 1956, p.1-40.

[23] H. Hasse Zahlentheorie, Berlin 1949.

[24] I. Kaplansky Groups with representations of bounded degree, Canad. Jour. of Math., 1, 1949, p.105-112.

[25] I. Kaplansky Elementary divisors and modules, Trans. A.M.S., 66,1949, p. 464-491.

[26] M. Krasner Theorie des corps values, C.R.Acad. Sci., 239, 1954, p.745-747.

[27] G.W. Mackey Induced representations of locally compact groups Annals of Math. 55, 1952, p.101-134.

[28] F.I. Mautner Spherical functions on *p*-adic fields, Amer. Jour. of Math., 80, 1958, p.441-457.

[29] P. Samuel Algebre locale, Memorial des Sci. Math., 123, Paris, 1953.

[30] O. Schilling Theory of valuations, New-York, A.M.S., 1950.

[31] L. Schnirelmann Sur les fonctions dans les corps normes algebriquement clos, Bull. Acad. Sci. U.R.S.S., 19 p.487-497.

[32] J.P. Serre Representations lineaires et espaces homogenes Kahleriens des groups de Lie Compacts. Seminaire Bourbaki Mai 1954.

[33] R. Steinberg The representations of GL(3, q), GL(4, q), PGL(3. q) and PGL(4, q), Canad. Jour. of Math., 3, 1951, p.225.

[34] A. Weil L'integration dans les groupes topologiques, Paris 1940.

[35] A. Weil Sur les courbes algebriques et les varietes qui s'en deduisent, Paris, 1948.

[36] A. Weil Numbar of solutions of equations in finite fields, Bull. A.M.S., 5, 1949, p.497.

For Part I, see (1), (7), (23), (29), (30) **160**

For Part II, see (9), (19), (24), (27) and (34) for the theory of spherical functions in general. See (2), (6), (13), (14), (17), (24), for classical groups. See (10), (11), (17) and (28) for *p*-adic groups.

For Part III, see (15), (16), (26) and (31) for analytic functions and (16), (34), (36) for zeta-function.