CHAPTER II

Global Fields

J. W. S. CASSELS

1. Valuations

We shall be concerned only with rank 1 valuations, so for brevity, valuation will mean "rank 1 valuation".

DEFINITION. *A valuation $|\ |$ on a field k is a function defined on k with values in the non-negative real numbers satisfying the following axioms.*

(1) $|\alpha| = 0$ *if and only if* $\alpha = 0$.

(2) $|\alpha\beta| = |\alpha||\beta|$.

(3) *There is a constant* C *such that* $|1+\alpha| \leq C$ *whenever* $|\alpha| \leq 1$.

DEFINITION. *The trivial valuation of* k *is that for which* $|\alpha| = 1$ *for all* $\alpha \neq 0$.

Note: This will often be tacitly excluded from consideration.

From (2) we have

$$|1| = |1|.|1|,$$

so $|1| = 1$ by (1). If now some power of $\omega \in k$ is 1, say $\omega^n = 1$ we have $|\omega| = 1$ by (2). In particular the only valuation of the finite fields is the trivial one.

The same argument shows that $|-1| = 1$ and so

$$|-\alpha| = |\alpha| \quad \text{all } \alpha \in k.$$

DEFINITION. *Two valuations $|\ |_1$, $|\ |_2$ on the same field k are equivalent if there is a $c > 0$ such that*

$$|\alpha|_2 = |\alpha|_1^c. \tag{1.1}$$

Note: If $|\alpha|_1$ is a valuation then $|\alpha|_2$ defined by (1.1) is one also. Equivalence is clearly an equivalence relation.

Trivially every valuation is equivalent to one with $C = 2$. For such a valuation it can be shown† that

$$(3') \qquad |\beta+\gamma| \leq |\beta|+|\gamma|$$

(The "triangle inequality".) Conversely (1), (2) and (3′) trivially imply (3) with $C = 2$. We shall at first be almost entirely concerned with properties of valuations unaffected by equivalence and so will often use (3′) instead of (3).

† We shall actually be concerned only with valuations with $C = 1$, for which (3′) is trivial (see next section), or with valuations equivalent to the ordinary absolute value of the real or complex numbers, for which (3′) is well known to hold: and we use (3) instead of (3′) (following Artin) only for the technical reason that we will want to call the square of the absolute value of the complex numbers a valuation. For completeness, however, we give the deduction of (3′) from (3) with $C = 2$. First, $|\alpha_1 + \alpha_2| \leq 2 \max |\alpha_1|, |\alpha_2|$, on putting $\alpha_2 = \alpha\alpha_1$ if, say, $|\alpha_1| \geq |\alpha_2|$. Then, by induction,

$$|\sum_{j=1}^{2^r} \alpha_j| \leq 2^r \max |\alpha_j|,$$

and so for any $n > 0$, we have

$$|\sum_{j=1}^{n} \alpha_j| \leq 2^r \max |\alpha_j| \leq 2n \max |\alpha_j|,$$

where $2^{r-1} < n \leq 2^r$, on inserting $2^r - n$ zero summands. In particular

$$|n| \leq 2n|1| = 2n \qquad (n > 0).$$

But now

$$\begin{aligned} |\beta + \gamma|^n &= |\sum_j \binom{n}{j} \beta^j \gamma^{n-j}| \\ &\leq 2(n+1) \max |\binom{n}{j}| |\beta|^j |\gamma|^{n-j} \\ &\leq 4(n+1) \max \binom{n}{j} |\beta|^j |\gamma|^{n-j} \\ &\leq 4(n+1)(|\beta| + |\gamma|)^n; \end{aligned}$$

and (3′) follows on extracting nth roots and making $n \to \infty$.

For later use we note the formal consequence

$$||\beta|-|\gamma|| \leq |\beta-\gamma|$$

of (3′) where the outside $||$ are the ordinary absolute value. For one need only apply the triangle inequality to the identity

$$\beta = \gamma+(\beta-\gamma) \qquad \gamma = \beta+(\gamma-\beta).$$

2. Types of Valuation

We define two important properties of a valuation, both of which apply to whole equivalence classes of valuation.

DEFINITION. *The valuation $||$ is discrete if there is a $\delta > 0$ such that*

$$1-\delta < |\alpha| < 1+\delta$$

implies $|\alpha| = 1$.

This is the same as saying that the set of $\log|\alpha|$, $\alpha \in k$, $\alpha \neq 0$ form a discrete subgroup of the reals under addition. Such a group is necessarily free on one generator, i.e. there is a $c < 1$ such that $|\alpha|$, $\alpha \neq 0$ runs through precisely the set of c^m, $m \in \mathbf{Z}$. If $|\alpha| = c^m$ we call $m = m(\alpha)$ the *order* of α. Axiom 2 implies

$$\operatorname{ord}(\alpha\beta) = \operatorname{ord}\alpha+\operatorname{ord}\beta.$$

DEFINITION. *The valuation $||$ is non-archimedean if one can take $C = 1$ in Axiom 3, i.e. if*

$$|\beta+\gamma| \leq \max\{|\beta|,|\gamma|\}. \tag{2.1}$$

If it is not non-archimedean, then it is archimedean.

We note at once the consequence

$$|\beta+\gamma| = |\beta| \quad \text{if } |\gamma| < |\beta|$$

of (2.1). For

$$|\beta| = |(\beta+\gamma)-\gamma| \leq \max\{|\beta+\gamma|,|\gamma|\}.$$

For non-arch. $||$ the α with $|\alpha| \leq 1$ clearly form a ring, the *ring* $\mathfrak{o}$ *of integers*. Two non-archimedean valuations are equivalent if and only if they give the same $\mathfrak{o}$: for $|\beta| < |\gamma|$ if and only if $\beta\gamma^{-1} \in \mathfrak{o}$, $\beta^{-1}\gamma \notin \mathfrak{o}$ (cf. § 4).

The set of α with $|\alpha| < 1$ form an ideal $\mathfrak{p}$ in $\mathfrak{o}$, clearly maximal. It consists precisely of the $\alpha \in \mathfrak{o}$ with $\alpha^{-1} \notin \mathfrak{o}$.

The notation $\mathfrak{o}$ and $\mathfrak{p}$ will be standard. The reader will easily prove the

LEMMA. *Let $||$ be non-archimedean. A necessary and sufficient condition for it to be discrete is that $\mathfrak{p}$ is a principal ideal.*

We need later the

LEMMA. *A necessary and sufficient condition that $||$ be non-archimedean is that $|n| \leq 1$ for all n in the ring generated by 1 in k.*

Note: We cannot identify this ring with $\mathbf{Z}$ if k has a characteristic.

Proof. Necessity is obvious. For sufficiency let $|\alpha| \leq 1$, and then by the triangle inequality

$$\begin{aligned}|1+\alpha|^n &= |(1+\alpha)^n| \\ &\leq \sum_{j=0}^{n}\left|\binom{n}{j}\right||\alpha| \\ &\leq 1+1+\ldots+1 = n,\end{aligned}$$

so $(n \to \infty)$, $|1+\alpha| \leq 1$.

COROLLARY. *If* $\operatorname{Char} k = p \neq 0$ *then any valuation of k is non-archimedean.*

For the ring generated by 1 in k is the field $\mathbf{F}$ of p elements. If $b \in \mathbf{F}$, then $b^{p-1} = 1$ and so $|b| = 1$.

3. Examples of Valuations

The archetypal example of an arch. valuation is the absolute value on the field $\mathbf{C}$ of complex numbers. It is essentially the only one:

THEOREM (Gelfand-Tornheim). *Any field k with an arch. valuation is isomorphic to a subfield of* $\mathbf{C}$, *the valuation being equivalent to that induced by the absolute valuation on* $\mathbf{C}$.

We do not prove this as we do not need it. See e.g. E. Artin, "Theory of Algebraic Numbers" (Striker, Göttingen), pp. 45 and 67.

The non-arch. valuations are legion. On the rationals $\mathbf{Q}$ there is one for every prime $p > 0$, the *p-adic valuation* defined by

$$|p^a u/v|_p = p^{-a}$$

for $a, u, v \in \mathbf{Z}$, $p \nmid u$, $p \nmid v$.

THEOREM (Ostrowski). *The only non-trivial valuations on* $\mathbf{Q}$ *are those equivalent to the $|\ |_p$ or the ordinary absolute value $|\ |_\infty$.*

Proof. Let $||$ be a non-trivial valuation on $\mathbf{Q}$ which (without loss of generality) satisfies the triangle inequality.

Let $a \in \mathbf{Z}$ be greater than 1. Every $b \in \mathbf{Z}$ can be put in the shape

$$b = b_m a^m + b_{m-1}a^{m-1} + \ldots + b_0$$

where

$$0 \leq b_j < a \qquad (0 \leq j \leq m)$$

and

$$m \leq \frac{\log b}{\log a}.$$

By the triangle inequality

$$|b| \leq \mathcal{M}\left(\frac{\log b}{\log a}+1\right)\max\left\{1,|a|^{\frac{\log b}{\log a}}\right\}$$

where

$$\mathscr{M} = \max_{1 \le d < a} |d|.$$

On putting $b = c^n$ and letting $n \to \infty$, we nave

$$|c| \le \max\left\{1, |a|^{\frac{\log c}{\log a}}\right\}. \tag{3.1}$$

First Case. $\exists\, c > 1$ in $\mathbf{Z}$ with $|c| > 1$. Then $|a| > 1$ for every $a > 1$ in $\mathbf{Z}$ and (3.1) gives

$$|c|^{\frac{1}{\log c}} = |a|^{\frac{1}{\log a}}.$$

Hence $|\ |$ is equivalent to the ordinary absolute value.

Second Case. $|c| \le 1$ for all $c \in \mathbf{Z}$ so by a previous lemma $|\ |$ is non-arch. Since $|\ |$ is non-trivial the set $\mathfrak{a}$ of $a \in \mathbf{Z}$ with $|a| < 1$ is non-empty and is clearly a $\mathbf{Z}$-ideal. Since $|bc| = |b||c|$ the ideal $\mathfrak{a}$ is prime, say belonging to $p > 0$ and then clearly $|\ |$ is equivalent to $|\ |_p$.

Now let k_0 be any field and let $k = k_0(t)$, where t is transcendental. If $p = p(t)$ is an irreducible polynomial in the ring $k_0[t]$ we define a valuation by

$$|(p(t))^a u(t)/v(t)|_p = c^{-a} \tag{3.2}$$

where $c < 1$ is fixed, $a \in \mathbf{Z}$ and $u(t), v(t) \in k_0[t]$, $p(t) \nmid u(t)$, $p(t) \nmid v(t)$.

In addition there is the *non-arch.* valuation $|\ |_\infty$ defined by

$$\left|\frac{u(t)}{v(t)}\right|_\infty = c^{(\deg v - \deg u)}. \tag{3.3}$$

Note the analogy between $k_0(t)$ and $\mathbf{Q}$, which is however not perfect. If $s = t^{-1}$, so $k_0(t) = k_0(s)$, the valuation $|\ |_\infty$ is seen to be of the type (3.2) belonging to the irreducible polynomial $p(s) = s$.

The reader will easily prove the

LEMMA. *The only non-trivial valuations on $k_0(t)$ which are trivial on k_0 are equivalent to the valuation* (3.2) *or* (3.3).

COROLLARY. *If $\mathbf{F}$ is a finite field the only non-trivial valuations on $\mathbf{F}(t)$ are equivalent to* (3.2) *or* (3.3).

4. Topology

A valuation $|\ |$ on a field k induces a topology in which a basis for the neighbourhoods of α are the "open spheres"

$$S_d(\alpha) = \{\xi \mid |\xi - \alpha| < d\}$$

for $d > 0$. Equivalent valuations induce the same topology. A valuation satisfying the triangle inequality gives a metric for the topology on defining the distance from α to β to be $|\alpha - \beta|$.

LEMMA. *A field with the topology induced by a valuation is a topological field, i.e. the operations sum, product, reciprocal are continuous.*

Proof. For example (product) the triangle inequality implies that

$$|(\alpha+\theta)(\beta+\phi) - \alpha\beta| \le |\theta||\phi| + |\alpha||\phi| + |\beta||\theta|$$

is small when $|\theta|$, $|\phi|$ are small (α, β fixed).

LEMMA. *If two valuations $|\ |_1$, $|\ |_2$ on the same field induce the same topology then they are equivalent in the sense defined above.*

Proof. $|\alpha|_1 < 1$ if and only if $\alpha^n \to 0$ $(n \to +\infty)$ in the topology and so $|\alpha|_1 < 1$ if and only if $|\alpha|_2 < 1$. On taking reciprocals we see that $|\alpha|_1 > 1$ if and only if $|\alpha|_2 > 1$ so finally $|\alpha|_1 = 1$ if and only if $|\alpha|_2 = 1$.

Let now $\beta, \gamma \in k$ and not 0. On applying the foregoing to

$$\alpha = \beta^m \gamma^n \qquad (m, n \in \mathbf{Z})$$

we see that

$$m \log|\beta|_1 + n \log|\gamma|_1 \gtrless 0$$

according as

$$m \log|\beta|_2 + n \log|\gamma|_2 \gtrless 0$$

and so

$$\frac{\log|\beta|_1}{\log|\beta|_2} = \frac{\log|\gamma|_1}{\log|\gamma|_2}.$$

5. Completeness

A field k is *complete* with respect to a valuation $|\ |$ if it is complete as a metric space with respect to the metric $|\alpha - \beta|$ $(\alpha, \beta \in k)$ i.e. if given any sequence α_n $(n = 1, 2, \ldots)$ with

$$|\alpha_m - \alpha_n| \to 0 \qquad (m, n \to \infty, \infty)$$

(a fundamental sequence), there is an $\alpha^* \in k$ such that

$$\alpha_n \to \alpha^* \qquad \text{w.r.t.}\ |\ |$$

(i.e. $|\alpha_n - \alpha^*| \to 0$).

THEOREM. *Every field k with valuation $|\ |$ can be embedded in a complete field $\bar{k}$ with a valuation $|\ |$ extending the original one in such a way that k is the closure of k with respect to $|\ |$. Further, $\bar{k}$ is unique (up to isomorphism).*

Proof (sketch). We define $\bar{k}$ as a metric space to be the completion of k as a metric space with respect to $|\ |$. Since the field operations $+$, $\times$ and inverse are continuous on k they are well-defined on $\bar{k}$. Q.E.D.

COROLLARY 1. *$|\ |$ is non-arch. on $\bar{k}$ if and only if it is so on k. If that is so, the set of values taken by $|\ |$ on k and $\bar{k}$ are the same.*

Proof. Use second lemma of § 2. Alternatively, if k is non-arch., the functional inequality

$$|\beta + \gamma| \le \max(|\beta|, |\gamma|)$$

holds also in $\bar{k}$ by continuity. If now $\beta \in \bar{k}$, $\beta \neq 0$ there is a $\gamma \in k$ such that $|\beta-\gamma| < |\beta|$ and then $|\beta| = |\gamma|$. Converse trivial.

COROLLARY 2. *Any valuation-preserving embedding of k in a complete field K can be uniquely continued to an embedding of $\bar{k}$.*

6. Independence

The following theorem asserts that inequivalent valuations are in fact almost totally independent. For our purposes it will be superseded by the result of § 15.

LEMMA ("weak approximation theorem"). *Let $|\ |_n$ $(1 \leq n \leq N)$ be inequivalent non-trivial valuations of a field k. For each n let k_n be the topological space consisting of the set of elements of k with the topology induced by $|\ |_n$. Let Δ be the image of k in the topological product $\prod = \prod_{1 \leq n \leq N} k_n$ (with the product topology). Then Δ is everywhere dense in $\prod$.*

The conclusion of the lemma may be expressed in a less topological manner: given any $\alpha_n \in k$ $(1 \leq n \leq N)$ and real $\varepsilon > 0$ there is a $\xi \in k$ such that simultaneously:

$$|\alpha_n - \xi|_n < \varepsilon \qquad (1 \leq n \leq N).$$

Note. If $k = \mathbf{Q}$ and the $|\ |$ are p-adic valuations this is related to the "Chinese Remainder Theorem", but the strong approximation theorem is the real generalization.

Proof. We note first that it will be enough to find $\theta_n \in k$ such that

$$|\theta_n|_n > 1, \quad |\theta_n|_m < 1 \qquad (n \neq m) \tag{6.1}$$

where $1 \leq n \leq N$, $1 \leq m \leq N$. For then as $r \to +\infty$ we have

$$\frac{\theta_n^r}{1+\theta_n^r} = \frac{1}{1+\theta_n^{-r}} \to \begin{cases} 1 \text{ w.r.t. } |\ |_n \\ 0 \text{ w.r.t. } |\ |_m, \quad m \neq n \end{cases}$$

and it is enough to take

$$\xi = \sum_{n=1}^{N} \frac{\theta_n^r}{1+\theta_n^r} \alpha_n$$

with sufficiently large r.

By symmetry it is enough to show the existence of $\theta = \theta_1$ with

$$|\theta|_1 > 1 \qquad |\theta|_n < 1 \qquad (2 \leq n \leq N)$$

and we use induction on N.

$N = 2$. Since $|\ |_1$ and $|\ |_2$ are unequivalent there is an α such that

$$|\alpha|_1 < 1, \qquad |\alpha|_2 \geq 1$$

and similarly a β such that

$$|\beta|_1 \geq 1, \qquad |\beta|_2 < 1$$

and then $\theta = \beta\alpha^{-1}$ will do.

$N \geq 3$. By the case $N-1$ there is a $\phi \in k$ such that

$$|\phi|_1 > 1, \qquad |\phi|_n < 1 \qquad (2 \leq n \leq N-1)$$

and by the case $N = 2$ there is a $\psi \in k$ such that

$$|\psi|_1 > 1, \qquad |\psi|_N < 1.$$

Then put

$$\theta = \begin{cases} \phi & \text{if } |\phi|_N < 1 \\ \phi^r\psi & \text{if } |\phi|_N = 1 \\ \dfrac{\phi^r}{1+\phi^r}\psi & \text{if } |\phi|_N > 1 \end{cases}$$

where $r \in \mathbf{Z}$ is sufficiently large.

7. Finite Residue Field Case

Let k be a field with non-archimedean valuation $|\ |$. Then the set of $\alpha \in k$ with $|\alpha| \leq 1$ form a ring $\mathfrak{o}$, the ring of integers for $|\ |$. The $\varepsilon \in k$ with $|\varepsilon| = 1$ are a group under multiplication, the group of units. Finally, the set of α with $|\alpha| < 1$ is a maximal ideal $\mathfrak{p}$, so the quotient ring $\mathfrak{o}/\mathfrak{p}$ is a field. We consider the case when $\mathfrak{o}/\mathfrak{p}$ has a finite number P of elements.

Suppose further, that $|\ |$ is discrete. Then $\mathfrak{p}$ is a principal ideal (π), say, and every α is of the form $\alpha = \pi^v\varepsilon$, where ε is a unit. We call v the *order* of α. If also $\mathfrak{p} = (\pi')$ then π/π' is a unit and conversely, so the order of α is independent of the choice of π.

Let $\bar{\mathfrak{o}}$, $\bar{\mathfrak{p}}$ be defined with respect to the completion $\bar{k}$ of k. Then clearly $\bar{\mathfrak{o}}/\bar{\mathfrak{p}} = \mathfrak{o}/\mathfrak{p}$ and $\bar{\mathfrak{p}} = (\pi)$ as an $\bar{\mathfrak{o}}$-ideal.

LEMMA. *Suppose, further, that k is complete with respect to $|\ |$ then $\mathfrak{o}$ is precisely the set of*

$$\alpha = \sum_{j=0}^{\infty} a_j \pi^j \tag{7.1}$$

where the a_j run independently through some set $\sum$ of representatives in $\mathfrak{o}$ of $\mathfrak{o}/\mathfrak{p}$.

By (7.1) is meant of course the limit of the fundamental sequence $\sum_{j=0}^{J} a_j\pi^j$ as $J \to \infty$. For there is a uniquely defined $a_0 \in \sum$ such that $|\alpha - a_0| < 1$. Then $\alpha_1 = \pi^{-1}(\alpha - a_0) \in \mathfrak{o}$. Now define $a_1 \in \sum$ by $|\alpha_1 - a_1| < 1$. And so on.

THEOREM. *Under the conditions of the preceding lemma $\mathfrak{o}$ is compact with respect to the $|\ |$-topology.*

Proof. Let O_λ $(\lambda \in \Lambda)$ be some family of open sets covering $\mathfrak{o}$. We must show there is a finite subcover. We suppose not.

Let $\sum$ be a set of representatives of $\mathfrak{o}/\mathfrak{p}$. Then $\mathfrak{o}$ is the union of the finite

number of sets $a+\pi\mathfrak{o}$ ($a \in \sum$). Hence for at least one $a_0 \in \sum$ the set $a_0+\pi\mathfrak{o}$ is not covered by finitely many of the O_λ. Then similarly there is an $a_1 \in \sum$ such that $a_0+a_1\pi+\pi^2\mathfrak{o}$ is not finitely covered. And so on. Let $\alpha = a_0+a_1\pi+\dots$. Then $\alpha \in O_{\lambda_0}$ for some $\lambda_0 \in \Lambda$. Since O_{λ_0} is open, $\alpha+\pi^J\mathfrak{o} \subset O_{\lambda_0}$ for some J. Contradiction.

COROLLARY. *k is locally compact.*

[The converse is also true. If k is locally compact with respect to a non-arch. valuation $||$ then

(1) k is complete;
(2) the residue field is finite;
(3) the valuation is discrete.

For there is a compact neighbourhood c of 0. Then $\pi^v\mathfrak{o} \subset c$ for sufficiently large v so $\pi^v\mathfrak{o}$ is compact, being closed. Hence $\mathfrak{o}$ is compact. Since $|\ |$ is a metric, $\mathfrak{o}$ is sequentially compact, i.e. every fundamental sequence in $\mathfrak{o}$ has a limit, which implies (1). Let a_λ ($\lambda \in \Lambda$) be a set of representatives in $\mathfrak{o}$ of $\mathfrak{o}/\mathfrak{p}$. Then $O_\lambda : |\xi - a_\lambda| < 1$ is an open covering of $\mathfrak{o}$. Thus (2) holds since $\mathfrak{o}$ is compact. Finally, $\mathfrak{p}$ is compact being a closed subset of $\mathfrak{o}$. Let S_n be the set of $\alpha \in k$ with $|\alpha| < 1 - 1/n$. Then S_n ($1 \le n < \infty$) is an open cover of $\mathfrak{p}$, so $\mathfrak{p} = S_n$ for some n, i.e. (3) is true.

If we allow $|\ |$ to be archimedean the only further possibilities are $k = \mathbf{R}$ and $k = \mathbf{C}$ with $|\ |$ equivalent to the absolute value.]

We denote by k^+ the commutative topological group whose points are the elements of k, whose law is addition and whose topology is that induced by $|\ |$. General theory tells us that there is an invariant measure (Haar measure) defined on k^+ and that this measure is unique up to a multiplicative constant. We can easily deduce what that measure μ is.

Since μ is invariant

$$\mu(\alpha+\pi^v\mathfrak{o}) = \mu_v$$

is independent of α. Further

$$\alpha+\pi^v\mathfrak{o} = \bigcup_{1 \le j \le P} (\alpha+\pi^v a_j+\pi^{v+1}\mathfrak{o})$$

where a_j ($1 \le j \le P$) is a set of representatives of $\mathfrak{o}/\mathfrak{p}$. Hence

$$\mu_v = P\mu_{v+1}.$$

If we normalize μ by putting

$$\mu(\mathfrak{o}) = 1, \tag{7.2}$$

we have

$$\mu_v = P^{-v}.$$

Conversely, without the theory of Haar measure, it is easy to see that there is a unique invariant measure on k^+ subject to (7.2).

Everything so far in this section has depended not on the valuation $|\ |$ but only on its equivalence class. The above considerations now single out one valuation as particularly important.

DEFINITION. *Let k be a field with discrete valuation $|\ |$ and residue class field with $P < \infty$ elements. We say that $|\ |$ is normalized if*

$$|\pi| = P^{-1},$$

where $\mathfrak{p} = (\pi)$.

THEOREM. *Suppose, further, that k is complete with respect to the normalized valuation $|\ |$. Then*

$$\mu(\alpha+\beta\mathfrak{o}) = |\beta|$$

where μ is the Haar measure on k^+ normalized by $\mu(\mathfrak{o}) = 1$.

We can express the result of the theorem in a more suggestive way. Let $\beta \in k$, $\beta \neq 0$ and let μ be a Haar measure on k^+ (not necessarily normalized as in the theorem). Then we can define a new Haar measure μ_β on k^+ by putting $\mu_\beta(E) = \mu(\beta E)$ ($E \subset k^+$). But Haar measure is unique up to a multiplicative constant and so $\mu_\beta(E) = \mu(\beta E) = f\mu(E)$ for all measurable sets E, where the factor f depends only on β. The theorem states that f is just $|\beta|$ in the normalized valuation.

[The theory of locally compact topological groups leads to the consideration of the dual (character) group of k^+. It turns out that it is isomorphic to k^+. We do not need this fact for class field theory so do not prove it here. For a proof and applications see Tate's thesis (Chapter XV of this book) or Lang: "Algebraic Numbers" (Addison Wesley), and, for generalizations; Weil: "Adeles and Algebraic Groups" (Princeton lecture notes) and Godement: Bourbaki seminars 171 and 176. The determination of the character group of $k^\times$ is local class-field theory.]

The set of non-zero elements of k form a group $k^\times$ under multiplication. Clearly multiplication and taking the reciprocal are continuous with respect to the topology induced in $k^\times$ as a subset of k, so $k^\times$ is a topological group with this topology.† We have

$$k^\times \supset E \supset E_1$$

where E is the group of units of k and where E_1 is the group of einseinheiten, i.e. the $\varepsilon \in k$ with $|\varepsilon-1| < 1$. Clearly E and E_1 are both open and closed in $k^\times$. $E_1 = \{\varepsilon \in k : |\varepsilon| \le 1 \text{ and } \varepsilon \equiv 1 \pmod{\mathfrak{p}}\} \subseteq E$ (since $|\varepsilon| > 1 \Rightarrow |\varepsilon-1| = |\varepsilon| > 1$, $|\varepsilon| < 1$

Obviously $k^\times/E$ is isomorphic to the additive group $\mathbf{Z}^+$ of integers with the discrete topology, the map being

$$\pi^v E \to v \qquad (v \in \mathbf{Z}).$$

Further, E/E_1 is isomorphic to the multiplicative group $\kappa^\times$ of the non-zero elements of the residue class field, where the finite group $\kappa^\times$ has the discrete topology.‡ Further, E is compact, so $k^\times$ is locally compact. Clearly the

† We shall later have to consider the situation for topological rings R, where $R^\times$ in general is given a different topology from the subset topology.

‡ $\kappa^\times$ is cyclic of order $P-1$. It can be shown that k always contains a primitive $P-1$-th root of unity ρ and so the elements of $k^\times$ are just the $\pi^v\rho^u\varepsilon$, $\varepsilon \in E_1$, i.e. $k^\times$ is the direct product of $\mathbf{Z}$, $\mathbf{Z}/(P-1)\mathbf{Z}$ and E_1.

In fact let $f(X) = X^{P-1} - 1$ and let $\alpha \in \mathfrak{o}$ be such that $\alpha \bmod \mathfrak{p}$ generates $\kappa^\times$. Then $|f(\alpha)| < 1$, $|f'(\alpha)| = 1$. Then by Hensel's Lemma (App. C) there is $\rho \in k$ such that $f(\rho) = 0$, $\rho \equiv \alpha \pmod{\mathfrak{p}}$.

additive Haar measure on E_1 is also invariant under multiplication so gives a Haar measure on E_1: and this gives the Haar measure on $k^\times$ in an obvious way.

Finally we note the

LEMMA. *k^+ and $k^\times$ are totally disconnected (the only connected sets are points).*

Beweis. Klar.

[It is perhaps worth mentioning that $k^\times$ and k^+ are locally isomorphic if k has characteristic 0. We have the exponential map

$$\alpha \to \exp \alpha = \Sigma \frac{\alpha^n}{n!}$$

valid for all sufficiently small α with its inverse

$$\log \alpha = \Sigma \frac{(-)^{n-1}(\alpha-1)^n}{n}$$

valid for all α sufficiently near to 1.]

8. Normed Spaces

DEFINITION. *Let k be a field with valuation $|\ |$ and let V be a vector space over k. A real-valued function $\|\ \|$ on V is called a norm if*

(1) $\|a\| > 0$ *for* $a \in V$, $a \neq 0$.
(2) $\|a+b\| \leq \|a\| + \|b\|$.
(3) $\|\alpha a\| = |\alpha|\,\|a\|$ $(\alpha \in k,\ a \in V)$.

DEFINITION. *Two norms $\|\ \|_1$, $\|\ \|_2$ on the same space are equivalent if there exist constants c_1, c_2 such that*

$$\|a\|_1 \leq c_1\|a\|_2 \qquad \|a\|_2 \leq c_2\|a\|_1.$$

This is clearly an equivalence relation.

LEMMA. *Suppose that k is complete with respect to $|\ |$ and that V is finite-dimensional. Then any two norms on V are equivalent.*

Note. As we shall see, completeness is essential.

Proof. Let $a_1, \ldots, a_N$ be any basis for V. We define a norm $\|\ \|_0$ by

$$\|\Sigma \xi_n a_n\|_0 = \max_n |\xi_n|.$$

It is enough to show that any norm $\|\ \|$ is equivalent to $\|\ \|_0$. Clearly

$$\|\Sigma \xi_n a_n\| \leq \Sigma |\xi_n|\,\|a_n\| \leq c_1\|\Sigma \xi_n a_n\|_0$$

with

$$c_1 = \Sigma \|a_n\|.$$

Suppose that there is no c_2 such that†

$$\|a\|_0 \leq c_2\|a\|.$$

Then for any $\varepsilon > 0$ there exist $\xi_1, \ldots, \xi_n$ such that

$$0 < \|\Sigma \xi_n a_n\| \leq \varepsilon \max |\xi_n|.$$

By symmetry we may suppose that

$$\max |\xi_n| = |\xi_N|$$

and then by homogeneity that

$$\xi_N = 1.$$

For $m = 1, 2, \ldots$, we thus have $\xi_{n,m}$ $(1 \leq n \leq N-1)$ with

$$\Big\|\sum_{n=1}^{N-1} \xi_{n,m} a_n + a_N\Big\| \to 0 \qquad (m \to \infty);$$

so

$$\Big\|\sum_{n=1}^{N-1} (\xi_{n,\ell} - \xi_{n,m}) a_n\Big\| \to 0 \qquad (\ell, m \to \infty, \infty).$$

The lemma being trivial for $N = 1$, we may suppose by induction that it is true for the $(N-1)$-dimensional space spanned by $a_1, \ldots, a_{N-1}$ and hence

$$|\xi_{n,\ell} - \xi_{n,m}| \to 0 \qquad (\ell, m \to \infty, \infty)$$

for $1 \leq n \leq N-1$. Since k is complete there are $\xi_n^* \in k$ with

$$|\xi_{n,m} - \xi_n^*| \to 0 \qquad (m \to \infty).$$

Then

$$\Big\|\sum^{N-1} \xi_n^* a_n + a_N\Big\| \leq \Big\|\sum^{N-1} \xi_{n,m} a_n + a_n\Big\| + \sum^{N-1} |\xi_n^* - \xi_{n,m}|\,\|a_n\| \to 0 \qquad (m \to \infty)$$

in contradiction to (1), since $\sum \xi_n^* a_n + a_N \neq 0$ but $\|\sum \xi_n^* a_n + a_N\| = 0$.

9. Tensor Product

We need only a special case. Let A, B be commutative rings containing a field k and suppose that B is of finite dimension N over k, say with basis

$$1 = \omega_1, \omega_2, \ldots, \omega_N.$$

Then B is determined up to isomorphism by the multiplication table

$$\omega_\ell \omega_m = \sum c_{\ell m n} \omega_n \qquad c_{\ell m n} \in k.$$

We can define a new ring C containing k whose elements are expressions of

† When k is not merely complete with respect to $|\ |$ but locally compact, which will be the case of primary interest, one can argue more simply as follows. By what has been shown already, the function $\|a\|$ is continuous in the $\|\ \|_0$-topology, and so attains its lower bound δ on $\|a\|_0 = 1$. Then $\delta > 0$ by condition (i), and then $\|a\|_0 \leq \delta^{-1}\|a\|$ by homogeneity for all a.

the type

$$\sum a_m \varpi_m \qquad a_m \in A$$

where the ϖ_m have the same multiplication rule

$$\varpi_\ell \varpi_m = \sum c_{\ell mn} \varpi_n$$

as the ω_m. There are ring isomorphisms

$$i : a \to a\varpi_1$$

and

$$j : \sum \lambda_m \omega_m \to \sum \lambda_m \varpi_m$$

of A and B respectively into C. It is clear that C is defined up to isomorphism by A and B and is independent of the particular choice of basis ω_m. We write

$$C = A \otimes_k B$$

since it is, in fact, a special case of the ring tensor-product.

[The reader will have no difficulty in checking that C together with the maps i, j possesses the defining Universal Mapping Property.]

Let us now suppose, further, that A is a topological ring, i.e. has a topology with respect to which addition and multiplication are continuous. The map

$$\sum a_m \varpi_m \to (a_1, \ldots, a_N)$$

is a $1-1$ correspondence between C and N copies of A (considered as sets). We give C the product topology. It is readily verified (i) that this topology is independent of the choice of basis $\omega_1, \ldots \omega_N$ and (ii) that multiplication and addition in C are continuous with respect to it; i.e. C is now a topological ring.

We shall speak of this topology on C as the tensor product topology.

Now let us drop our supposition that A has a topology but suppose that A, B are not merely rings but fields.

LEMMA. *Let A, B be fields containing the field k and suppose that B is a separable extension of degree $[B:k] = N < \infty$. Then $C = A \otimes_k B$ is the direct sum of a finite number of fields K_j, each containing an isomorphic image of A and an isomorphic image of B.*

Proof. By a well-known theorem (appendix B) we have $B = k(\beta)$ where $f(\beta) = 0$, for some separable $f(X) \in k[X]$ of degree N irreducible in $k[X]$.

Then $1, \beta, \ldots, \beta^{N-1}$ is a basis for B/k and so $A \otimes_k B = A[\bar{\beta}]$ where $1, \bar{\beta}, \ldots, \bar{\beta}^{N-1}$ are linearly independent over A and $f(\bar{\beta}) = 0$.

Although $f(X)$ is irreducible in $k[X]$ it need not be in $A[X]$, say

$$f(X) = \prod_{1 \le j \le J} g_j(X)$$

where $g_j(X) \in A[X]$ is irreducible. The $g_j(X)$ are distinct because $f(X)$ is separable. Let $K_j = A(\beta_j)$ where $g_j(\beta_j) = 0$. Clearly the map

$$A \otimes_k B \xrightarrow{\mu_j} K_j$$

given by

$$h(\bar{\beta}) \xrightarrow{\mu_j} h(\beta_j) \qquad h(X) \in A[X]$$

is a ring homomorphism.

We thus have a ring homomorphism

$$A \otimes_k B \xrightarrow{\mu_1 \oplus \ldots \oplus \mu_J} \bigoplus_{1 \le j \le J} K_j. \tag{9.1}$$

Let $h(\bar{\beta})$, $h(X) \in A[X]$ be in the kernel. Then $h(X)$ is divisible by every $g_j(X)$, so also by $f(X)$, i.e. $h(\bar{\beta}) = 0$. Thus (9.1) is an injection. Since both sides of (9.1) have the same dimension as vector spaces over A it must be an isomorphism, as required.

It remains to show that the ring homomorphisms

$$\lambda_j : B \to A \otimes_k B \xrightarrow{\mu_j} K_j$$

are injections. If $\lambda_j(\beta) \neq 0$ for any $\beta \in B$ then $\lambda_j(\beta_1) \neq 0$ for all $\beta_1 \neq 0$ because $\lambda_j(\beta) = \lambda_j(\beta_1)\lambda_j(\beta\beta_1^{-1})$. Hence all we have to show is that λ_j does not map the whole of B onto 0: and this is trivial.

COROLLARY. *Let $\alpha \in B$ and let $F(X) \in k[X]$, $G_j(X) \in A[X]$ $(1 \le j \le J)$ be the characteristic polynomial of α over k and of the image of α under*

$$B \to A \otimes_k B \to K_j$$

over A respectively. Then

$$F(X) = \prod_{1 \le j \le J} G_j(X). \tag{9.2}$$

Proof. We show that both sides of (9.2) are the characteristic polynomial $T(X)$ of the image of α in $A \otimes_k B$ over A. That $F(X) = T(X)$ follows at once by computing the characteristic polynomial in terms of a basis $\varpi_1, \ldots \varpi_N$, where $\omega_1, \ldots, \omega_{N'}$ is a basis for B/k. That $T(X) = \Pi G_j(X)$ follows similarly by using a base of

$$A \otimes_k B = \oplus K_j$$

composed of bases of the individual K_j/A.

COROLLARY. For $\alpha \in B$ we have

$$\mathrm{Norm}_{B/k}\, \alpha = \prod_{1 \le j \le J} \mathrm{Norm}_{K_j/A}\, \alpha$$

$$\mathrm{Trace}_{B/k}\, \alpha = \sum_{1 \le j \le J} \mathrm{Trace}_{K_j/A}\, \alpha.$$

Proof. For the norm and trace are just the second and the last coefficient in the characteristic equation.

10. Extension of Valuations

Let $k \subset K$ be fields and $|\ |$, $\|\ \|$ be valuations on k, K respectively. We say that $\|\ \|$ extends $|\ |$ if $|b| = \|b\|$ for all $b \in k$.

THEOREM. *Let k be complete with respect to the valuation $|\ |$ and let K be an extension of k with $[K:k] = N < \infty$. Then there is precisely one extension of $|\ |$ to K namely*

$$\|\alpha\| = |\mathrm{Norm}_{K/k}\alpha|^{1/N}. \tag{10.1}$$

Proof. Uniqueness. K may be regarded as a vector space over k and then $\|\ \|$ is a norm in the sense defined earlier. Hence any two extensions $\|\ \|_1$ and $\|\ \|_2$ of $|\ |$ are equivalent as norms and so induce the same topology in K. But as we have seen two valuations which induce the same topology are equivalent valuations, i.e. $\|\ \|_1 = \|\ \|_2^c$ for some c. Finally $c = 1$ because $\|b\|_1 = \|b\|_2$ for all $b \in k$.

Existence. For a proof of existence in the general case see e.g. E. Artin: "Theory of Algebraic Numbers" (Striker, Göttingen) and for a proof valid for separable non-arch. discrete valuations see Chapter I, § 4, Prop. 1, Corollary. Here we give a proof (suggested by Dr. Geyer at the conference) valid when k is locally compact, the only case which will be used. In any case it is easy to see that the definition (10.1) satisfies the conditions (i) that $\|\alpha\| \geq 0$ with equality only for $\alpha = 0$ and (ii) $\|\alpha\beta\| = \|\alpha\|\|\beta\|$: the difficulty is to show that there is a constant C such that $\|\alpha\| \leq 1$ implies $\|1+\alpha\| \leq C$. Let $\|\ \|_0$ be any norm on K considered as a vector space over k. Then $\|\alpha\|$ defined by (10.1) is a continuous non-zero function on the compact set $\|\alpha\|_0 = 1$, so $\Delta \geq \|\alpha\| \geq \delta > 0$ for some constants Δ, δ. Hence by homogeneity

$$\Delta \geq \frac{\|\alpha\|}{\|\alpha\|_0} \geq \delta > 0. \quad (\text{all } \alpha \neq 0).$$

Suppose, now, that $\|\alpha\| \leq 1$. Then $\|\alpha\|_0 \leq \delta^{-1}$ and so

$$\begin{aligned} \|1+\alpha\| &\leq \Delta\|1+\alpha\|_0 \\ &\leq \Delta(\|1\|_0 + \|\alpha\|_0) \\ &\leq \Delta(\|1\|_0 + \delta^{-1}) \\ &= C \quad (\text{say}), \end{aligned}$$

as required.

Formula. Geyer's existence proof also gives (10.1). But it is perhaps worth noting that in any case (10.1) is a consequence of unique existence, as follows. Let $L \supset K$ be a finite normal extension of k. Then by the above there is a unique extension of $|\ |$ to L which we shall denote also by $\|\ \|$. If σ is an automorphism of L/K then

$$\|\alpha\|_\sigma = \|\sigma\alpha\|$$

is also an extension of $|\ |$ to L, so $\|\ \|_\sigma = \|\ \|$, i.e.

$$\|\sigma\alpha\| = \|\alpha\| \quad (\text{all } \alpha \in L).$$

But now

$$\mathrm{Norm}_{K/k}\alpha = \sigma_1\alpha\,\sigma_2\alpha \ldots \sigma_N\alpha$$

for $\alpha \in K$, where $\sigma_1, \ldots, \sigma_N$ are automorphisms of L/k. Hence

$$\begin{aligned} |\mathrm{Norm}_{K/k}\alpha| &= \|\mathrm{Norm}_{K/k}\alpha\| \\ &= \prod_{1 \leq n \leq N} \|\sigma_n\alpha\| \\ &= \|\alpha\|^N, \end{aligned}$$

as required.

COROLLARY. *Let $\omega_1, \ldots, \omega_N$ be a basis for K/k. Then there are constants c_1, c_2 such that*

$$c_1 \leq \frac{|\sum b_n\omega_n|}{\max|b_n|} \leq c_2$$

for $b_1, \ldots, b_N \in k$ (not all 0).

Proof. For $|\sum b_n\omega_n|$ and $\max|b_n|$ are two norms on K considered as a vector space over k.

COROLLARY 2. *A finite extension of a completely valued field k is complete with respect to the extended valuation.*

For by the preceding corollary it has the topology of a finite-dimension vector space over k.

When k is no longer complete under $|\ |$ the position is more complicated:

THEOREM. *Let K be a separable extension of k of degree $[K:k] = N < \infty$. Then there are at most N extensions of a valuation $|\ |$ of k to K, say $\|\ \|_j$ $(1 \leq j \leq J)$. Let $\bar{k}$, K_j be the completion of k resp. K with respect to $|\ |$, resp. $\|\ \|_j$. Then*

$$\bar{k} \otimes_k K = \bigoplus_{1 \leq j \leq J} K_j \tag{10.2}$$

algebraically and topologically, where the R.H.S. is given the product topology.

Proof. We know already that $\bar{k} \otimes K$ is of the shape (10.2) where the K_j are finite extensions of $\bar{k}$. Hence there is a unique extension $|\ |_j^*$ of $|\ |$ to the K_j and the K_j are complete with respect to the extended valuation. Further, by a previous proof, the ring homomorphisms

$$\lambda_j : K \to \bar{k} \otimes_k K \to K_j$$

are injections. Hence we get an extension $\|\ \|_j$ of $|\ |$ to K by putting

$$\|\beta\|_j = |\lambda_j(\beta)|_j^*.$$

Further, $K \cong \lambda_j(K)$ is dense in K_j with respect to $\|\ \|_j$ because $K = k \otimes_k K$ is dense in $\bar{k} \otimes_k K$. Hence K_j is exactly the completion of K.

It remains to show that the $\| \|_j$ are distinct and that they are the only extensions of $|\ |$ to K.

Let $\| \|$ be any valuation of K extending $|\ |$. Then $\| \|$ extends by continuity to a real-valued function of $\bar{k} \otimes_k K$, a function also to be denoted by $\| \|$. By continuity we have

$$\left.\begin{aligned} \|\alpha+\beta\| &\le \max \|\alpha\|, \|\beta\| \\ \|\alpha\beta\| &= \|\alpha\| \|\beta\| \end{aligned}\right\} \quad \alpha, \beta \in \bar{k} \otimes K.$$

We consider the restriction of $\| \|$ to one of the K_j. If $\|\alpha\| \neq 0$ for some $\alpha \in K_j$ then $\|\alpha\| = \|\beta\| \|\alpha\beta^{-1}\|$ for every $\beta \neq 0$ in K_j so $\|\beta\| \neq 0$. Hence either $\| \|$ is identically 0 on K_j or it induces a valuation on K_j.

Further, $\| \|$ cannot induce a valuation on *two* of the K_j. For

$$(\alpha_1 \oplus 0 \oplus \ldots \oplus 0).(0 \oplus \alpha_2 \oplus 0 \ldots \oplus 0) = (0 \oplus 0 \ldots \oplus 0)$$

and so

$$\|\alpha_1\| \|\alpha_2\| = 0 \qquad \alpha_1 \in K_1, \quad \alpha_2 \in K_2.$$

Hence $\| \|$ induces a valuation in precisely one of the K_j and it clearly extends the given valuation $|\ |$ of $\bar{k}$. Hence $\| \| = \| \|_j$ for precisely one j.

It remains only to show that (10.2) is also a topological homomorphism. For $(\beta_1, \ldots, \beta_J) \in K_1 \oplus \ldots \oplus K_J$ put

$$\|(\beta_1, \ldots, \beta_J)\|_0 = \max_{1 \le j \le J} \|\beta_j\|_j.$$

Clearly, $\| \|_0$ is a norm on the R.H.S. of (10.2), considered as a vector space over $\bar{k}$ and it induces the product topology. On the other hand, any two norms are equivalent, since $\bar{k}$ is complete, and so $\| \|_0$ induces the tensor product topology on the left-hand side of (10.2).

COROLLARY. *Let $K = k(\beta)$ and let $f(x) \in k[X]$ be the irreducible equation for β. Suppose that*

$$f(X) = \prod_{1 \le j \le J} g_j(X)$$

in $\bar{k}[X]$, where the g_j are irreducible. Then $K_j = \bar{k}(\beta_j)$ where $g_j(\beta_j) = 0$.

11. Extensions of Normalized Valuations

Let k be a field with valuation $|\ |$. We consider the three cases:

(1) $|\ |$ is discrete non-arch. and the residue class field is finite.
(2(i)) The completion of k with respect to $|\ |$ is **R**.
(2(ii)) The completion of k with respect to $|\ |$ is **C**.

[In virtue of the remarks in § 7, these cases can be subsumed in one: the completion $\bar{k}$ is locally compact.]

In case (1) we have already defined a normalized valuation (§ 7). In case (2(i)) we say $|\ |$ is normalized if it is the ordinary absolute value and in

case (2(ii)) if it is the *square* of the absolute value. Thus in every case the map

$$\alpha : \xi \to \alpha\xi \qquad \xi \in \bar{k}^+ \quad (\alpha \in \bar{k})$$

of the additive group $\bar{k}^+$ of the completion of k multiplies the Haar measure on $\bar{k}^+$ by $|\alpha|$: and this characterizes the normalized valuation among equivalent ones.

LEMMA. *Let k be complete with respect to the normalized valuation $|\ |$ and let K be an extension of k of degree $[K:k] = N < \infty$. Then the normalized valuation $\| \|$ of K which is equivalent to the unique extension of $|\ |$ to K is given by the formula*

$$\|\alpha\| = |\mathrm{Norm}_{K/k}\alpha| \qquad (\alpha \in K).$$

Proof. By the preceding section we have

$$\|\alpha\| = |\mathrm{Norm}_{K/k}\alpha|^c \qquad (\alpha \in K) \tag{11.1}$$

for some real $c > 0$ and all we have to do is to prove that $c = 1$. This is trivial in case 2 and follows from the structure theorems of Chapter I in case 1. Alternatively one can argue in a unified way as follows. Let $\omega_1, \ldots, \omega_N$ be a basis for K/k. Then the map

$$\Xi = \sum \xi_n \omega_n \leftrightarrow (\xi_1, \ldots, \xi_N) \qquad (\xi_1, \ldots, \xi_N \in k)$$

gives an isomorphism between the additive group K^+ and the direct sum $\oplus^N k^+$ of N copies of k^+, and this is a homeomorphism if the R.H.S. is given the product topology. In particular, the Haar measures on K^+ and $\oplus^N k^+$ are the same up to a multiplicative constant. Let $b \in k$. Then the map

$$b : \Xi \to b\Xi$$

of K^+ is the same as the map

$$(\xi_1, \ldots, \xi_N) \to (b\xi_1, \ldots, b\xi_N)$$

of $\oplus^N k^+$ and so multiplies the Haar measure by $|b|^N$, since $|\ |$ is normalized. Hence

$$\|b\| = |b|^N.$$

But $\mathrm{Norm}_{K/L} b = b^N$ and so $c = 1$ in (11.1).

In the incomplete case we have

THEOREM. *Let $|\ |$ be a normalized valuation of a field k and let K be a finite extension of k. Then*

$$\prod_{1 \le j \le J} \|\alpha\|_j = |\mathrm{Norm}_{K/k}\alpha|,$$

where the $\| \|_j$ are the normalized valuations equivalent to the extensions of $|\ |$ to K.

Proof. Let

$$\bar{k} \otimes_k K = \bigoplus_{1 \le j \le J} K_j,$$

where $\bar{k}$ is the completion of K. Then (§ 9)

$$\mathrm{Norm}_{K/k}\alpha = \prod_{1 \le j \le J} (\mathrm{Norm}_{K_j/\bar{k}}\alpha).$$

The theorem now follows from the preceding lemma and the results of § 10.

12. Global Fields

By a global field k we shall mean either a finite extension of the rational field $\mathbf{Q}$ or a finite separable† extension of $\mathbf{F}(t)$, where $\mathbf{F}$ is a finite field and t is transcendental over $\mathbf{F}$. We shall focus attention in the exposition on the extensions of $\mathbf{Q}$ (algebraic number case) leaving the extension of $\mathbf{F}(t)$ (function field case) to the reader.

LEMMA. *Let $\alpha \neq 0$ be in the global field k. Then there are only finitely many unequivalent valuations $|\ |$ of k for which*

$$|\alpha| > 1.$$

Proof. We know this already for $\mathbf{Q}$ and $\mathbf{F}(t)$. Let k be a finite extension of $\mathbf{Q}$, so

$$\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0$$

for some n and $a_1, \ldots, a_n$. If $|\ |$ is a non-arch. valuation of k we have

$$\begin{aligned} |\alpha|^n &= |-a_1\alpha^{n-1} - \ldots - a_n| \\ &\le \max(1, |\alpha|^{n-1}) \max(|a_1|, \ldots, |a_n|) \end{aligned}$$

and so

$$|\alpha| \le \max(1, |a_1|, \ldots, |a_n|).$$

Since every valuation of $\mathbf{Q}$ has finitely many extensions to k and since there are only finitely many arch. valuations altogether, the theorem for k follows from that for $\mathbf{Q}$.

All the valuations of a global field k are of the type described in § 11, since this is true of $\mathbf{Q}$ and $\mathbf{F}(t)$. Hence it makes sense to talk of normalized valuations.

THEOREM. *Let $\alpha \in k$, where k is a global field and $\alpha \neq 0$. Let $|\ |_v$ run through all the normalized valuations of k. Then $|\alpha|_v = 1$ for all except finitely many v and*

$$\prod_v |\alpha|_v = 1.$$

Note. We shall later give a less computational proof of this.

† This condition is not really necessary. If k is any finite extension of $\mathbf{F}(t)$ there is a "separating element" s, i.e. an $s \in k$ such that k is a finite separable extension of $\mathbf{F}(s)$.

Proof. By the lemma $|\alpha|_v \le 1$ for almost all v (i.e. all except finitely many). Similarly $|\alpha^{-1}|_v \le 1$ for almost all v, so $|\alpha|_v = 1$ for almost all v.

Let V run through all the normalized valuations of $\mathbf{Q}$ [or $\mathbf{F}(t)$] and write $v|V$ to mean that the restriction of v to $\mathbf{Q}$ is equivalent to V. Then

$$\prod_v |\alpha|_v = \prod_V \Big(\prod_{v|V} |\alpha|_v \Big) = \prod_V |\mathrm{Norm}_{k/\mathbf{Q}}\alpha|_V,$$

by the preceding section. This reduces the theorem to the case $k = \mathbf{Q}$. But if now

$$b = \pm \prod_p p^{\beta_p} \in \mathbf{Q},$$

where p runs through all the primes and $\beta_p \in \mathbf{Z}$, we have

$$|b|_p = p^{-\beta_p}$$

for the p-adic valuation $|\ |_p$ and

$$|b|_\infty = \prod_p p^{\beta_p}$$

for the absolute value $|\ |_\infty$. Q.E.D.

Let K be a finite separable extension of the global field k. Then for every valuation v of k we have an isomorphism

$$k_v \otimes_k K = K_1 \oplus \ldots \oplus K_J$$

where k_v is the completion of k with respect to v and $K_1, \ldots, K_J$, are the completions of K with respect to the extensions $V_1, \ldots, V_J$ of v to K (§ 10), the number $J = J(v)$ depending on v. We shall later need the

LEMMA. *Let $\omega_1, \ldots, \omega_N$ be a basis for K/k. Then for almost all normalized v we have*

$$\omega_1\mathfrak{o} \oplus \omega_2\mathfrak{o} \oplus \ldots \oplus \omega_N\mathfrak{o} = \mathfrak{O}_1 \oplus \ldots \oplus \mathfrak{O}_J \tag{12.1}$$

where $N = [K:k]$, $\mathfrak{o} = \mathfrak{o}_v$ is the ring of integers of k_v for $|\ |_v$ and $\mathfrak{O}_j \subset K_j$ is the ring of integers for $|\ |_{V_j}$ $(1 \le j \le J)$. Here we have identified $\alpha \in K$ with its canonical image in $k_v \otimes K$.

Proof. The L.H.S. of (12.1) is included in the R.H.S. provided that $|\omega_n|_{V_j} \le 1$ $(1 \le n \le N,\ 1 \le j \le J)$. Since $|\alpha|_V \le 1$ for almost all V it follows that L.H.S. $\subset$ R.H.S. for almost all v.

To get an inclusion the other way we use the discriminant

$$D(\gamma_1, \ldots, \gamma_N) = \det_{m,n}(\mathrm{trace}_{K/k}\gamma_m\gamma_n),$$

where $\gamma_1, \ldots, \gamma_N \in k_v \otimes_k K$. If $\gamma_n \in$ R.H.S. $(1 \le n \le N)$ we have (§ 9)

$$\mathrm{trace}_{K/k}\gamma_m\gamma_n = \sum_{1 \le j \le J} \mathrm{trace}_{K_j/k}\gamma_m\gamma_n \in \mathfrak{o} = \mathfrak{o}_v$$

and so

$$D(\gamma_1, \ldots, \gamma_N) \in \mathfrak{o}_v.$$

Now suppose that $\alpha \in$ R.H.S. and that

$$\beta = \sum_1^N b_n \omega_n \in \text{R.H.S.} \quad (b_n \in k_v). \tag{12.2}$$

Then for any m, $1 \le m \le N$ we have

$$D(\omega_1, \ldots, \omega_{m-1}, \beta, \omega_{m+1}, \ldots, \omega_N) = b_m^2 D(\omega_1, \ldots, \omega_N),$$

and so

$$d b_m^2 \in \mathfrak{o}_v \quad (1 \le m \le N)$$

where

$$d = D(\omega_1, \ldots, \omega_N) \in k.$$

But (Appendix B) we have $d \neq 0$, and so $|d|_v = 1$ for almost all v. For almost all v the condition (12.2) thus implies

$$b_m \in \mathfrak{o}_v \quad (1 \le m \le N),$$

i.e.

$$\text{R.H.S.} \subset \text{L.H.S.}$$

This proves the lemma.

[COROLLARY. *Almost all v are unramified in the extension K/k.*
For by the results of Chapter I a necessary and sufficient condition for v to be unramified is that there are $\gamma_1, \ldots, \gamma_N \in$ R.H.S. with $|D(\gamma_1, \ldots, \gamma_N)|_v = 1$. And for almost all v we can put $\gamma_n = \alpha^{n-1}$.]

13. Restricted Topological Product

We describe here a topological tool which will be needed later:

DEFINITION. *Let Ω_λ ($\lambda \in \Lambda$) be a family of topological spaces and for almost all† λ let $\Theta_\lambda \subset \Omega_\lambda$ be an open subset of Ω_λ. Consider the space Ω whose points are sets $\alpha = \{\alpha_\lambda\}_{\lambda \in \Lambda}$, where $\alpha_\lambda \in \Omega_\lambda$ for every λ and $\alpha_\lambda \in \Theta_\lambda$ for almost all λ. We give Ω a topology by taking as a basis of open sets the sets*

$$\prod \Gamma_\lambda$$

where $\Gamma_\lambda \subset \Omega_\lambda$ is open for all λ and $\Gamma_\lambda = \Theta_\lambda$ for almost all λ. With this topology Ω is the restricted topological product of the Ω_λ with respect to the Θ_λ.

COROLLARY. *Let S be a finite subset of Λ and let Ω_S be the set of $\alpha \in \Omega$ with $\alpha_\lambda \in \Theta_\lambda$ ($\lambda \notin S$), i.e.*

$$\Omega_S = \prod_{\lambda \in S} \Omega_\lambda \times \prod_{\lambda \notin S} \Theta_\lambda. \tag{13.1}$$

Then Ω_S is open in Ω and the topology induced in Ω_S as a subset of Ω is the same as the product topology.

Beweis. Klar.

The restricted topological product depends on the totality of the Θ_λ but not on the individual Θ_λ:

† i.e. all except possibly finitely many.

LEMMA. *Let $\Theta'_\lambda \subset \Omega_\lambda$ be open sets defined for almost all λ and suppose that $\Theta_\lambda = \Theta'_\lambda$ for almost all λ. Then the restricted product of the Ω_λ with respect to the Θ'_λ is the same as† the restricted product with respect to the Θ_λ.*

Beweis. Klar.

LEMMA. *Suppose that the Ω_λ are locally compact and that the Θ_λ are compact. Then Ω is locally compact.*

Proof. The Ω_S are locally compact by (13.1) since S is finite. Since $\Omega = \cup \Omega_S$ and the Ω_S are open in Ω, the result follows.

DEFINITION. *Suppose that measures μ_λ are defined on the Ω_λ with $\mu_\lambda(\Theta_\lambda) = 1$ when Θ_λ is defined. We define the product measure μ on Ω to be that for which a basis of measurable sets is the*

$$\prod_\lambda M_\lambda$$

where $M_\lambda \subset \Omega_\lambda$ has finite μ_λ-measure and $M_\lambda = \Theta_\lambda$ for almost all λ and where

$$\mu\left(\prod_\lambda M_\lambda\right) = \prod_\lambda \mu_\lambda(M_\lambda).$$

COROLLARY. *The restriction of μ to Ω_S is just the ordinary product measure.*

14. Adele Ring (or Ring of Valuation Vectors)

Let k be a global field. For each normalized valuation $|\ |_v$ of k denote by k_v the completion of k. If $|\ |_v$ is non-archimedean denote by $\mathfrak{o}_v$ the ring of integers of k_v. The adele ring V_k of k is the topological ring whose underlying topological space is the restricted product of the k_v with respect to the $\mathfrak{o}_v$ and where addition and multiplication are defined componentwise:

$$(\alpha\beta)_v = \alpha_v \beta_v \qquad (\alpha+\beta)_v = \alpha_v + \beta_v \qquad \alpha, \beta \in V_k. \tag{14.1}$$

It is readily verified (i) that this definition makes sense, i.e. if $\alpha, \beta \in V_k$ then $\alpha\beta$, $\alpha+\beta$ whose components are given by (14.1) are also in V_k and (ii) that addition and multiplication are continuous in the V_k-topology, so V_k is a topological ring, as asserted.

V_k is locally compact because the k_v are locally compact and the $\mathfrak{o}_v$ are compact (§ 7).

There is a natural mapping of k into V_k which maps $\alpha \in k$ into the adele every one of whose components is α: this *is* an adele because $\alpha \in \mathfrak{o}_v$ for almost all v. The map is an injection, because the map of k into any k_v is an injection. The image of k under this injection is the ring of *principal adeles*. It will cause no trouble to identify k with the principal adeles, so we shall speak of k as a subring of V_k.

LEMMA. *Let K be a finite (separable) extension of the global field k. Then*

$$V_k \otimes_k K = V_K \tag{14.2}$$

† A purist would say "canonically isomorphic to".

algebraically and topologically. In this correspondence $k \otimes_k K = K \subset V_k \otimes_k K$, *where* $k \subset V_k$, *is mapped identically on to* $K \subset V_K$.

Proof. We first establish an isomorphism of the two sides of (14.2) as topological spaces. Let $\omega_1, \ldots, \omega_N$ be a basis for K/k and let v run through the normalized valuations of k. It is easy to see that the L.H.S. of (14.2), with the tensor product topology, is just the restricted product of the

$$k_v \otimes_k K = k_v\omega_1 \oplus \ldots \oplus k_v\omega_N \tag{14.3}$$

with respect to the

$$\mathfrak{o}_v\omega_1 \oplus \ldots \oplus \mathfrak{o}_v\omega_N. \tag{14.4}$$

But now (cf. §10), (14.3) is just

$$K_{V_1} \oplus \ldots \oplus K_{V_J}, \quad (V_1|v, \ldots, V_J|v) \tag{14.5}$$

where $V_1, \ldots, V_J$, $J = J(v)$ are the normalized extensions of v to K. Further (§ 12) the identification of (14.3) with (14.5) identifies (14.4) with

$$\mathfrak{O}_{V_1} \oplus \ldots \oplus \mathfrak{O}_{V_J} \tag{14.6}$$

for almost all† v. Hence the L.H.S. of (14.2) is the restricted product of (14.3) with respect to (14.4), which is clearly the same thing as the restricted product of the K_V with respect to the $\mathfrak{O}_V$, where V runs through all the normalized valuations of K. This is just the R.H.S. of (14.2). This establishes an isomorphism between the two sides of (14.2) as topological spaces. A moment's consideration shows that it is also an algebraic isomorphism. Q.E.D.

COROLLARY. *Let* V_k^+ *denote the topological group obtained from* V_k *by forgetting the multiplicative structure. Then*

$$V_K^+ = \underbrace{V_k^+ \oplus \ldots \oplus V_k^+}_{N \text{ summands}} \quad (N = [K : k]).$$

In this isomorphism the additive group $K^+ \subset V_K^+$ *of the principal adeles is mapped into* $k^+ \oplus \ldots \oplus k^+$, *in an obvious notation.*

Proof. $\omega V_k^+ \subset V_K^+$, for any non-zero $\omega \in K$, is clearly isomorphic to V_k^+ as a topological group. Hence we have the isomorphisms

$$V_K^+ = V_k^+ \otimes_k K = \omega_1 V_k^+ \oplus \ldots \oplus \omega_N V_k^+ = V_k^+ \oplus \ldots \oplus V_k^+.$$

THEOREM. *k is discrete*‡ *in* V_k *and* V_k^+/k^+ *is compact in the quotient topology.*

Proof. The preceding corollary (with k for K and $\mathbf{Q}$ or $\mathbf{F}(t)$ for k) shows that it is enough to verify the theorem for $\mathbf{Q}$ or $\mathbf{F}(t)$ and we shall do it for $\mathbf{Q}$.

To show that $\mathbf{Q}^+$ is discrete in $V_{\mathbf{Q}}^+$ it is enough because of the group

† This was proved there only when $\omega_n = \alpha^{n-1}$, where $K = k(\alpha)$. We should therefore take this choice of ω_n.

‡ It is impossible to conceive of any other uniquely defined topology in k. This meta-mathematical reason is more persuasive than the argument that follows!

structure to find a neighbourhood U of 0 which contains no other elements of $\mathbf{Q}^+$. We take for U the set of $\alpha = \{\alpha_v\} \in V_{\mathbf{Q}}^+$ with

$$|\alpha_\infty|_\infty < 1$$
$$|\alpha_p|_p \leq 1 \quad \text{(all } p\text{)},$$

where $|\ |_p$, $|\ |_\infty$ are respectively the p-adic and the absolute values on $\mathbf{Q}$.

If $b \in \mathbf{Q} \cap U$ then in the first place $b \in \mathbf{Z}$ (because $|b|_p \leq 1$ for all p) and then $b = 0$ because $|b|_\infty < 1$.

Now let $W \subset V_{\mathbf{Q}}^+$ consists of the $\alpha = \{\alpha_v\}$ with

$$|\alpha_\infty|_\infty \leq \tfrac{1}{2}, \quad |\alpha_p|_p \leq 1 \quad \text{(all } p\text{)}.$$

We show that every adele β is of the shape

$$\beta = b + \alpha, \qquad b \in \mathbf{Q}, \quad \alpha \in W. \tag{14.7}$$

For each p we can find an

$$r_p = z_p/p^{x_p} \qquad (z_p \in \mathbf{Z}, \quad x_p \in \mathbf{Z}, \quad x_p \geq 0)$$

such that

$$|\beta_p - r_p|_p \leq 1$$

and since β is an adele we may take

$$r_p = 0 \quad \text{(almost all } p\text{)}.$$

Hence $r = \sum_p r_p$ is well defined and

$$|\beta_p - r| \leq 1 \quad \text{(all } p\text{)}.$$

Now choose $s \in \mathbf{Z}$ such that

$$|\beta_\infty - r - s| \leq \tfrac{1}{2}.$$

Then $b = r + s$, $\alpha = \beta - b$ do what is required.

Hence the continuous map $W \to V_{\mathbf{Q}}^+/\mathbf{Q}^+$ induced by the quotient map $V_{\mathbf{Q}}^+ \to V_{\mathbf{Q}}^+/\mathbf{Q}^+$ is surjective. But W is compact (topological product of $|\alpha_\infty|_\infty \leq \frac{1}{2}$ and the $\mathfrak{o}_p$) and hence so is $V_{\mathbf{Q}}^+/\mathbf{Q}^+$.

As already remarked, V_k^+ is a locally compact group and so it has an invariant (Haar) measure. It is easy to see that in fact this Haar measure is the product of the Haar measures on the k_v in the sense described in the previous section.

COROLLARY 1. *There is a subset* W *of* V_k *defined by inequalities of the type* $|\xi_v|_v \leq \delta_v$, *where* $\delta_v = 1$ *for almost all* v, *such that every* $\varphi \in V_k$ *can be put in the form*

$$\varphi = \theta + \gamma, \qquad \theta \in W, \quad \gamma \in k$$

Proof. For the W constructed in the proof is clearly contained in some W of the type described above.

COROLLARY 2. V_k^+/k^+ *has finite measure in the quotient measure induced by the Haar measure on* V_k^+.

Note. This statement is, of course, independent of the particular choice of the multiplicative constant in the Haar measure on V_k^+. We do not here go into the question of finding the measure of V_k^+/k^+ in terms of our explicitly given Haar measure. (See Tate's thesis, Chapter XV of this book.)

Proof. This can be reduced similarly to the case of $\mathbf{Q}$ or $\mathbf{F}(t)$, which is almost immediate: thus W defined above has measure 1 for our Haar measure.

Alternatively finite measure follows from compactness. For cover V_k^+/k^+ with the translates of F, where F is an open set of finite measure. The existence of a finite subcover implies finite measure.

[We give an alternative proof of the product formula $\Pi\,|\xi|_v = 1$ for $\xi \in k$, $\xi \neq 0$. We have seen that if $\beta_v \in k_v$ then multiplication by β_v magnifies the Haar measure in k_v^+ by the factor $|\beta_v|_v$. Hence if $\beta = \{\beta_v\} \in V_k$, multiplication by β magnifies Haar measure in V_k^+ by $\Pi\,|\beta_v|_v$. In particular multiplication by the principal adele ξ magnifies Haar measure by $\Pi\,|\xi|_v$. But now multiplication by ξ takes $k^+ \subset V_k^+$ into k^+ and so gives a well-defined $1-1$ map of V_k^+/k^+ onto V_k^+/k^+ which magnifies the measure by the factor $\Pi\,|\xi|_v$. Hence $\Pi\,|\xi|_v = 1$ by the Corollary.]

In the next section we shall need the

LEMMA. *There is a constant $C > 0$ depending only on the global field k with the following property:*

Let $\alpha = \{\alpha_v\} \subset V_k$ be such that

$$\prod_v |\alpha_v|_v > C. \tag{14.8}$$

Then there is a principal adele $\beta \in k \subset V_k$, $\beta \neq 0$ such that

$$|\beta|_v \leq |\alpha_v|_v \quad \text{(all } v\text{)}.$$

Proof. This is modelled on Blichfeldt's proof of Minkowski's Theorem in the Geometry of Numbers and works in quite general circumstances.

Note that (14.8) implies $|\alpha_v|_v = 1$ for almost all v because $|\alpha_v|_v \leq 1$ for almost all v.

Let c_0 be the Haar measure of V_k^+/k^+ and let c_1 be that of the set of $\gamma = \{\gamma_v\} \subset V_k^+$ with

$$|\gamma_v|_v \leq \tfrac{1}{10} \quad \text{if } v \text{ is arch.}$$
$$|\gamma_v|_v \leq 1 \quad \text{if } v \text{ is non-arch.}$$

Then $0 < c_0 < \infty$ and $0 < c_1 < \infty$ because the number of arch. v's is finite. We show that

$$C = c_0/c_1$$

will do.

The set T of $\tau = \{\tau_v\} \subset V_k^+$ with

$$|\tau_v|_v \leq \tfrac{1}{10}|\alpha_v|_v \quad \text{if } v \text{ is arch.}$$
$$|\tau_v|_v \leq |\alpha_v|_v \quad \text{if } v \text{ is non-arch.}$$

has measure

$$c_1 \prod_v |\alpha_v|_v > c_1 C = c_0.$$

Hence in the quotient map $V_k^+ \to V_k^+/k^+$ there must be a pair of distinct points of T which have the same image in V_k^+/k^+, say

$$\tau' = \{\tau_v'\} \in T, \qquad \tau'' = \{\tau_v''\} \in T$$

and

$$\tau' - \tau'' = \beta \text{ (say)} \in k^+.$$

Then

$$|\beta|_v = |\tau_v' - \tau_v''|_v \leq |\alpha_v|_v$$

for all v, as required.

COROLLARY. *Let v_0 be a normalized valuation and let $\delta_v > 0$ be given for all $v \neq v_0$ with $\delta_v = 1$ for almost all v. Then there is a $\beta \in k$, $\beta \neq 0$ with*

$$|\beta|_v \leq \delta_v \quad (\text{all } v \neq v_0).$$

Proof. This is just a degenerate case. Choose $\alpha_v \in k_v$ with $0 < |\alpha_v|_v \leq \delta_v$ and $|\alpha_v|_v = 1$ if $\delta_v = 1$. We can then choose $\alpha_{v_0} \in k_{v_0}$ so that $\prod_{\text{all } v \text{ inc. } v_0} |\alpha_v|_v > C$. Then the lemma does what is required.

[The character group of the locally compact group V_k^+ is isomorphic to V_k^+ and k^+ plays a special role. See Chapter XV (Tate's thesis), Lang: "Algebraic Numbers" (Addison-Wesley), Weil: "Adeles and Algebraic Groups" (Princeton lecture notes) and Godement: Bourbaki seminars 171 and 176. This duality lies behind the functional equation of ζ and L-functions. Iwasawa has shown (*Annals of Math.*, **57** (1953), 331–356) that the rings of adeles are characterized by certain general topologico-algebraic properties.]

15. Strong Approximation Theorem

The results of the previous section, in particular the discreteness of k in V_k depend critically on the fact that *all* normalized valuations are used in the definition of V_k:

THEOREM. (Strong approximation theorem.) *Let v_0 be any valuation of the global field k. Define $\mathcal{V}$ to be the restricted topological product of the k_v with respect to the $\mathfrak{o}_v$, where v runs through all normalized $v \neq v_0$. Then k is everywhere dense in $\mathcal{V}$.*

Proof.† It is easy to see that the theorem is equivalent to the following statement. Suppose we are given (i) a finite set S of valuations $v \neq v_0$, (ii) elements $\alpha_v \in k_v$ for all $v \in S$ and (iii) $\varepsilon > 0$. Then there is a $\beta \in k$ such that $|\beta - \alpha_v|_v < \varepsilon$ for all $v \in S$ and $|\beta|_v \leq 1$ for all $v \notin S$, $v \neq v_0$.

By Corollary 1 to the Theorem of § 14 there is a $W \subset V_k$ defined by inequalities of the type $|\xi_v|_v \leq \delta_v$ ($\delta_v = 1$ for almost all v) such that every

† Suggested by Prof. Kneser at the Conference.

$\varphi \in V_k$ is of the form

$$\varphi = \theta + \gamma, \qquad \theta \in W, \quad \gamma \in k. \tag{15.1}$$

By the corollary to the last lemma of §14, there is a $\lambda \in k$, $\lambda \neq 0$ such that

$$\begin{aligned} |\lambda|_v &< \delta_v^{-1}\varepsilon \quad (v \in S), \\ |\lambda|_v &\leq \delta_v^{-1} \quad (v \notin S, v \neq v_0). \end{aligned} \tag{15.2}$$

Hence, on putting $\varphi = \lambda^{-1}\alpha$ in (15.1) and multiplying by λ we see that every $\alpha \in V_k$ is of the shape

$$\alpha = \psi + \beta, \qquad \psi \in \lambda W, \quad \beta \in k, \tag{15.3}$$

where λW is the set of $\lambda\xi$, $\xi \in W$. If now we let α have components the given α_v at $v \in S$ and (say) 0 elsewhere, it is easy to see that β has the properties required.

[The proof clearly gives a quantitative form of the theorem (i.e. with a bound for $|\beta|_{v_0}$). For an alternative approach, see K. Mahler: Inequalities for ideal bases, *J. Australian Math. Soc.* **4** (1964), 425–448.]

16. Idele Group

The set of invertible elements of any commutative topological ring R form a group $R^\times$ under multiplication. In general, $R^\times$ is not a topological group if it is endowed with the subset topology because inversion need not be continuous. It is usual therefore to give $R^\times$ the following topology. There is an injection

$$x \to (x, x^{-1}) \tag{16.0}$$

of $R^\times$ into the topological product $R \times R$. We give to $R^\times$ the corresponding subset topology. Clearly $R^\times$ with this topology is a topological group and the inclusion map $R^\times \to R$ is continuous.

DEFINITION. *The idele group J_k of k is the group $V_k^\times$ of invertible elements of the adele ring V_k with the topology just defined.*

We shall usually speak of J_k as a subset of V_k and will have to distinguish between the J_k- and V_k-topologies.†

We have seen that k is naturally embedded in V_k and so $k^\times$ is naturally embedded in J_k. We shall call $k^\times$ considered as a subgroup of J_k the *principal* ideles.

LEMMA. *$k^\times$ is a discrete subgroup of J_k.*

Proof. For k is discrete in V_k and so $k^\times$ is injected into $V_k \times V_k$ by (16.0) as a discrete subset.

LEMMA. *J_k is just the restricted topological product of the $k_v^\times$ with respect to the units $U_v \subset k_v$ (with the restricted product topology).*

Beweis. Klar.

† Let $\alpha^{(q)}$ for a rational prime q be the element of J_Q with components $\alpha_q^{(q)} = q$, $\alpha_v^{(q)} = 1$ $(v \neq q)$. Then $\alpha^{(q)} \to 1$ $(q \to \infty)$ in the V_Q-topology, but not in the J_Q-topology.

DEFINITION. *For $\alpha = \{\alpha_v\} \subset J_k$ we define $c(\alpha) = \prod_{\text{all } v} |\alpha_v|_v$ to be the content of α.*

LEMMA. *The map $\alpha \to c(\alpha)$ is a continuous homomorphism of the topological group J_k into the multiplicative group of the (strictly) positive real numbers.*

Beweis. Klar.

[*Lemma.* Let $\alpha \in J_k$. Then the map $\xi \to \alpha\xi$ of V_k^+ onto itself multiplies Haar measure on V_k^+ by a factor $c(\alpha)$.

Beweis. Klar.

Note also that the J_k-topology is that appropriate to a group of operators on V_k^+: a basis of open sets is the $S(C, O)$ where $C, O \subset V_k^+$ are respectively V_k-compact and V_k-open and S consists of the $\alpha \in J_k$ such that $(1 - \alpha)C \subset O$, $(1 - \alpha^{-1})C \subset O$.]

Let J_k^1 be the kernel of the map $\alpha \to c(\alpha)$ with the topology as a subset of J_k. We shall need the

LEMMA. *J_k^1 considered as a subset of V_k is closed and the V_k-subset topology on J_k^1 coincides with the J_k-topology.*

Proof. Let $\alpha \in V_k$, $\alpha \notin J_k^1$. We must find a V_k-neighbourhood W of α which does not meet J_k^1.

1st Case. $\prod |\alpha_v|_v < 1$ (possibly $= 0$). Then there is a finite set S of v such that

(i) S contains all the v with $|\alpha_v|_v > 1$ and

(ii) $\prod_{v \in S} |\alpha_v|_v < 1$. Then the set W can be defined by

$$\begin{aligned} |\xi_v - \alpha_v|_v &< \varepsilon \quad v \in S \\ |\xi_v|_v &\leq 1 \quad v \notin S \end{aligned}$$

for sufficiently small ε.

2nd Case. $\prod_v |\alpha_v|_v = C$ (say) > 1. Then there is a finite set S of v such that (i) S contains all the v with $|\alpha_v|_v > 1$ and (ii) if $v \notin S$ an inequality $|\xi_v|_v < 1$ implies† $|\xi_v|_v < \frac{1}{2}C$. We can choose ε so small that $|\xi_v - \alpha_v|_v < \varepsilon$ $(v \in S)$ implies $1 < \prod_{v \in S} |\xi_v| < 2C$. Then W may be defined by

$$\begin{aligned} |\xi_v - \alpha_v|_v &< \varepsilon \quad (v \in S) \\ |\xi_v| &\leq 1 \quad (v \notin S). \end{aligned}$$

We must now show that the J_k- and V_k-topologies on J_k^1 are the same. If $\alpha \in J_k^1$ we must show that every J_k-neighbourhood of α contains a V_k-neighbourhood and vice-versa.

Let‡ $W \subset J_k^1$ be a V_k-neighbourhood of α. Then it contains a V_k-neigh-

† If $k \supset \mathbf{Q}$ and v is a normalized extension of the p-adic valuation then the value group of v consists of (some of the) powers of p. Hence it is enough for (ii) to include in S all the arch. v and all the extensions of p-adic valuations with $p \leq 2C$. Similarly if $k \supset \mathbf{F}(t)$.

‡ This half of the proof of the equality of the topologies makes no use of the special properties of ideles. It is only an expression of the fact noted above that the inclusion $R^\times \to R$ is continuous for any topological ring R.

bourhood of the type

$$\left.\begin{aligned} |\xi_v - \alpha_v|_v &< \varepsilon \quad (v \in S) \\ |\xi_v|_v &\leq 1 \quad (v \notin S) \end{aligned}\right\} \tag{16.1}$$

where S is a finite set of v. This contains the J_k-neighbourhood in which $\leq$ in (16.1) is replaced by $=$.

Now let $H \subset J_k^1$ be a J_k-neighbourhood. Then it contains a J_k-neighbourhood of the type

$$\left.\begin{aligned} |\xi_v - \alpha_v|_v &< \varepsilon \quad (v \in S) \\ |\xi_v|_v &= 1 \quad (v \notin S) \end{aligned}\right\} \tag{16.2}$$

where the finite set S contains at least all arch. v and all v with $|\alpha_v|_v \neq 1$. Since $\prod |\alpha_v|_v = 1$ we may also suppose that ε is so small that (16.2) implies

$$\prod_v |\xi_v|_v < 2.$$

Then the intersection of (16.2) with J_k^1 is the same† as that of (16.1) with J_k^1, i.e. (16.2) defines a V_k-neighbourhood.

By the product formula we have $k^\times \subset J_k^1$. The following result is of vital importance in class-field theory.

THEOREM. *$J_k^1/k^\times$ with the quotient topology is compact.*

Proof. After the preceding lemma it is enough to find a V_k-compact set $W \subset V_k$ such that the map

$$W \cap J_k^1 \to J_k^1/k^\times$$

is surjective.

We take for W the set of $\xi = \{\xi_v\}$ with

$$|\xi_v|_v \leq |\alpha_v|_v$$

where $\alpha = \{\alpha_v\}$ is any idele of content greater than the C of the last lemma of § 14.

Let $\beta = \{\beta_v\} \in J_k^1$. Then by the lemma just quoted there is a $\eta \in k^\times$ such that

$$|\eta|_v \leq |\beta_v^{-1}\alpha_v|_v \quad (\text{all } v).$$

Then $\eta\beta \in W$, as required.

[$J_k/k^\times$ is totally disconnected in the function field case. For the structure of its connected component in the number theory case see papers of Artin and Weil in the "Proceedings of the Tokyo Symposium on Algebraic Number Theory, 1955" (Science Council of Japan) or Artin-Tate: "Class Field Theory", 1951/2 (Harvard, 1960(?)). The determination of the character group of $J_k/k^\times$ is global class field theory.]

17. Ideals and Divisors

Suppose that k is a finite extension of $\mathbf{Q}$. We define the ideal group I_k of k to be the free abelian group on a set of symbols in 1–1 correspondence

† See previous footnote.

with the *non-arch.* valuations v of k, i.e. formal sums

$$\sum_{v \text{ non-arch.}} n_v . v \tag{17.1}$$

where $n_v \in \mathbf{Z}$ and $n_v = 0$ for almost all v, addition being defined componentwise. We call (17.1) an ideal and call it integral if $n_v \geq 0$ for all v. This language is justified by the existence of a 1–1 correspondence between integral ideals and the ideals (in the ordinary sense) in the Dedekind ring

$$\mathfrak{o} = \bigcap_{\text{non-arch.}} \mathfrak{o}_v:$$

cf. Chapter I, §2, Prop. 2.

There is a natural continuous map

$$J_k \to I_k$$

of the idele group on to the ideal group† given by

$$\alpha = \{\alpha_v\} \to \sum (\operatorname{ord}_v \alpha) . v.$$

The image of $k^\times \subset J_k$ is the group of principal ideals.

THEOREM. *The group of ideal classes, i.e. I_k modulo principal ideals, is finite.*

Proof. For the map $J_k^1 \to I_k$ is surjective and so the group of ideal classes is the continuous image of the compact group $J_k^1/k^\times$ and hence compact. But a compact discrete group is finite.

When k is a finite separable extension of $\mathbf{F}(t)$ we define the divisor group D_k of k to be the free group on all the v. For each v the number of elements in the residue class field of v is a power, say q^{d_v} of the number q of elements in $\mathbf{F}$. We call d_v the degree of v and similarly define $\sum n_v d_v$ to be the degree of $\sum n_v . v$. The divisors of degree 0 form a group D_k^0. One defines the principal divisors similarly to principal ideals and then one has the

THEOREM. *D_k^0 modulo principal divisors is a finite group.*

For the quotient group is the continuous image of the compact group $J_k^1/k^\times$.

18. Units

In this section we deduce the structure theorem for units from our results about idele classes.

Let S be any finite non-empty set of normalized valuations and suppose that S contains all the archimedean valuations. The set of $\eta \in k$ with

$$|\eta|_v = 1 \quad (v \notin S) \tag{18.1}$$

are a group under multiplication, the group H_S of S-units. When $k \supset \mathbf{Q}$ and S is just the archimedean valuations, then H_S is the group of units *tout court*.

† I_k being given the discrete topology.

(≤ so it can be used in the next lemma)

LEMMA 1. *Let* $0 < c \le C < \infty$. Then the set of S-units η with

$$c \le |\eta|_v \le C \quad (v \in S) \tag{18.2}$$

is finite.

Proof. The set W of ideles $\alpha = \{\alpha_v\}$ with

$$|\alpha_v|_v = 1 \quad (v \notin S), \qquad c \le |\alpha_v|_v \le C \quad (v \in S) \tag{18.3}$$

is compact (product of compact sets with the product topology). The required set of units is just the intersection of W with the discrete subset k^+ of J_k and so is both discrete and compact, hence finite.

LEMMA 2. *There are only finitely many* $\varepsilon \in k$ *such that* $|\varepsilon|_v = 1$ *for every* v. *They are precisely the roots of unity in* k.

Proof. If ε is a root of unity it is clear that $|\varepsilon|_v = 1$ for every v. Conversely, by the previous lemma (with any S and $c = C = 1$) there are only finitely many $\varepsilon \in k$ with $|\varepsilon|_v = 1$ for all v. They form a group under multiplication and so are all roots of 1.

THEOREM. (Unit theorem.) *H_S is the direct sum of a finite cyclic group and a free abelian group of rank $s-1$.* ($s = \#S$)

Proof. To avoid petty notational troubles we treat only the case when $\mathbf{Q} \subset k$ and S is the set of arch. valuations.

Let J_S consist of the ~~ideals~~ ideles $\alpha = \{\alpha_v\}$ with $|\alpha_v|_v = 1$ $(v \notin S)$ and put

$$J_S^1 = J_S \cap J_k^1.$$

Clearly J_S^1 is open in J_k^1 and so

$$J_S^1/H_S = J_S^1/(J_S^1 \cap k^\times) \tag{18.4}$$

is open in $J_k^1/k^\times$. Since it is a subgroup, it is also closed, and so compact (§ 16).

Consider the map

$$\lambda : J_S \to \underbrace{\mathbf{R}^+ \oplus \mathbf{R}^+ \oplus \ldots \oplus \mathbf{R}^+}_{s \text{ times}},$$

where $\mathbf{R}^+$ is the additive group of reals, given by

$$\alpha \to (\log|\alpha_1|_1, \log|\alpha_2|_2, \ldots, \log|\alpha_s|_s),$$

where $1, 2, \ldots, s$ are the valuations in S. Clearly λ is both continuous and surjective.

The kernel of λ restricted to H_S consists just of the ε with $|\varepsilon|_v = 1$ for every v, so is a finite cyclic group by Lemma 2. By Lemma 1 there are only finitely many $\eta \in H_S$ with

$$\tfrac{1}{2} \le |\eta|_v \le 2 \quad v \in S. \tag{18.5}$$

Hence the group Λ (say) $= \lambda(H_S)$ is discrete.

Further, $T = \lambda(J_S^1)$ is just the set of $(x_1, \ldots, x_s)$ with

$$x_1 + x_2 + \ldots + x_s = 0,$$

i.e. an $s-1$ dimensional real vector space. Finally, T/Λ is compact, being the continuous image of the compact set (18.4). Hence Λ is free on $s-1$ generators, as asserted.

Of course this structure-theorem (Dirichlet) and the finiteness of the class-number (Minkowski) are older than ideles. It is more usual to deduce the compactness of $J_k^1/k^\times$ from these theorems instead of vica versa.

19. Inclusion and Norm Maps for Adeles, Ideles and Ideals

Let K be a finite extension of the global field k. We have already seen (§ 14, Lemma) that there is a natural isomorphism

$$V_k \otimes_k K = V_K \tag{19.1}$$

algebraically and topologically. Hence $V_k = V_k \otimes_k k$ can naturally be regarded as a subring of V_K which is closed in the topology of V_K. This injection of V_k into V_K is called the injection map or the conorm map and is written

$$\text{con}: \quad \alpha \to \text{con}\,\alpha = \text{con}_{K/k}\alpha \in V_K \quad (\alpha \in V_k).$$

Explicitly if $\mathbf{A} = \text{con}\,\alpha$, then the components satisfy

$$A_V = \alpha_v \in k_v \subset K_V \tag{19.2}$$

where V runs through the normalized valuations of K and v is the normalized valuation of k which extends to V. If $k \subset L \subset K$ it follows that

$$\text{con}_{K/k}\alpha = \text{con}_{L/k}(\text{con}_{K/L}\alpha). \tag{19.3}$$

Finally, for principal adeles the conorm map is just the usual injection of k into K.

It is customary, and usually leads to no confusion, to identify $\text{con}_{K/k}\alpha$ with α.

One can also define norm and trace maps from V_K to V_k by imitating the usual procedure (cf. Appendix A). Let $\omega_1, \ldots, \omega_n$ be a basis for K/k. Then by (19.1) every $\mathbf{A} \in V_K$ is uniquely of the shape

$$\mathbf{A} = \sum \alpha_j \omega_j \quad \alpha_j \in V_k \tag{19.4}$$

and the map $\mathbf{A} \to \alpha_j$ of V_K into V_k is continuous by the very definition of the tensor product topology (§ 9). Hence if we define

$$\alpha_{ij} = \alpha_{ij}(\mathbf{A}) \in V_k$$

by

$$\mathbf{A}\omega_i = \sum_j \alpha_{ij}\omega_j \tag{19.5}$$

the $n \times n$ matrices (α_{ij}) give a continuous representation of the ring V_K over V_k. In particular, the

$$S_{K/k}\mathbf{A} = \sum \alpha_{ii} \tag{19.6}$$

$$N_{K/k}\mathbf{A} = \det(\alpha_{ij}) \tag{19.7}$$

are *continuous* functions of A and have the usual formal properties

$$S_{K/k}(\mathbf{A}_1+\mathbf{A}_2) = S_{K/k}\mathbf{A}_1 + S_{K/k}\mathbf{A}_2 \tag{19.8}$$

$$S_{K/k}\,\mathrm{con}_{K/k}\,\alpha = n\alpha \tag{19.9}$$

$$N_{K/k}(\mathbf{A}_1\mathbf{A}_2) = N_{K/k}\mathbf{A}_1\, N_{K/k}\mathbf{A}_2 \tag{19.10}$$

$$N_{K/k}\,\mathrm{con}_{K/k}\,\alpha = \alpha^n. \tag{19.11}$$

Further, the norm and trace operations are compatible with the embedding of k, $\mathbf{K}$ in V_k, V_K respectively, i.e. if $A \in K \subset V_K$ we get the same answer whether we compute $N_{K/k}A$, $S_{K/k}A$ in K or in V_K, so there is no ambiguity in the notation.

Finally if $K \supset L \supset k$ we have $V_k \subset V_L \subset V_K$ (on regarding conorm as an identification), and so the usual relations (cf. Appendix A)

$$S_{L/k}(S_{K/L}\mathbf{A}) = S_{K/k}\mathbf{A} \tag{19.12}$$

and

$$N_{L/k}N_{K/L}\mathbf{A} = N_{K/k}\mathbf{A}. \tag{19.13}$$

We can express the maps (19.6), (19.7) componentwise if we like. Let $V_1, \ldots, V_J$ be the extensions of any given valuation v of k to K. Then (§ 9)

$$K_v\,(\text{say}) = \bigoplus_{1\le j\le J} K_j = k_v \otimes_k K = \bigoplus_{1\le i\le n} k_v\omega_i \tag{19.14}$$

where k_v, K_j are the completions of k, K with respect to v, V_j respectively. Any $\mathbf{A} \in V_K$ can be regarded as having components

$$A_{V_1} \oplus \ldots \oplus A_{V_J} = A_v \tag{19.15}$$

in the K_v and then the components in the matrix representation (19.5) of A are just the representations of the A_v. In particular

$$S_{K/k}(\mathbf{A}) = \{S_{K_v/k_v}A_v\} \tag{19.16}$$

and

$$N_{K/k}\mathbf{A} = \{N_{K_v/k_v}A_v\}. \tag{19.17}$$

Finally, making use of the final remarks of § 9, we deduce that

$$S_{K/k}\mathbf{A} = \Big\{\sum_{V|v} S_{K_V/k_v}(A_V)\Big\}_v \tag{19.18}$$

and

$$N_{K/k}\mathbf{A} = \Big\{\prod_{V|v} N_{K_V/k_v}(A_V)\Big\}_v, \tag{19.19}$$

where $V|v$ means "V is a continuation of v".

We now consider the consequences for ideles. If α is an idele, it is clear from the definition (19.2) that $\mathrm{con}_{K/k}\,\alpha$ is an idele, so we have an injection

$$\mathrm{con}_{K/k} : J_k \to J_K$$

which is clearly a homomorphism of J_k with a closed subset of V_K. Further,

if $\mathbf{A} \in J_K \subset V_K$, so $\mathbf{A}$ is invertible, it follows from (19.9) that $N_{K/k}\mathbf{A}$ is invertible, i.e. is an element of J_k. Hence we have a map

$$N_{K/k} : J_K \to J_k$$

which is continuous by the definition of the idele topology (§16) and which clearly satisfies (19.10), (19.11), (19.13) and (19.19). On the other hand, the definition of trace does not go over to ideles.

Finally, we consider the conorm and norm maps for ideals, where k is a finite extension of $\mathbf{Q}$. The kernel of the map (§17)

$$J_k \to I_k$$

of the idele group into the ideal group is just the group U_k (say) of ideles $\alpha = \alpha_v$ which have $|\alpha_v|_v = 1$ for every non-archimedean v. If K is a finite extension of k, it is clear that

$$\mathrm{con}_{K/k}\,U_k \subset U_K$$

and from the Lemma of §11 and (19.17) we have

$$N_{K/k}U_K \subset U_k.$$

Hence on passing to the quotient from J_k we have the induced maps

$$\mathrm{con}_{K/k} : I_k \to I_K$$

$$N_{K/k} : I_K \to I_k$$

with the usual properties (19.10), (19.11) and (19.13); and these maps are compatible with the norm and conorm maps for elements of K and k on taking principal ideals. By definition (19.2) we have

$$\mathrm{con}_{K/k}\,v = \sum_{V|v} e_V\, V \tag{19.20}$$

where the positive integers e_V are defined by

$$|\pi_v|_V = |\Pi_V|_V^{e_V}, \tag{19.21}$$

π_v and Π_V being prime elements of k_v, K_V respectively. Similarly, it follows from (19.19) that

$$N_{K/k}V = f_V v, \tag{19.22}$$

where f_V is the degree of the residue class field of V over that of v. We note in passing that (19.11), (19.20) and (19.22) imply that

$$\sum_{V|v} e_V f_V = n,$$

as it should since

$$e_V f_V = [K_V : k_V].$$

Similarly, when k is a finite extension of $\mathbf{F}(t)$ one defines conorm and norm of divisors, with the appropriate properties.

APPENDIX A

Norms and Traces

Let R be a commutative ring with 1. By a vector space V over R of dimension n we shall mean a free R-module on n generators, say $\omega_1, \ldots, \omega_n$ (a *basis*). If $\omega_1', \ldots, \omega_n'$ is another basis, there are $u_{ij}, v_{ij} \in R$ such that

$$\omega_i = \sum_j u_{ij}\omega_j', \omega_j' = \sum v_{ij}\omega_j \tag{A.1}$$

and

$$\sum_j u_{ij}v_{jl} = \sum v_{ij}u_{jl} = \delta_{il} \tag{A.2}$$

(Kronecker δ).

The set of all R-linear endomorphisms of V is a ring, which we denote by $\mathrm{End}_R V$. The ring R is injected into $\mathrm{End}_R V$ if we identify $b \in R$ with the module action of b on V, and we shall do this. The ring $\mathrm{End}_R V$ is isomorphic but not canonically, to the ring of all $n \times n$ matrices with elements in R. The isomorphism becomes canonical if V is endowed with a fixed choice of basis. In fact if $\beta \in \mathrm{End}_R(V)$ and

$$\beta\omega_i = \sum_j b_{ij}\omega_j, \quad (b_{ij} \in R) \tag{A.3}$$

the 1–1 correspondence between β and the transposed matrix (b_{ji}) is a ring isomorphism.

For $\beta \in \mathrm{End}_V$ we denote by

$$F_\beta(x) = \det(x\delta_{ij} - b_{ij}) \tag{A.4}$$

the characteristic polynomial of R. On using (A.2) it is easy to see that $F_\beta(x)$ is independent of the choice of bases of V. The Cayley-Hamilton theorem† states that

$$F_\beta(\beta) = 0. \tag{A.5}$$

We define further the *trace*

$$\begin{aligned} S_{V/R}(\beta) = S(\beta) &= \sum_j b_{jj} \\ &= -\text{coefficient of } x^{n-1} \text{ in } F_\beta(x) \end{aligned} \tag{A.6}$$

and the *norm*

$$\begin{aligned} N_{V/R}(\beta) = N(\beta) &= \det(b_{ij}) \\ &= (-)^n \text{ constant term in } F_\beta(x), \end{aligned} \tag{A.7}$$

† *Proof.* Write (A.3) in the form

$$\sum_j (\delta_{ij}\beta - b_{ij})\omega_j = 0.$$

Working in the commutative ring $R[\beta]$ multiply the equations (*) by the cofactors of the "coefficients" of ω_1, and add. Then $\omega_2, \ldots, \omega_n$ are "eliminated" and one obtains $F_\beta(\beta)\omega_1 = 0$. Similarly $F_\beta(\beta)\omega_j = 0$ $(2 \le j \le n)$ and so $F_\beta(\beta) = 0$.

which are independent of the choice of basis because $F_\beta(x)$ is. Clearly

$$S(\beta_1 + \beta_2) = S(\beta_1) + S(\beta_2) \tag{A.8}$$

$$S(b) = nb \quad (b \in R) \tag{A.9}$$

$$N(\beta_1\beta_2) = N(\beta_1)N(\beta_2) \tag{A.10}$$

$$N(b) = b^n \quad (b \in R), \tag{A.11}$$

because the correspondence (A.3) between $\beta \in \mathrm{End}_R(V)$ and the matrix b_{ji} is a ring isomorphism.

LEMMA A.1. *Let t be transcendental over R. Then*

$$N(t - \beta) = F_\beta(t). \tag{A.12}$$

Pedantically, what is meant is, of course, that we consider a vector space V with basis $\omega_1, \ldots, \omega_n$ defined over $R[t]$ and a β given by (A.3).

Proof. We have

$$(t - \beta)\omega_i = \sum_j (t\delta_{ij} - b_{ij})\omega_j$$

and so

$$\begin{aligned} N(t - \beta) &= \det(t\delta_{ij} - b_{ij}) \\ &= F_\beta(t) \end{aligned}$$

by (A.4) and (A.7).

COROLLARY. (A.12) *holds for any $t \in R$.*

LEMMA A.2. *Let $\beta_1, \ldots, \beta_l \in \mathrm{End}_R V$ and let t be transcendental over R. Then*

$$N(t^l + \beta_1 t^{l-1} + \ldots + \beta_l) = t^{nl} + g_1 t^{nl-1} + \ldots + g_{nl} \tag{A.13}$$

where $g_1, \ldots, g_{nl} \in R$ and in particular

$$g_1 = S(\beta_1); \qquad g_{nl} = N(\beta_l). \tag{A.14}$$

Proof. Similar to that of Lemma A.1 and left to the reader.

Now let R and $P \subset R$ be commutative rings with 1 and suppose that R regarded as a P-module is free on a finite-number, say, m of generators $\Omega_1, \ldots, \Omega_m$ (i.e. an m-dimensional P-vector space). Let V be an n-dimensional R-vector space with basis $\omega_1, \ldots, \omega_n$. Then V can also be regarded as an mn-dimensional P-vector space with basis

$$\Omega_i\omega_j \qquad (1 \le i \le m, \quad 1 \le j \le n)$$

and there is an obvious natural injection of $\mathrm{End}_R(V)$ into $\mathrm{End}_P(V)$. We have now the key

THEOREM A.1. *Let*

$$\beta \in \mathrm{End}_R(V) \subset \mathrm{End}_P(V). \tag{A.15}$$

Then

$$S_{V/P}\beta = S_{R/P}(S_{V/R}\beta), \tag{A.16}$$

$$N_{V/P}\beta = N_{R/P}(N_{V/R}\beta). \tag{A.17}$$

Further

$$\Phi(x) = N_{R/P}F(x), \tag{A.18}$$

where $\Phi(x) \in P[x]$, $F(x) \in R[x]$ *are the characteristic polynomials of* β *in* $\mathrm{End}_P(V)$ *and* $\mathrm{End}_R(V)$ *respectively.*

Proof. If β is given by (A.3) let $\gamma \in \mathrm{End}_R(V)$ be given by

$$\begin{aligned} \gamma\omega_1 &= \omega_1 - \sum_{j>1} b_{ij}\omega_j \\ \gamma\omega_i &= b_{11}\omega_i \quad (i>1). \end{aligned} \tag{A.19}$$

Then for $\alpha = \gamma\beta$ we have

$$\begin{aligned} \alpha\omega_1 &= b_{11}\omega_1 \\ \alpha\omega_i &= b_{i1}\omega_1 + \sum_{j>1}(b_{11}b_{ij} - b_{i1}b_{1j})\omega_j \\ &= b_{i1}\omega_1 + \sum_{j>1} a_{ij}\omega_j \quad \text{(say)}. \end{aligned} \tag{A.20}$$

Hence

$$N_{V/R}\alpha = b_{11}N_{W/R}\alpha^* \tag{A.21}$$

where W is the $n-1$ dimensional R-vector space spanned by $\omega_2, \ldots, \omega_n$ and α^* is the R-linear map

$$\omega_i \to \sum_{j>1} a_{ij}\omega_j \quad (i>1).$$

Consequently

$$N_{R/P}(N_{V/R}\alpha) = N_{R/P}b_{11} \cdot N_{R/P}(N_{W/R}\alpha^*). \tag{A.22}$$

We now use induction on the dimension n, since the Theorem is trivial for $n = 1$. Since W has dimension $n-1$ we have by the induction hypothesis

$$N_{R/P}(N_{W/R}\alpha^*) = N_{W/P}\alpha^*. \tag{A.23}$$

On the other hand, it follows directly from (A.20) that

$$N_{V/P}\alpha = N_{R/P}b_{11}N_{W/P}\alpha^*$$

and so

$$N_{V/P}\alpha = N_{R/P}N_{V/P}\alpha. \tag{A.24}$$

Further, clearly

$$N_{V/P}\gamma = N_{R/P}N_{V/P}\gamma = (N_{R/P}b_{11})^{n-1}.$$

Since $\alpha = \beta\gamma$ and both $N_{V/P}$ and $N_{R/P}N_{V/R}$ are multiplicative (by (A.10)), it follows from (A.24) that

$$(N_{R/P}b_{11})^{n-1}N_{V/P}\beta = (N_{R/P}b_{11})^{n-1}N_{R/P}(N_{V/R}\beta). \tag{A.25}$$

If $N_{R/P}b_{11}$ were invertible, this would give (A.17) at once. In general, however, this is not the case and we must use a common trick.

Let t be a transcendental over R and let β_t be the transformation obtained from β by replacing b_{11} by $b_{11}+t$ but leaving the remaining b_{ij} unchanged. Then (A.25) applied to β_t gives

$$(N_{R/P}(b_{11}+t))^{n-1}N_{V/P}\beta_t = N_{R/V}(b_{11}+t)^{n-1}N_{R/P}(N_{V/R}\beta_t). \tag{A.26}$$

All the norms occurring in (A.26) are polynomials in t. On comparing coefficients of powers of t in (A.26), starting at the top, we deduce that

$$N_{V/P}\beta_t = N_{R/P}(N_{V/R}\beta_t) \tag{A.27}$$

because the coefficient of the highest power of t in $N_{R/P}(b_{11}+t)$ is 1. Then (A.17) follows on putting $t = 0$.

We now prove (A.18). By Lemma 1 we have

$$\Phi(x) = N_{V/P}(x-\beta), \qquad F(x) = N_{V/R}(x-\beta)$$

and so (A.18) is just (A.17) with $x-\beta$ for β.

Finally, (A.16) follows from (A.18) on using (A.6) and the first half of (A.14).

When $R = k$ is a field there is some simplification, since every finitely-generated module V over k is free, i.e. is a vector space. Further each $\beta \in \mathrm{End}_k(V)$ has a minimum polynomial, i.e. a non-zero polynomial $f(x)$ of lowest degree, with highest coefficient 1, such that $f(\beta) = 0$. Then $g(\beta) = 0$ for $g(x) \in k[x]$ if and only if $f(x)$ divides $g(x)$ in $k[x]$. In particular the Cayley-Hamilton theorem (A.5) now states that $f(x)$ divides the characteristic polynomial $F_\beta(x)$.

Finally we have

THEOREM A.2. *Let* K *be a field of finite degree* n *over the field* k *and let* $\beta \in K$. *Then the degree* m *(say) of the minimum polynomial* $f(x)$ *of* β *over* k *divides* n *and*

$$F(x) = (f(x))^{n/m},$$

where $F(x)$ *is the characteristic polynomial of* β. *In particular*

$$S_{K/k}(\beta) = \frac{n}{m}(\beta_1 + \ldots + \beta_m),$$

$$N_{K/k}(\beta) = (\beta_1, \beta_2, \ldots, \beta_m)^{n/m},$$

where $\beta_1, \ldots, \beta_m$ *are the roots of* $f(x)$ *in any splitting field.*

Proof. Suppose first that $K = k(\beta)$. Then the minimum polynomial $f(x)$ and the characteristic polynomial $F(x)$ of β have the same degree and highest coefficient, so $F(x) = f(x)$ by the remarks preceding the enunciation of the Lemma.

The general case now follows from Theorem A.1, with $V = K$, $R = k(\beta)$, $P = k$ on using (A.11).

APPENDIX B

Separability

In this book we are primarily interested in separable algebraic field extensions. Here we recall their most important elementary properties.

LEMMA B.1. *Let K, M be extensions of finite degree of the field k. Then there are at most $[K:k]$ injections of K into M which leave k elementwise fixed.*

Proof. Trivial when $K = k(\alpha)$ for some α on considering the minimal polynomial for α. For general K we have a chain

$$k = K_0 \subset K_1 \subset K_2 \ldots \subset K_J = K \tag{B.1}$$

where $K_j = K_{j-1}(\alpha_{j-1})$ and use induction on J.

DEFINITION. *The finite field extension K/k is separable if there is some finite extension M/k such that there are $[K:k]$ distinct injections of K into M which leave k elementwise fixed. If K/k is not separable then it is said to be inseparable.*

COROLLARY 1. *Let $K \supset L \supset k$. If K/k is separable then so are K/L and L/k.*

Proof. By Lemma 1 there are at most $[L:k]$ distinct injections of L into M and by Lemma 1 again each of these can be extended in at most $[K:L]$ ways into injections of K into M. By definition, there are

$$[K:k] = [K:L][L:k]$$

injections of K into M, and so there must be equality both times.

COROLLARY 2. *Let $\alpha \in K$ where K/k is separable and let $\alpha_1, \ldots, \alpha_m$ be the roots in M of the irreducible polynomial $f(x)$ for α over k. Then the $\sigma_i\alpha$ $(1 \le i \le n = [K:k])$ are just the $\alpha_1, \ldots, \alpha_m$ each taken n/m times, where $\sigma_1, \ldots, \sigma_m$ are the injections of K into some M.*

Proof. For put $L = k(\alpha)$ in the preceding argument.

COROLLARY 3.

$$S_{K/k}(\alpha) = \sum_i \sigma_i\alpha.$$

Proof. Follows from Theorem A.2 and the preceding Corollary.

LEMMA B.2. *Let K/k be a finite field extension and let σ be an injection of k into some field M. Then there is a finite extension M_1 of M and an injection σ_1 of K into M_1 which reduces to σ on k.*

Proof. Trivial if $K = k(\alpha)$, and then follows for general K on using a chain (B.1).

THEOREM B.1. *Let K/L and L/k be separable extensions. Then K/k is a separable extension.*

Proof. Let U/L be a finite extension and

$$\tau_i : K \to U \quad (1 \le i \le [K:L])$$

be injections extending the identity on L and similarly let V/k be a finite extension and

$$\sigma_j : L \to V \quad (1 \le j \le [L:k])$$

extend the identity on k. By repeated application of Lemma 2 there is a finite field extension M/V and $[L:k]$ injections

$$\sigma_j' : U \to M \quad (1 \le j \le [L:k])$$

which extend the σ_j. Then the $\sigma_j'\tau_i$ give

$$[K:L][L:k] = [K:k]$$

distinct injections of K into M extending the identity on k.

COROLLARY. *In characteristic zero every finite field extension is separable.*

Proof. For a simple extension $k(\alpha)/k$ clearly is, and then apply the theorem to a tower of simple extensions.

THEOREM B.2. *Let K/k be a separable extension. Then it is simple, i.e. $K = k(\gamma)$ for some γ.*

Note. The converse is, of course, false.

Proof. If k is a finite field then so is K and so indeed $K = \Pi(\alpha)$ for some $\alpha \in K$, where Π is the prime field, by the structure theory of finite fields. Hence we need consider only the case when k has infinitely many elements. Suppose first that $K = k(\alpha, \beta)$ and let $\sigma_1, \ldots, \sigma_n$ where $n = [K:k]$ be the distinct injections of K into M (say). If $i \ne j$, distinctness implies that

$$\text{either} \quad \sigma_i\alpha \ne \sigma_j\alpha \quad \text{or} \quad \sigma_i\beta \ne \sigma_j\beta$$

(or both). Hence we may find $a, b \in k$ to satisfy the finitely many inequalities

$$a(\sigma_i\alpha - \sigma_j\alpha) + b(\sigma_i\beta - \sigma_j\beta) \ne 0 \; (i \ne j).$$

Put

$$\gamma = a\alpha + b\beta,$$

so

$$\sigma_i\gamma \ne \sigma_j\gamma \quad (i \ne j).$$

The $\sigma_i\gamma$ are all roots of the irreducible equation for γ over k and so

$$[k(\gamma):k] \ge n.$$

But $k(\gamma) \subset K$, so $K = k(\gamma)$.

For the general case when $K = k(\alpha_1, \alpha_2, \ldots, \alpha_J)$ with $J > 2$ one uses induction on J. We have $k(\alpha_2, \ldots, \alpha_J) = k(\beta)$ for some β and then $k(\alpha_1, \beta) = k(\gamma)$.

THEOREM B.3. *Let K/k be a separable extension. Then*

$$S(\alpha, \beta) = S_{K/k}(\alpha\beta)$$

is a non-degenerate symmetric bilinear form on K considered as a vector space over k.

Proof. Only the non-degeneracy needs proof. Let $\omega_1, \ldots, \omega_n$ be a base of K/k. The statement of the Theorem is equivalent to

$$D(\text{say}) = \det \{S_{K/k}(\omega_i \omega_j)\}_{\substack{1 \le i \le n \\ 1 \le j \le n}} \neq 0.$$

Let $\sigma_1, \ldots, \sigma_n$ be distinct injections of K into some M. By Lemma B.1, Corollary 3 we have

$$D = \Delta^2$$

where

$$\Delta = \det (\sigma_i \omega_j)_{\substack{1 \le i \le n \cdot \\ 1 \le j \le n}}$$

By Theorem B.2 we have $K = k(\gamma)$ and so can take $\omega_j = \gamma^{j-1}$. Then

$$\Delta = \prod_{i<j} (\sigma_j \gamma - \sigma_i \gamma)$$
$$\neq 0,$$

as required.†

We now consider when a simple extension $k(\alpha)/k$ is separable. Let $f(x)$ be an irreducible polynomial in $k[x]$ and let $f'(x)$ be its derivative. If $f'(x) \neq 0$ it must be coprime to $f(x)$, since it is of lower degree, and so there are $a(x), b(x) \in k[x]$ such that

$$a(x)f(x) + b(x)f'(x) = 1.$$

Hence $f(\beta) = 0$ for β in any extension of k, implies that $f'(\beta) \neq 0$, and so β is a simple root. Hence the number of roots of $f(x)$ in a splitting field is equal to the degree. On the other hand, if $f'(x) = 0$, every root of $f(x)$ is multiple, and so the total number of roots is less than the degree. In the first case we say that $f(x)$ is separable, in the second inseparable. The second case occurs if and only if $f(x) = g(x^p)$ for some $g(x) \in k[x]$, where p is the characteristic.

LEMMA B.3. *A necessary and sufficient condition for $k(\alpha)/k$ to be separable is that the irreducible polynomial $f(x) \in k[x]$ for α be separable.*

Proof. Clear.

COROLLARY 1. *Let $K \supset k$, and suppose that $k(\alpha)/k$ is separable. Then $K(\alpha)/K$ is separable.*

Proof. For the irreducible polynomial $F(x) \in K[x]$ over K divides $f(x)$.

COROLLARY 2. *A necessary and sufficient condition that K/k be separable is that every element of K be separable $/k$.*

Proof. Suppose that every element of K is separable and that K is given by a chain

$$k = K_0 \subset K_1 \subset \ldots \subset K_J = K$$

† Instead of using the fact that $K = k(\gamma)$ we could have used Artin's theorem that any set of injections of one field into another is linearly independent. See Artin: "Galois Theory" (Notre Dame) or Adamson: "Introduction to Field Theory" (Oliver and Boyd).

where $K_j = K_{j-1}(\alpha_{j-1})$. Then K_j/K_{j-1} is separable by the previous corollary and so K/k is separable by Theorem 1.

The converse follows from Lemma 1 Corollary.

In striking contrast to Theorem B.3 we have

THEOREM B.4. *Let K/k be inseparable. Then the trace $S_{K/k}(\beta)$ vanishes for all $\beta \in K$.*

Proof. Suppose, first, that $K = k(\alpha)$ where $\alpha^p \in k$, $\alpha \notin k$ and p is the characteristic. Then

$$\omega_1 = 1, \omega_2 = \alpha, \ldots, \omega_p = \alpha^{p-1}$$

is a basis for K/k. If $\beta = b_1 + b_2\alpha + \ldots + b_p\alpha^{p-1}$ with $b_j \in k$, then

$$\beta\omega_i = \sum b_{ij}\omega_j \quad b_{ij} \in k$$

where clearly

$$b_{ii} = b_1 \quad (1 \le i \le p).$$

Hence

$$S_{K/k}\beta = \sum_i b_{ii} = pb_1 = 0.$$

Now let K/k be any inseparable extension. By the latest Corollary there is an inseparable $\alpha \in K$. Put $L = k(\alpha)$, $M = k(\alpha^p)$, so L/M is an extension of the kind just discussed. The general result now follows because of the transitivity of the trace:

$$S_{K/k}\beta = S_{M/k}\{S_{L/M}(S_{K/L}\beta)\}.$$

APPENDIX C

Hensel's Lemma

In the literature a variety of results go under this name. Their common feature is that the existence of an approximate solution of an equation or system of equations in a complete valued field implies the existence of an exact solution to which it is an approximation, subject to conditions to the general effect that the approximate solution is "good enough". These results are essentially just examples of the process of solution by successive approximation, which goes back to Newton (at least). In this appendix we give a typical specimen.

LEMMA. *Let k be a field complete with respect to the non-archimedean valuation $|\ |$ and let*

$$f(X) \in \mathfrak{o}[X], \tag{C.1}$$

where $\mathfrak{o} \subset k$ is the ring of integers for $|\ |$. Let $\alpha_0 \in \mathfrak{o}$ be such that

$$|f(\alpha_0)| < |f'(\alpha_0)|^2, \tag{C.2}$$

where $f'(X)$ is the (formal) derivative of $f(X)$. Then there is a solution of

$$f(\alpha) = 0, \qquad |\alpha - \alpha_0| \le |f(\alpha_0)|/|f'(\alpha_0)|. \tag{C.3}$$

Proof. (Sketch.) Let $f_j(X) \in \mathfrak{o}[X]$ be defined by the identity

$$f(X+Y) = f(X)+f_1(X)Y+\ldots+f_j(X)Y^j+\ldots, \tag{C.4}$$

where X, Y are independent variables, so $f_1(X) = f'(X)$. Define β_0 by

$$f(\alpha_0)+\beta_0 f_1(\alpha_0) = 0. \tag{C.5}$$

Then by (C.4) and since $f_j(\alpha_0) \in \mathfrak{o}$ we have

$$\begin{aligned} |f(\alpha_0+\beta_0)| &\le \max_{j\ge 2} |f_j(\alpha_0)\beta_0^j| \\ &\le \max_{j\ge 2} |\beta_0|^j \\ &\le |f(\alpha_0)|^2/|f_1(\alpha_0)|^2 \\ &< |f(\alpha_0)|. \end{aligned} \tag{C.6}$$

On using the analogue of (C.4) for $f_1(X)$, it is easy to verify that

$$|f_1(\alpha_0+\beta_0)-f_1(\alpha_0)| < |f_1(\alpha_0)|.$$

Thus on putting $\alpha_1 = \alpha_0+\beta_0$, we have

$$\begin{aligned} |f(\alpha_1)| &\le |f(\alpha_0)|^2/|f_1(\alpha_0)|^2, \\ |f_1(\alpha_1)| &= |f_1(\alpha_0)| \end{aligned}$$

and

$$|\alpha_1-\alpha_0| \le |f(\alpha_0)|/|f_1(\alpha_0)|.$$

On repeating the process with α_1, etc., we get a sequence $\alpha_0, \alpha_1, \alpha_2, \ldots$, which is easily seen to be a fundamental sequence. By the completeness of k there is an $\alpha = \lim_{n\to\infty} \alpha_n \in k$, which clearly does what is required.

In fact, the solution of (C.3) not merely exists, but is unique. For if $\alpha+\beta$, $\beta \neq 0$ is another solution one readily gets a contradiction by putting $X = \alpha$ $Y = \beta$ in (C.4).

CHAPTER III

Cyclotomic Fields and Kummer Extensions

B. J. BIRCH

1. Cyclotomic Fields

Let K be any field of characteristic zero, and $m > 1$ be an integer. Then there is a minimal extension L/K such that x^m-1 splits completely in L. The zeros of x^m-1 form a subgroup of the multiplicative group of L; this subgroup is cyclic (since every finite subgroup of the multiplicative group of a field is). The generators of this subgroup are called the primitive mth roots of unity. If ζ is a primitive mth root of unity then every zero of (x^m-1) is a power of ζ, and $L = K(\zeta)$. Clearly, L is a normal extension of K; we write $L = K(\sqrt[m]{1})$.

If σ is an element of the Galois group $G(L/K)$, then $\sigma\zeta$ must be another primitive mth root of unity, so $\sigma\zeta = \zeta^k$ for some integer k, $(k,m) = 1$. If ζ^a is another primitive root of unity then $\sigma\zeta^a = \zeta^{ak}$; accordingly, $\sigma \mapsto k$ is a canonical map of $G(L/K)$ into the multiplicative group $G(m)$ of residues modulo m prime to m. In particular, $[L:K] \le \phi(m)$.

If $m = rs$ where $(r,s) = 1$ then there exist integers a, b with $ar+bs = 1$, $\zeta = (\zeta^r)^a(\zeta^s)^b$, so $K(\zeta) = K(\zeta^r, \zeta^s)$; one obtains the extension $K(\zeta)$ by composing $K(\zeta^r)$ and $K(\zeta^s)$. So to some extent it is enough to consider $K(\sqrt[m]{1})$ when m is a prime power. If p is odd then the group $G(p^n)$ is cyclic, so if $m = p^n$, $L = K(\sqrt[m]{1})$, then $G(L/K)$ is cyclic; on the other hand $G(2^n)$ is generated by -1 and 5, so if we write $\eta = \zeta+\zeta^{-1}$ where $\zeta^{2^n} = 1$ then $K(\zeta) = K(i,\eta)$ and $G[K(\eta)/K]$ is cyclic.

We are particularly interested in the extensions $\mathbf{Q}(\sqrt[m]{1})$ and $\mathbf{Q}_p(\sqrt[m]{1})$; by Chapter I (Section 4 and start of Section 5) the study of the factorization of the prime p in the extension $\mathbf{Q}(\sqrt[m]{1})/\mathbf{Q}$ is essentially the same as the study of the extension $\mathbf{Q}_p(\sqrt[m]{1})/Q_p$. As one of my jobs is to supply explicit examples for abstract theorems, I will prove things several times over by different routes. Good accounts of cyclotomic extensions are given by Weyl: "Algebraic Theory of Numbers" (Princeton U.P., Annals of Math. Studies