AXIOMATIC CHARACTERIZATION OF FIELDS BY THE PRODUCT FORMULA FOR VALUATIONS

EMIL ARTIN AND GEORGE WHAPLES

Introduction. The theorems of class field theory are known to hold for two kinds of fields: algebraic extensions of the rational field and algebraic extensions of a field of functions of one variable over a field of constants. We shall refer to these fields as number fields and function fields, respectively. For class field theory, the function fields must indeed be restricted to those with a Galois field as field of constants; however, we make this restriction only in §5, and until then consider fields with an arbitrary field of constants.

In proving these theorems, the product formula for valuations plays an important rôle. This formula states that, for a suitable set of inequivalent valuations $|\ |_\mathfrak{p}$,

$$\prod_\mathfrak{p} |\alpha|_\mathfrak{p} = 1$$

for all numbers $\alpha \neq 0$ of the field. For fields of the types mentioned, this product formula is easy to prove. After reviewing this proof (§1), we shall show (§2) that, conversely, the number fields and function fields are characterized by their possession of a product formula. Namely, we prove that if a field has a product formula for valuations, and if one of its valuations is of suitable type, then it is either a function field or a number field.

This shows that the theorems of class field theory are consequences of two simple axioms concerning the valuations, and suggests the possibility of deriving these theorems directly from our axioms. We do this in the later sections of this paper for the generalized Dirichlet unit theorem, the theorem that the class number is finite, and certain others fundamental to class field theory. This axiomatic method has the decided advantage of uniting the two cases; also, it simplifies the proofs. For example, we avoid the use of either ideal theory or the Minkowski theory of lattice points. Thus these two theories are unnecessary to class field theory, since they are needed only to prove the unit theorem.

1. **Preliminaries on valuations.** If k is any field, then a function $|\alpha|$, defined for all $\alpha \in k$, is called a valuation of K if:

An address delivered by Professor Artin before the Chicago meeting of the Society on April 23, 1943, by invitation of the Program Committee; received by the editors February 3, 1945.

(1) $|\alpha|$ *is a real number not less than* 0, *and* $|\alpha|=0$ *only if* $\alpha=0$,

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

(3) $$|\alpha+\beta| \leqq |\alpha| + |\beta|.$$

We call a valuation nonarchimedean if in addition to (3) it satisfies

(3′) $$|\alpha+\beta| \leqq \max(|\alpha|, |\beta|).$$

Note that the assumption that $|\alpha|$ is a real number eliminates the possibility of certain valuations discussed in various recent papers.

The theory of a field with respect to one given valuation is supposed to be known by the reader and shall be called the local theory. We review the most important facts. The valuation $|\alpha|=1$ for all $\alpha\neq 0$ is called the trivial valuation. Two nontrivial valuations $|\alpha|_1$ and $|\alpha|_2$ are called equivalent when $|\alpha|_1<1$ implies $|\alpha|_2<1$, and it is easy to show[1] that there is a positive real number ρ such that $|\alpha|_1^{\rho}=|\alpha|_2$ for all $\alpha\in k$. If $|\alpha|$ is a nonarchimedean valuation, then $|\alpha|^{\rho}$ is an equivalent valuation for any $\rho>0$. If $|\alpha|$ is archimedean and ρ positive, then $|\alpha|^{\rho}$ will be a valuation only for sufficiently small values of ρ. However, we shall in the remainder of this paper use the word "valuation" to mean any function $|\alpha|^{\rho}$ where ρ is any positive number and $|\alpha|$ is a true valuation.

A set of equivalent and nontrivial valuations of a field k is called a prime divisor of that field, and denoted by letters like p, $\mathfrak{p}$, $\mathfrak{P}$, q, $\mathfrak{q}$, $\mathfrak{Q}$, $\cdots$. If $\mathfrak{p}$ is a prime divisor, $|\alpha|_{\mathfrak{p}}$ stands for a particular, fixed valuation chosen from this set. The sign $\|\alpha\|_{\mathfrak{p}}$ will later be used to stand for another valuation of the same set.

If R is a subfield of k then each set $\mathfrak{p}$ of equivalent valuations of k is also a set of equivalent valuations of R. If these valuations are nontrivial on R then they define a prime divisor p of R, and $\mathfrak{p}$ is said to divide p: $\mathfrak{p}|p$. One p may be divisible by several $\mathfrak{p}$ of k. By well known methods,[2] the field k can be extended to the field $k_{\mathfrak{p}}$ which is completed with respect to the valuations of $\mathfrak{p}$. If R_p is the corresponding completion of R then R_p is a subfield of k and the degree $n(\mathfrak{p})=(k_{\mathfrak{p}}/R_p)$ is called the local degree. If k itself is a finite extension of R of degree n it is easy to prove[3] the inequality

---

[1] See van der Waerden [7, pp. 254–255], or Artin [1]. Numbers in brackets refer to the references cited at the end of the paper.

[2] van der Waerden [7, p. 250].

[3] To prove this, assume first that $k=R(\alpha)$, where α is a root of a polynomial $f(x)$, irreducible in R of degree n. Let $P(x)$ be the polynomial, irreducible in R_p of degree $n_{\mathfrak{p}}$, with root α. Since (van der Waerden [7, p. 264]) an extension field of R_p can be evaluated in only one way by a divisor $\mathfrak{p}$ of p, it follows that different divisors

$$\sum_{\mathfrak{p}|p} n(\mathfrak{p}) \leqq n \tag{4}$$

for each p of R.

In case $\mathfrak{p}$ is a discrete valuation, $n(\mathfrak{p}) = e(\mathfrak{p})f(\mathfrak{p})$ where $e(\mathfrak{p})$ is the ramification number and $f(\mathfrak{p})$ the degree of the residue class field of k over that of R.

We proceed now to study a finite set of nontrivial inequivalent valuations $|\ |_1, |\ |_2, \cdots, |\ |_n$.

LEMMA 1. *If* $|\ |_1$ *and* $|\ |_2$ *are two nontrivial, inequivalent valuations of* k, *then there is a* $\gamma \in k$ *with* $|\gamma|_1 < 1$ *and* $|\gamma|_2 > 1$.

PROOF. Since the valuations are inequivalent there is an α with $|\alpha|_1 < 1$ and $|\alpha|_2 \geqq 1$ and a β with $|\beta|_1 \geqq 1$ and $|\beta|_2 < 1$. Take $\gamma = \alpha/\beta$.

LEMMA 2. *If* $|\ |_1, |\ |_2, \cdots, |\ |_n$ *are nontrivial and inequivalent there is an* $\alpha \in k$ *such that* $|\alpha|_1 > 1$ *and* $|\alpha|_\nu < 1$ *for* $\nu = 2, \cdots, n$.

PROOF. The lemma is true for $n = 2$ by Lemma 1. We use induction, assuming that we have found a β such that $|\beta|_1 > 1$ and $|\beta|_\nu < 1$ for $\nu = 2, \cdots, n-1$. Choose γ so that $|\gamma|_1 > 1$ and $|\gamma|_n < 1$. There are two cases:

Case 1. If $|\beta|_n \leqq 1$ let $\alpha = \beta^r\gamma$. Then $|\alpha|_1 > 1$ and, for r sufficiently large, $|\alpha|_2, |\alpha|_3, \cdots, |\alpha|_n$ are all less than 1.

Case 2. If $|\beta|_n > 1$ let

$$\alpha = \frac{\beta^r}{\beta^r + 1}\gamma$$

so that

$$|\alpha|_\nu = \frac{|\beta|_\nu^r |\gamma|_\nu}{|\beta^r + 1|_\nu} \leqq \frac{|\beta|_\nu^r}{1 - |\beta|_\nu^r} |\gamma|_\nu, \qquad \nu = 2, \cdots, n-1,$$

$$|\alpha|_n \leqq \frac{|\beta|_n^r}{|\beta|_n^r - 1} |\gamma|_n.$$

Now $|\alpha|_\nu < 1$ for r large; namely $\lim_{r\to\infty} |\beta|_\nu^r = 0$ and $|\alpha|_n < 1$ since

---

$\mathfrak{p}_1, \mathfrak{p}_2, \cdots$ of p will lead to different irreducible polynomials $P(x)$. Since $f(x)$ is divisible by the product of the polynomials $P(x)$, this proves the inequality for this case. If several elements have to be adjoined to R in order to get k, we prove the theorem by repeated application of the simple case.

This proof shows also that in case of an inseparable extension k one can not expect to replace the inequality by an equality. If this can be done in a special case, it is a noteworthy property of the particular field. In §3 we shall find a class of fields with this property.

$$\lim_{r\to\infty} \frac{|\beta|_n^r}{|\beta|_n^r - 1} = 1.$$

For $\nu=1$ we find

$$|\alpha|_1 \geqq \frac{|\beta|_1^r}{1+|\beta|_1^r}|\gamma|_1,$$

so for large r, $|\alpha|_1>1$.

LEMMA 3. *If any n nontrivial inequivalent valuations of k are given, then for any positive ϵ there is an α such that*

$$|\alpha-1|_1 \leqq \epsilon, \quad |\alpha|_\nu \leqq \epsilon \quad \text{for} \quad \nu > 1.$$

PROOF. Choose β, by Lemma 2, so that $|\beta|_1>1$ and $|\beta|_\nu<1$ for $\nu>1$ and take

$$\alpha = \frac{\beta^r}{1+\beta^r}.$$

Then

$$|\alpha - 1|_1 = \frac{1}{|1+\beta^r|_1} \leqq \frac{1}{|\beta|^r - 1} \leqq \epsilon$$

for r sufficiently large. For $\nu>1$,

$$|\alpha|_\nu = \frac{|\beta|_\nu^r}{|1+\beta|_\nu^r} \leqq \frac{|\beta|_\nu^r}{1-|\beta|_\nu^r} \leqq \epsilon$$

for r sufficiently large.

THEOREM 1 (APPROXIMATION THEOREM). *If we are given any n nontrivial inequivalent valuations $|\ |_\nu$ of k, an element α_ν of k for each valuation, and an $\epsilon>0$, then we can find an element α of k such that*

$$|\alpha - \alpha_\nu|_\nu \leqq \epsilon \quad \text{for} \quad \text{each} \quad \nu = 1, 2, \cdots, n.$$

PROOF. Let M be the maximum of the numbers $|\alpha_i|_j$ for all combinations of i and j and choose β_i $(i=1, 2, \cdots, n)$ such that

$$|1-\beta_i|_i < \frac{\epsilon}{nM}, \qquad |\beta_i|_\nu < \frac{\epsilon}{nM} \quad \text{for} \quad \nu \neq i.$$

Let

$\alpha = \beta_1\alpha_1 + \beta_2\alpha_2 + \cdots + \beta_n\alpha_n$; then $|\alpha - \alpha_i|_i < \epsilon$ for each i.

COROLLARY. *If* $|\ |_1, |\ |_2, \cdots, |\ |_n$ *are nontrivial and inequivalent then a relation*

$$|x|_1^{\nu_1} |x|_2^{\nu_2} \cdots |x|_n^{\nu_n} = 1$$

is true for all $x \in k$, $x \neq 0$, *if and only if all* $\nu_i = 0$.

PROOF. If any $\nu_i \neq 0$, an x for which $|x|_i$ is sufficiently large and the other $|x|_\nu$ for $\nu \neq i$ are sufficiently near 1 gives a contradiction.

2. **The product formula.** Our corollary precludes the possibility that a finite number of valuations can be interrelated in a field. Such an interrelation may nevertheless happen for an infinite number of valuations. In case of the ordinary function fields and number fields that is not only the case but this fact may even be used to derive all the properties of these fields on a common basis.

We shall assume for our field k:

AXIOM 1. *There is a set* $\mathfrak{M}$ *of prime divisors* $\mathfrak{p}$ *and a fixed set of valuations* $|\ |_\mathfrak{p}$, *one for each* $\mathfrak{p} \in \mathfrak{M}$, *such that, for every* $\alpha \neq 0$ *of* k, $|\alpha|_\mathfrak{p} = 1$ *for all but a finite number of* $\mathfrak{p} \in \mathfrak{M}$ *and*

$$\prod_\mathfrak{p} |\alpha|_\mathfrak{p} = 1,$$

where this product is extended over all $\mathfrak{p} \in \mathfrak{M}$.

If this axiom is satisfied, $\mathfrak{M}$ can contain only a finite number of archimedean divisors: for $|1+1|_\mathfrak{p} > 1$ at all archimedean $\mathfrak{p}$. Suppose that Axiom 1 is satisfied and that $\mathfrak{M}$ contains no archimedean divisors at all; consider the set k_0 of all α for which $|\alpha|_\mathfrak{p} \leqq 1$ at all $\mathfrak{p} \in \mathfrak{M}$. Let α and β be two elements of k_0. It follows at once that $-\alpha$, $\alpha\beta$, and $\alpha+\beta$ are also in the set. If $\alpha \in k_0$ and $\alpha \neq 0$, the product formula gives at once $|\alpha|_\mathfrak{p} = 1$ for all $\mathfrak{p}$. It now follows that α^{-1} is in k_0. Thus k_0 forms a subfield of k, called the field of constants. It consists of 0 and those elements of k which satisfy $|\alpha|_\mathfrak{p} = 1$ for all $\mathfrak{p}$. It may also be defined as the largest subfield of k for which all $\mathfrak{p}$ reduce to the trivial valuation. If $\mathfrak{M}$ contains archimedean divisors, then there is no field of constants.

We associate with our set $\mathfrak{M}$ of valuations $\mathfrak{p}$ a certain space of vectors $\mathfrak{a}$ with one component $\alpha_\mathfrak{p}$ for each divisor $\mathfrak{p}$. The component $\alpha_\mathfrak{p}$ may range freely over the $\mathfrak{p}$-adic completion $k_\mathfrak{p}$ of k. If $\mathfrak{a}$ is such a vector we shall for brevity write $|\mathfrak{a}|_\mathfrak{p}$ instead of $|\alpha_\mathfrak{p}|_\mathfrak{p}$. The idèles of Chevalley[4] are special cases of these vectors; for an idèle we must have $\alpha_\mathfrak{p} \neq 0$ for all $\mathfrak{p}$ and $|\mathfrak{a}|_\mathfrak{p} = 1$ for all but a finite number of $\mathfrak{p}$.

[4] See Chevalley [3, 4].

Our field k may be considered a subset of this space inasmuch as $\alpha \in k$ may also be considered as the vector whose $\mathfrak{p}$-coordinate is the element α of $k_{\mathfrak{p}}$.

With each idèle $\mathfrak{a}$ we associate the product

$$V(\mathfrak{a}) = \prod_{\mathfrak{p}} |\mathfrak{a}|_{\mathfrak{p}}$$

and think of it as something measuring the size of $\mathfrak{a}$. In a moment we shall see that it may be interpreted as a "volume."

For elements α of k the product formula yields

$$V(\alpha) = 1$$

so that for all idèles $\mathfrak{a}$ we get

$$V(\alpha\mathfrak{a}) = V(\mathfrak{a}).$$

If we select real numbers $x_{\mathfrak{p}} > 0$ for each $\mathfrak{p}$ and take care that $x_{\mathfrak{p}} \neq 1$ for a finite number of $\mathfrak{p}$ only, then we call the set of vectors $\mathfrak{c}$ satisfying

$$|\mathfrak{c}|_{\mathfrak{p}} \leqq x_{\mathfrak{p}} \quad \text{for all } \mathfrak{p}$$

a parallelotope of dimensions $x_{\mathfrak{p}}$.

We shall find later that every valuation is either archimedean or discrete. If this is true then there is an element $\alpha_{\mathfrak{p}}$ in $k_{\mathfrak{p}}$ whose value is maximal and not greater than $x_{\mathfrak{p}}$ so that it is no restriction of generality to start with a given idèle $\mathfrak{a}$ and to construct all vectors $\mathfrak{c}$ satisfying

$$|\mathfrak{c}|_{\mathfrak{p}} \leqq |\mathfrak{a}|_{\mathfrak{p}}.$$

We talk in this case of a parallelotope of size $\mathfrak{a}$. The product $V(\mathfrak{a})$ may then be interpreted as its volume.

Next we introduce the "order" of a given set of elements. It is a notion that shall unite different types of fields. If k has an archimedean valuation we mean by order the number of elements. Otherwise k has a field k_0 of constants: we let q stand for an arbitrarily selected but fixed number greater than 1 when the number of elements of k_0 is infinite, and for the number of elements of k_0 when this number is finite. By order of a set we mean in this case the number q^s where s is the number of elements in our set that are linearly independent with respect to k_0. Should k_0 contain q elements and our set be closed under addition and under multiplication by elements of k_0 then q^s is the number of elements in the set.

In the next section we shall be interested in the order of the set of elements α of k that are contained in a given parallelotope of size $\mathfrak{a}$. We denote this order by $M(\mathfrak{a})$. If $\theta \neq 0$ is in k than $M(\theta\mathfrak{a}) = M(\mathfrak{a})$.

Indeed multiplication by θ transforms the parallelotope of size $\mathfrak{a}$ into the parallelotope of size $\theta\mathfrak{a}$ and does not change the order.

In the next section it will be shown that $V(\mathfrak{a})$ and $M(\mathfrak{a})$ are related; namely that they are of the same order of magnitude.

If $\mathfrak{p}$ is a nonarchimedean prime divisor, the elements $\alpha \in k$ for which $|\alpha|_{\mathfrak{p}} \leqq 1$ form a ring $\mathfrak{o}_{\mathfrak{p}}$, called the ring of $\mathfrak{p}$-integers (or local integers). The elements α for which $|\alpha|_{\mathfrak{p}} < 1$ form a prime ideal in this ring and we denote this ideal by the same symbol $\mathfrak{p}$ as the prime divisor. If the residue class field $\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}$ is of finite order then we call this order the norm of $\mathfrak{p}$ and denote it by $N\mathfrak{p}$. We can talk of the order also in case of a constant field k_0 since k_0 may be considered as subfield of the field $\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}$. Thus, if f is the degree of $\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}$ over k_0, and if f is finite, we put $N\mathfrak{p} = q^f$.

AXIOM 2. *The set $\mathfrak{M}$ of Axiom 1 contains at least one prime $\mathfrak{q}$, which is of one of the following two types:*

1. *Discrete, with a residue class field of finite order $N\mathfrak{q}$.*

2. *Archimedean, with a completed field $k_{\mathfrak{q}}$ which is either the real or the complex field.*[5]

As mentioned before, there are an infinity of equivalent valuations belonging to one prime divisor $\mathfrak{p}$. One of them, $|\alpha|_{\mathfrak{p}}$, is singled out by our Axiom 1. For primes $\mathfrak{p}$ satisfying Axiom 2 we shall define another one that is singled out by inner properties. In case 1 of Axiom 2 we put (for $\alpha \neq 0$)

$$\|\alpha\|_{\mathfrak{p}} = \frac{1}{N\mathfrak{p}^{\nu}}$$

where ν is the ordinal number of α at $\mathfrak{p}$. In case 2 we take $\|\alpha\|_{\mathfrak{p}}$ to be ordinary absolute value when $k_{\mathfrak{p}}$ is the real field and the square of ordinary absolute value when $k_{\mathfrak{p}}$ is the complex field. Note that in the latter case $\|\alpha\|_{\mathfrak{p}}$ is not a true valuation. We call $\|\alpha\|_{\mathfrak{p}}$ the normed valuation at $\mathfrak{p}$.

THEOREM 2. *In case of the following special fields k we can construct a set $\mathfrak{M}$ of valuations such that our axioms hold, and the second one even holds for all $\mathfrak{p}$ of $\mathfrak{M}$:*

1. *Any finite algebraic number field (that is, a finite extension of the field of rational numbers).*

2. *Any field of algebraic functions over any given field k_1 (that is, a finite extension of the field $k_1(z)$ where z is transcendental with respect to k_1).*

[5] It is well known (Ostrowski [5]) that we could drop this condition on the completed field.

In case 2, the constant field k_0 of k with respect to $\mathfrak{M}$ consists of all elements of k that are algebraic with respect to k_1.

The proof is contained in the following chain of statements:

LEMMA 4. *Let k be a field for which Axiom 1 holds and R a subfield consisting not exclusively of constants of k. Let $\mathfrak{N}$ be the set of those non-trivial divisors p of R that are divisible by some $\mathfrak{p}$ of $\mathfrak{M}$. Then Axiom 1 holds in R for this set $\mathfrak{N}$.*

PROOF. Let p be any divisor of $\mathfrak{N}$ and a an element of R such that $|a|_p > 1$. Then $|a|_{\mathfrak{p}} > 1$ for all $\mathfrak{p}$ that divide p. Because of Axiom 1 there can be only a finite number of $\mathfrak{p} \mid p$. Let us now define

$$|b|_p = \prod_{\mathfrak{p} \mid p} |b|_{\mathfrak{p}} \quad \text{for all} \quad b \in R$$

and we have a set of valuations $|\ |_p$ for which Axiom 1 holds.

LEMMA 5. *Let k be a field for which Axiom 1 holds and K a finite algebraic extension of k. Let $\mathfrak{N}$ be the set of all divisors $\mathfrak{P}$ of K that divide some $\mathfrak{p}$ of $\mathfrak{M}$. Then Axiom 1 holds in K for some subset $\mathfrak{N}'$ of $\mathfrak{N}$.*

(It would not be difficult to show now that $\mathfrak{N}' = \mathfrak{N}$, but it is better to postpone this and other details until the next section.)

PROOF. 1. Let $A \neq 0$ be an element of K and $f(x) = 0$ the equation for A with coefficients in k and with highest coefficient 1. If $\mathfrak{p}$ is a nonarchimedean valuation for which all coefficients in $f(x)$ have a value not greater than 1 and $\mathfrak{P}$ a divisor of $\mathfrak{p}$, then $|A|_{\mathfrak{P}} \leqq 1$ or else no cancellation could take place between the highest term in $f(A) = 0$ and the others. So $|A|_{\mathfrak{P}} \leqq 1$ for all but a finite number of $\mathfrak{P}$. For the same reason $|1/A|_{\mathfrak{P}} \leqq 1$ for all but a finite number of $\mathfrak{P}$. Therefore $|A|_{\mathfrak{P}} \neq 1$ for only a finite number of $\mathfrak{P}$.

2. Let $F(x)$ be a polynomial in k that has the generators of K among its roots ($F(x)$ need not be irreducible). If K' is the splitting field of $F(x)$ we may first prove Lemma 5 for K' instead of K and then descend to the subfield K by use of Lemma 4. This shows that we may already assume that K is the splitting field of a polynomial $F(x)$ in k.

The algebraic structure of such a field is well known. If $\mathfrak{G}$ is the group of all its automorphisms σ and if we construct for any $A \in K$ the product

$$\prod_{\sigma} A^{\sigma} = \alpha$$

then α is invariant under $\mathfrak{G}$. Since we have to consider also the in-

separable case we do not know that α is in k. But there is always a positive integer m such that

$$\prod_{\sigma} (A^{\sigma})^{m} = a$$

is in k whatever A may be. Because of the product formula in k we get

$$\prod_{\mathfrak{p}} |a|_{\mathfrak{p}} = 1.$$

Now select, for each $\mathfrak{p}$, one divisor $\mathfrak{P}$ of K which divides $\mathfrak{p}$ and define $|\ |_{\mathfrak{P}}$ in such a way that $|b|_{\mathfrak{P}} = |b|_{\mathfrak{p}}$ for all b in k. Then

$$|a|_{\mathfrak{p}} = \prod_{\sigma} |A^{\sigma}|_{\mathfrak{P}}^{m}.$$

If we consider the expression $|A^{\sigma}|_{\mathfrak{P}}$ as function of A, it is clearly a valuation of K that belongs to a divisor $\mathfrak{P}'$ which divides $\mathfrak{p}$ and may be equal to or different from $\mathfrak{P}$. If we change our notation slightly we obviously get

$$|a|_{\mathfrak{p}} = \prod_{\mathfrak{P}'} |A|'_{\mathfrak{P}'},$$

where $\mathfrak{P}'$ runs through some divisors of $\mathfrak{p}$ and where $|\ |'_{\mathfrak{P}'}$ is a certain valuation belonging to $\mathfrak{P}'$.

If we substitute this in our product-formula we get

$$\prod_{\mathfrak{p}} \prod_{\mathfrak{P}'} |A|'_{\mathfrak{P}'} = 1$$

and this proves Lemma 5.

Before we proceed with our next lemma let us consider the special field $R = k_1(z)$ of Theorem 2. If p is a nontrivial valuation of R that reduces to the trivial one on k_1 then p is nonarchimedean and we distinguish two cases:

1. If $|z|_p \leqq 1$ then $|f(z)|_p \leqq 1$ for every polynomial in z. Let $p(z)$ be a polynomial of lowest degree such that $|p(z)|_p < 1$. If $g(z)$ is another polynomial with $|g(z)|_p < 1$ then we divide:

$$g(z) = p(z)h(z) + r(z),$$

where the degree of $r(z)$ is lower than that of $p(z)$. From

$$r(z) = g(z) - p(z)h(z)$$

we get $|r(z)|_p < 1$; hence $r(z) = 0$.

Now let $\phi(z)$ be any element of R and put

$$\phi(z) = p(z)^{r} \cdot \psi(z),$$

where neither numerator nor denominator of $\psi(z)$ is divisible by $p(z)$. Then $|\psi(z)|_p = 1$ so

$$|\phi(z)|_p = |p(z)|_p^{\nu} = c^{\nu}, \quad \text{where} \quad c = |p(z)|_p < 1.$$

$p(z)$ is obviously irreducible.

In order to find the normed valuation $\| \ \|_p$ in this case we have to determine the degree of the residue class field (mod $p(z)$). It is the degree f of $p(z)$ so that $Np = q^f$ and

$$\|\phi(z)\|_p = q^{-\nu f}.$$

2. If $|z|_p > 1$ we replace z by $y = 1/z$. Then $|y|_p < 1$ and we have our previous case. The polynomial in y of lowest degree is y itself, so that there is only one prime divisor p of this kind. We denote it by p_∞.

Let $\phi(z) = g(z)/h(z)$ where $g(z)$ and $h(z)$ are polynomials of degrees m and n. Then

$$\phi(z) = y^{n-m} \cdot \frac{g_1(y)}{h_1(y)}$$

where $g_1(y)$ and $h_1(y)$ are polynomials not divisible by y. Hence

$$\|\phi(z)\|_{p_\infty} = q^{m-n}.$$

A product formula connecting all these valuations or a subset of them can be written in the form

$$\prod_p \|\phi(z)\|_p^{\lambda(p)} = 1,$$

where $\lambda(p)$ are constants not less than 0. If we substitute for $\phi(z)$ the irreducible polynomials $p(z)$, then only two factors can possibly be different from 1: the valuations at the p belonging to $p(z)$ and at p_∞. This gives

$$q^{-f\lambda(p_\infty)} \cdot q^{f\lambda(p)} = 1$$

or $\lambda(p) = \lambda(p_\infty)$. So all $\lambda(p)$ are equal and may therefore be assumed to be equal to 1. In order to show that this product formula holds we put

$$V(\phi(z)) = \prod_p \|\phi(z)\|_p.$$

It is obvious that $V(\phi(z) \cdot \psi(z)) = V(\phi(z)) \cdot V(\psi(z))$ and that a similar rule holds for quotients.

We have just seen that $V(p(z)) = 1$ for any irreducible polynomial; it follows that $V(\phi(z)) = 1$ for any element $\phi(z) \neq 0$ of R.

In the same fashion we can discuss the field R of rational numbers.

It is well known that all valuations are either the single archimedean p_∞ for which $\|a\|_{p_\infty}$ is the ordinary absolute value or the p-adic valuations of R where p is a prime number. The normed valuation $|a|_p$ in this latter case is given by $1/p^\nu$, if ν is the ordinal number of a. Just as before we consider a hypothetical product formula

$$\prod_p \|a\|_p^{\lambda(p)} = 1.$$

Substituting for a a prime number p we get

$$\left(\frac{1}{p}\right)^{\lambda(p)} \cdot p^{\lambda(p_\infty)} = 1$$

or $\lambda(p)=\lambda(p_\infty)$. The numbers $\lambda(p)$ are therefore equal and may be considered equal to 1. The same method as before shows that the product formula really holds.

LEMMA 6. *Axiom* 1 *holds in the case of the field R of rational numbers and that of $R=k_1(z)$. If R is the rational field, $\mathfrak{M}$ is the set of all valuations; if $R=k_1(z)$, it is the set of all valuations that are trivial on k_1. The product formula itself takes on the form*

$$\prod_p \|a\|_p = 1$$

or a power of it and there is no other relation between these valuations.

Lemmas 5 and 6 already show that Axiom 1 holds for the fields mentioned in Theorem 2. That all valuations of $\mathfrak{M}$ satisfy Axiom 2 follows from the fact that this is true in R and consequently in a finite extension k.

It remains to prove the statement about the field k_0 of constants. If $\mathfrak{p}$ is trivial on k_1 it is also trivial on an algebraic extension of k_1. Hence we need only show that any constant c of k_0 is algebraic with respect to k_1. If on the contrary c were transcendental with respect to k_1 then from the equation c satisfied with respect to $k_1(z)$ it follows that z would be algebraic with respect to $k_1(c)$. Since $k_1(c)$ is in k_0, this would mean that z is in k_0. So all of k would be in k_0, contradicting the fact that no $\mathfrak{p}$ of $\mathfrak{M}$ is trivial on k.

More detailed information about the fields of Theorem 2 will follow from the next section.

3. **Characterization of fields by the product formula.** In this section we assume k to be any field for which the Axioms 1 and 2 hold and are going to prove that k is of the type described in Theorem 2.

For any prime $\mathfrak{p}$ that satisfies Axiom 2 we shall have to distinguish the valuation $|\alpha|_{\mathfrak{p}}$ of Axiom 1 and the equivalent normed valuation $\|\alpha\|_{\mathfrak{p}}$. We define the real number $\rho(\mathfrak{p})>0$ by

$$|\alpha|_{\mathfrak{p}} = \|\alpha\|_{\mathfrak{p}}^{\rho(\mathfrak{p})}.$$

By R we mean the following subfield of k:

1. If $\mathfrak{M}$ has archimedean valuations, R is the rational field. By $\|a\|_{p_\infty}$ we mean the ordinary absolute value in R.

2. In the other case k has a field k_0 of constants and cannot contain any algebraic extension of k_0 since our valuations are trivial on k_0 and would be trivial on that extension. Let z be any element of k not in k_0; then $R=k_0(z)$ is a transcendental extension of k_0. By integers we mean in this case the polynomials in z. By $\|a\|_{p_\infty}$ we mean the one valuation we found in proving Lemma 6 that has $\|z\|_{p_\infty}>1$.

In both cases we mean by $\mathfrak{p}_\infty$ any divisor of $\mathfrak{M}$ that divides p_∞. Since the product formula, when applied to elements of R, must reduce to the formula of Theorem 2, our set $\mathfrak{M}$ always contains at least one $\mathfrak{p}_\infty$. The other primes of $\mathfrak{M}$ shall be called finite. For elements a of R the valuations $|a|_{\mathfrak{p}_\infty}$ and $\|a\|_{p_\infty}$ are equivalent. We define the real numbers $\lambda(\mathfrak{p}_\infty)>0$ by

$$|a|_{\mathfrak{p}_\infty} = \|a\|_{p_\infty}^{\lambda(\mathfrak{p}_\infty)} \text{ for all } a \in R.$$

LEMMA 7. *Let $\mathfrak{q}$ be one of the primes satisfying Axiom 2 and $\mathfrak{S}$ be a set of elements of k of an order $M>1$. Let x be an upper bound for $|\alpha|_{\mathfrak{q}}$ for all α of $\mathfrak{S}$: $|\alpha|_{\mathfrak{q}} \leqq x$. Then there is an element θ of k with the following properties:*

(1) *θ is either a difference of two elements of $\mathfrak{S}$ or, in case there is a field of constants, a linear combination of elements of $\mathfrak{S}$ with coefficients in k_0.*

(2) $\theta \neq 0$.

(3) $|\theta|_{\mathfrak{q}} \leqq A_{\mathfrak{q}} x/M^{\rho(\mathfrak{q})}$ *where $A_{\mathfrak{q}}$ is a constant depending only on $\mathfrak{q}$.*

PROOF. 1. $\mathfrak{q}$ archimedean, $k_{\mathfrak{q}}$ real. In this case we may treat k as a subfield of the real field. We have

$$\|\alpha\|_{\mathfrak{q}} \leqq x^{1/\rho(\mathfrak{q})}$$

for each of the M elements α of $\mathfrak{S}$. Divide the interval from $-x^{1/\rho(\mathfrak{q})}$ to $x^{1/\rho(\mathfrak{q})}$ into $M-1$ equal parts. Two of the α's must be in the same compartment so their difference θ satisfies

$$\|\theta\|_{\mathfrak{q}} \leqq \frac{2x^{1/\rho(\mathfrak{q})}}{M-1} \leqq \frac{4x^{1/\rho(\mathfrak{q})}}{M},$$

hence

$$|\theta|_{\mathfrak{q}} \leqq \frac{4^{\rho(\mathfrak{q})}x}{M^{\rho(\mathfrak{q})}}.$$

2. $\mathfrak{q}$ archimedean, $k_{\mathfrak{q}}$ complex. Treating k as a subfield of the complex field, $\|\alpha\|_{\mathfrak{q}}^{1/2} = |\alpha|_{\mathfrak{q}}^{1/2\rho(\mathfrak{q})}$ is the ordinary distance from the origin to the point α and is less than $x^{1/2\rho(\mathfrak{q})}$. Writing $\alpha = \xi + i\eta$ for each $\alpha \in \mathfrak{S}$ we know that $\mathfrak{S}$ is in the square $|\xi| \leqq x^{1/2\rho(\mathfrak{q})}$ $|\eta| \leqq x^{1/2\rho(\mathfrak{q})}$. Divide this square into N^2 small squares by dividing each side into N equal parts, where $N < M^{1/2} \leqq N+1$. Then some two α's are in the same subdivision so their difference θ satisfies:

$$\|\theta\|_{\mathfrak{q}}^{1/2} \leqq \frac{2^{3/2}x^{1/2\rho(\mathfrak{q})}}{N} \leqq \frac{2^{5/2}x^{1/2\rho(\mathfrak{q})}}{M^{1/2}}$$

so

$$|\theta|_{\mathfrak{q}} \leqq \frac{(2^{5/2})^{2\rho(\mathfrak{q})}x}{M^{\rho(\mathfrak{q})}}.$$

3. $\mathfrak{q}$ discrete. Let α_1 be an α for which $|\alpha|_{\mathfrak{q}}$ is maximum. This exists since $\mathfrak{q}$ is discrete and $|\alpha|_{\mathfrak{q}} \leqq x$. Then for each $\alpha \in \mathfrak{S}$, $|\alpha/\alpha_1|_{\mathfrak{q}} \leqq 1$.

Choose r so that $N\mathfrak{q}^r < M \leqq N\mathfrak{q}^{r+1}$. If the number of elements in the residue class field is finite then the local theory shows easily that $\mathfrak{o}_{\mathfrak{q}}$ contains at most $N\mathfrak{q}^r$ residue classes mod $\mathfrak{q}^r$. Hence two of the $M > N\mathfrak{q}^r$ elements of $(1/\alpha_1)\mathfrak{S}$ are in the same residue class and their difference θ/α_1 has at least the ordinal number r. Should there be a field k_0, let f be the degree of $\mathfrak{o}_{\mathfrak{q}}/\mathfrak{q}$ over k_0, so that $N\mathfrak{q} = q^f$. Then there are at most rf elements of $\mathfrak{o}_{\mathfrak{q}}$ that are linearly independent mod $\mathfrak{q}^r$. Taking more than rf of our elements α/α_1 that are independent considered as elements of k (possible since $M > N\mathfrak{q}^r$) we can find a linear combination $\theta/\alpha_1 \neq 0$ of them that is congruent to 0 (mod $\mathfrak{q}^r$) and hence has at least the ordinal number r. In both cases we get

$$\left\|\frac{\theta}{\alpha_1}\right\|_{\mathfrak{q}} \leqq \frac{1}{N\mathfrak{q}^r} = \frac{N\mathfrak{q}}{N\mathfrak{q}^{r+1}} \leqq \frac{N\mathfrak{q}}{M}, \qquad \|\theta\|_{\mathfrak{q}} \leqq \frac{N\mathfrak{q}\cdot\|\alpha_1\|_{\mathfrak{q}}}{M},$$

or

$$|\theta|_{\mathfrak{q}} \leqq \frac{N\mathfrak{q}^{\rho(\mathfrak{q})}|\alpha_1|_{\mathfrak{q}}}{M^{\rho(\mathfrak{q})}} \leqq \frac{N\mathfrak{q}^{\rho(\mathfrak{q})}\cdot x}{M^{\rho(\mathfrak{q})}}.$$

LEMMA 8. *Let M be the order of the set of elements $\alpha \in k$ that is contained in a parallelotope of dimensions $x_{\mathfrak{p}}$. If $\mathfrak{q}$ is a prime satisfying Axiom 2 we can find a constant $B_{\mathfrak{q}}$ depending only on $\mathfrak{q}$ such that either $M = 1$ (if our set contains only $\alpha = 0$) or*

$$M \leqq B_q\Big(\prod_{\mathfrak{p}} x_{\mathfrak{p}}\Big)^{1/\rho(q)}.$$

PROOF. Assume $M>1$. By Lemma 7 there is a $\theta\neq 0$ satisfying

$$|\theta|_q \leqq \frac{A_q x_q}{M^{\rho(q)}}.$$

For the other $\mathfrak{p}$ of $\mathfrak{M}$ we estimate θ directly and get

$$|\theta|_{\mathfrak{p}} \leqq \begin{cases} x_{\mathfrak{p}} \text{ at any nonarchimedean } \mathfrak{p}, \\ 4^{\rho(\mathfrak{p})}\cdot x_{\mathfrak{p}} \text{ at any archimedean } \mathfrak{p}. \end{cases}$$

Substituting in the product formula $\prod_{\mathfrak{p}}|\theta|_{\mathfrak{p}}=1$ we get (if D_q is a certain constant):

$$1 \leqq \frac{D_q\cdot\prod_{\mathfrak{p}} x_{\mathfrak{p}}}{M^{\rho(q)}},$$

hence the lemma.

LEMMA 9. *If $\alpha_1, \alpha_2, \cdots, \alpha_l$ are linearly independent with respect to the subfield R and if y is a given nonzero integer of R, we can construct a certain set $\mathfrak{S}$ of elements α with the following properties:*

1. $|\alpha|_{\mathfrak{p}} \leqq a_{\mathfrak{p}} = \max_{i=1,\ldots,l}(|\alpha_i|_{\mathfrak{p}})$ *for every finite* $\mathfrak{p}$.
2. $|\alpha|_{\mathfrak{p}_\infty} \leqq B\cdot|y|_{\mathfrak{p}_\infty}$ *with a certain constant B that can be easily estimated.*
3. *If there is a field of constants k_0 then $\mathfrak{S}$ is closed under addition and under multiplication by elements of k_0, so $\mathfrak{S}$ may be considered as a vector space over k_0.*
4. *The order of $\mathfrak{S}$ is greater than $\|y\|^l_{p_\infty}$.*

PROOF. Let $\mathfrak{S}$ consist of all α of the form

$$\alpha = \nu_1\alpha_1 + \nu_2\alpha_2 + \cdots + \nu_l\alpha_l$$

where the ν_i range over all integers of R that satisfy

$$\|\nu_i\|_{p_\infty} \leqq \|y\|_{p_\infty}.$$

This settles at once property 3 and implies $|\nu_i|_{\mathfrak{p}_\infty} \leqq |y|_{\mathfrak{p}_\infty}$ for each $\mathfrak{p}_\infty$ and consequently property 2. Property 1 holds since $|\nu_i|_{\mathfrak{p}} \leqq 1$ for all finite $\mathfrak{p}$. Property 4 is clear if p_∞ is archimedean; if not then assume $\|y\|_{p_\infty}=q^d$ so that y is a polynomial of degree d. Each ν_i ranges over all polynomials of degree not greater than d. This gives for $\mathfrak{S}$ a vector space of $(d+1)l$ dimensions and our statement is obvious.

LEMMA 10. *The degree n of k over R is finite; every $\mathfrak{p}$ of M satisfies Axiom 2; and the inequality*

$$n \leqq \frac{1}{\rho(\mathfrak{p})} \cdot \sum_{\mathfrak{p}_\infty} \lambda(\mathfrak{p}_\infty)$$

holds for each p.

PROOF. Apply Lemma 8 to the set of Lemma 9. We get the inequality

$$\|y\|_{p_\infty}^{l} \leqq E \cdot \prod_{\mathfrak{p}_\infty} |y|_{\mathfrak{p}_\infty}^{1/\rho(\mathfrak{q})} = E \cdot \|y\|_{p_\infty}^{(1/\rho(\mathfrak{q}))\sum \mathfrak{p}_\infty \lambda(\mathfrak{p}_\infty)},$$

where E is a certain constant that depends on the constants in the previous lemmas. Since $\|y\|_{p_\infty}$ takes on arbitrarily large values we get

$$l \leqq \frac{1}{\rho(\mathfrak{q})} \sum_{\mathfrak{p}_\infty} \lambda(\mathfrak{p}_\infty).$$

This proves that n is finite. None of our valuations $\mathfrak{p}$ is trivial on R or else it would be trivial on the finite extension k. Let p be the divisor of R that is divisible by $\mathfrak{p}$. The local theory shows now (since p is non-trivial) that $\mathfrak{p}$ satisfies Axiom 2. In our previous inequality we can therefore assume $l=n$ and take for $\mathfrak{q}$ each prime $\mathfrak{p}$ of $\mathfrak{M}$.

Let r be a positive real number and let us replace each valuation $|\alpha|_{\mathfrak{p}}$ by its rth power $|\alpha|_{\mathfrak{p}}^{r}$. This would be a new set of valuations for which Axioms 1 and 2 would hold again. The numbers $\lambda(\mathfrak{p}_\infty)$ would then be replaced by $r\lambda(\mathfrak{p}_\infty)$. This shows that it is no restriction of generality to assume that

$$\sum_{\mathfrak{p}_\infty} \lambda(\mathfrak{p}_\infty) = n.$$

Then Lemma 10 gives

$$\rho(\mathfrak{p}) \leqq 1$$

for every $\mathfrak{p}$.

Assume now that $\mathfrak{p} | p$, where p is a nonarchimedean divisor of R, and let us compare $\|a\|_{\mathfrak{p}}$ and $\|a\|_p$ for elements a of R. The ordinal number of a in k is $e(\mathfrak{p})$ times the ordinal number of a measured in R; we also have $N\mathfrak{p} = (Np)^{f(\mathfrak{p})}$. $e(\mathfrak{p})$ is the ramification number and $f(\mathfrak{p})$ the degree of the residue class fields. So

$$\|a\|_{\mathfrak{p}} = \|a\|_p^{e(\mathfrak{p})f(\mathfrak{p})} = \|a\|_p^{n(\mathfrak{p})}.$$

For an archimedean $\mathfrak{p}$ this equality follows directly from the definitions. Hence we have

$$|a|_{\mathfrak{p}} = \|a\|_p^{n(\mathfrak{p})\rho(\mathfrak{p})} \text{ for all } \mathfrak{p} \text{ and all } a \in R.$$

We note in particular $\lambda(\mathfrak{p}_\infty) = n(\mathfrak{p}_\infty)\rho(\mathfrak{p}_\infty)$ so that

$$\sum_{\mathfrak{p}_\infty} n(\mathfrak{p}_\infty)\rho(\mathfrak{p}_\infty) = n.$$

Now we apply the product formula to an $a \in R$:

$$1 = \prod_{\mathfrak{p}} |a|_{\mathfrak{p}} = \prod_{p} \Big(\prod_{\mathfrak{p}|p,\, \mathfrak{p} \in \mathfrak{M}} \|a\|_p^{n(\mathfrak{p})\rho(\mathfrak{p})} \Big) = \prod_{p} \|a\|_p^{\nu(p)},$$

where

$$\nu(p) = \sum_{\mathfrak{p}|p,\, \mathfrak{p} \in \mathfrak{M}} n(\mathfrak{p})\rho(\mathfrak{p}).$$

But Lemma 6 shows that all $\nu(p)$ are equal and the special case $p = p_\infty$ shows finally

$$n = \sum_{\mathfrak{p}|p,\, \mathfrak{p} \in \mathfrak{M}} n(\mathfrak{p})\rho(\mathfrak{p}).$$

If we compare this with $\rho(\mathfrak{p}) \leqq 1$ and $\sum_{\mathfrak{p}|p} n(\mathfrak{p}) \leqq n$ we find:

(1) all $\mathfrak{p}|p$ are in $\mathfrak{M}$,

(2) all $\rho(\mathfrak{p}) = 1$,

(3) $\sum_{\mathfrak{p}|p} n(\mathfrak{p}) = n$.

Thus we have proved:

THEOREM 3. *If k is a field that satisfies the Axioms* 1 *and* 2 *it is an extension of a finite degree n either of the rational field R or of the field $R = k_0(z)$ of rational functions over its field of constants k_0. All valuations satisfy Axiom* 2. *$\mathfrak{M}$ consists of all extensions of the well known valuations of R. Replacing if necessary all valuations in the product formula by the same power we can assume that they are all normed (that is, $|\alpha|_{\mathfrak{p}} = \|\alpha\|_{\mathfrak{p}}$). We have $\sum_{\mathfrak{p}|p} n_{\mathfrak{p}} = n$ for all p of R.*

Let now α be an element of k and $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r$ those among the finite primes for which $\|\alpha\|_{\mathfrak{p}_i} > 1$. Let $p_1, p_2, \cdots, p_l$ be the primes of R that have the $\mathfrak{p}_\nu$ as divisors. Construct an integer in R whose absolute value at each p_i is sufficiently small and $a\alpha$ will now be less than or equal to 1 at all finite primes. This shows that any set $\alpha_1, \alpha_2, \cdots, \alpha_l$ of elements that are linearly independent with respect to R can be replaced by a set of elements which are integral at all finite primes. This will be useful in the next section.

4. Parallelotopes. We still make the same assumptions as in the previous chapter so that we can assume Theorem 3. Thus we will take $|\alpha|_{\mathfrak{p}} = \|\alpha\|_{\mathfrak{p}}$ and $\rho(\mathfrak{p}) = 1$. In Lemma 9 we may assume $l = n$.

THEOREM 4. *There are two positive constants C and D such that for all idèles $\mathfrak{a}$ we have*

$$CV(\mathfrak{a}) < M(\mathfrak{a}) \leqq \max(1, DV(\mathfrak{a})).$$

PROOF. If we apply Lemma 8 for one particular $\mathfrak{q}$ we get the right half of the inequality.

If we replace $\mathfrak{a}$ by $\alpha\mathfrak{a}$ then $V(\mathfrak{a})$ and $M(\mathfrak{a})$ remain unchanged. Select $\alpha=\alpha_1 y$ where α_1 and y are selected as follows:

Theorem 1 shows that there is an α_1 such that

$$4B \leqq \|\alpha_1\mathfrak{a}\|_{\mathfrak{p}_\infty} \leqq 5B \quad \text{for all} \quad \mathfrak{p}_\infty,$$

where B is the constant of Lemma 9. We choose such an α_1 and then select an integer y of R in such a way that $\|\alpha_1 y\mathfrak{a}\|_{\mathfrak{p}} \leqq 1$ at all finite $\mathfrak{p}$. This shows that it is sufficient to prove our theorem for all idèles $\mathfrak{a}$ satisfying

$$4B\|y\|_{\mathfrak{p}_\infty} \leqq \|\mathfrak{a}\|_{\mathfrak{p}_\infty} \leqq 5B\|y\|_{\mathfrak{p}_\infty} \quad \text{for all} \quad \mathfrak{p}_\infty$$

and $\|\mathfrak{a}\|_{\mathfrak{p}} \leqq 1$ at all finite $\mathfrak{p}$, where y is an integer of R. Using this integer y, we now apply Lemma 9, taking $a_{\mathfrak{p}}=1$ at each finite $\mathfrak{p}$ and constructing a set $\mathfrak{S}$ of elements α of k with the following properties:

1. $\|\alpha\|_{\mathfrak{p}} \leqq 1$ for all finite $\mathfrak{p}$.
2. $\|\alpha\|_{\mathfrak{p}_\infty} \leqq B\|y\|_{\mathfrak{p}_\infty}$.
3. In case there is a field k_0, $\mathfrak{S}$ is a vectorspace over k_0.
4. The order of $\mathfrak{S}$ is greater than $\|y\|^n_{\mathfrak{p}_\infty}$ and we have

$$\|y\|^n_{\mathfrak{p}_\infty} = \|y\|_{\mathfrak{p}_\infty}^{\sum_{\mathfrak{p}_\infty}\lambda(\mathfrak{p}_\infty)} = \prod_{\mathfrak{p}_\infty}\|y\|_{\mathfrak{p}_\infty} \geqq \prod_{\mathfrak{p}_\infty}\frac{1}{5B}\|\mathfrak{a}\|_{\mathfrak{p}_\infty}.$$

So the order is greater than $C\prod_{\mathfrak{p}_\infty}\|a\|_{\mathfrak{p}_\infty}$ where C is a certain constant not equal to 0.

We distinguish two cases:

1. Order of a set means number. Consider the set $\mathfrak{o}$ of all integers of k (that is, all elements that are integers for every finite $\mathfrak{p}$) and the subset $\{\mathfrak{a}\}$ of all integers β satisfying $\|\beta\|_{\mathfrak{p}} \leqq \|\mathfrak{a}\|_{\mathfrak{p}}$ for all finite $\mathfrak{p}$. This subset $\{\mathfrak{a}\}$ forms an additive group which is the intersection of all the groups $\{\mathfrak{a}\}_{\mathfrak{p}}$ of integers satisfying $\|\beta\|_{\mathfrak{p}} \leqq \|\mathfrak{a}\|_{\mathfrak{p}}$ for only this particular $\mathfrak{p}$. The local theory shows that the index of $\mathfrak{o}$ mod $\{\mathfrak{a}\}_{\mathfrak{p}}$ is at most $1/\|\mathfrak{a}\|_{\mathfrak{p}}$. So the index of $\{\mathfrak{a}\}$ in the group of all integers is at most $N=\prod_{\mathfrak{p}\,\text{fin}}(1/\|\mathfrak{a}\|_{\mathfrak{p}})$. If we consider now our set $\mathfrak{S}$ modulo $\{\mathfrak{a}\}$ we get at most N residue classes. So one residue class contains more than

$$\frac{C\cdot\prod\|\mathfrak{a}\|_{\mathfrak{p}_\infty}}{N} = CV(\mathfrak{a})$$

elements. If we select one special element of this residue class and subtract it from each of the others, we get more than $CV(\mathfrak{a})$ elements γ of $\{\mathfrak{a}\}$. As such they satisfy $\|\gamma\|_{\mathfrak{p}} \leqq \|\mathfrak{a}\|_{\mathfrak{p}}$ for all finite p. At a $\mathfrak{p}_\infty$ we get $\|\gamma\|_{\mathfrak{p}_\infty} \leqq 4B\|y\|_{\mathfrak{p}_\infty} \leqq \|\mathfrak{a}\|_{\mathfrak{p}_\infty}$. (The factor 4 instead of the expected 2 must be used since one of the valuations may be the square of a true valuation.) So we have found more than $CV(\mathfrak{a})$ elements in our parallelotope of size $\mathfrak{a}$.

2. There is a constant field k_0. We define $\{\mathfrak{a}\}$ and $\{\mathfrak{a}\}_{\mathfrak{p}}$ as before. Assume that m is the dimension of the vector space $\mathfrak{S}$ over k_0. The residue classes of the integers mod $\{\mathfrak{a}\}_{\mathfrak{p}}$ also form a vector space over k_0; let $d(\mathfrak{p})$ denote its dimension. Then $q^{d(\mathfrak{p})} \leqq 1/\|\mathfrak{a}\|_{\mathfrak{p}}$. Let $\mathfrak{S}_1$ be the intersection of $\mathfrak{S}$ and $\{\mathfrak{a}\}_{\mathfrak{p}_1}$. Starting with a basis for the space $\mathfrak{S}_1$, we need at most $d(\mathfrak{p}_1)$ vectors to complete it to a basis of $\mathfrak{S}$. So the dimension of $\mathfrak{S}_1$ is at least $m-d(\mathfrak{p}_1)$. Repeating this process for all finite $\mathfrak{p}$ and calling $\mathfrak{T}$ the intersection of $\mathfrak{S}$ and $\{\mathfrak{a}\}$, we see that its dimension is at least $m-\sum_{\mathfrak{p}\text{ fin}} d(\mathfrak{p})$. So the order of $\mathfrak{T}$ is at least

$$q^m \cdot \prod_{\mathfrak{p}\text{ fin}} \frac{1}{q^{d(\mathfrak{p})}} \geqq q^m \cdot \prod_{\mathfrak{p}\text{ fin}} \|\mathfrak{a}\|_{\mathfrak{p}}.$$

Since the order q^m of $\mathfrak{S}$ is $C\prod_{\mathfrak{p}_\infty}\|\mathfrak{a}\|_{\mathfrak{p}_\infty}$ we find that the order of $\mathfrak{T}$ is greater than $CV(\mathfrak{a})$. That the elements γ of $\mathfrak{T}$ satisfy $\|\gamma\|_{\mathfrak{p}} \leqq \|\mathfrak{a}\|_{\mathfrak{p}}$ follows for a finite $\mathfrak{p}$ from the fact that they are in $\{\mathfrak{a}\}$. For $\mathfrak{p}_\infty$, since they are in $\mathfrak{S}$,

$$\|\gamma\|_{\mathfrak{p}_\infty} \leqq B\|y\|_{\mathfrak{p}_\infty} \leqq \|\mathfrak{a}\|_{\mathfrak{p}_\infty}.$$

COROLLARY. *If $V(\mathfrak{a}) \geqq 1/C$ then there is a β in k such that*

$$1 \leqq \|\beta\mathfrak{a}\|_{\mathfrak{p}} \leqq V(\mathfrak{a}) \quad \textit{for all} \quad \mathfrak{p}.$$

PROOF. The field elements in the parallelotope of size $\mathfrak{a}$ form a set of order greater than 1 so there is an $\alpha \neq 0$ such that $\|\alpha\|_{\mathfrak{p}} \leqq \|\mathfrak{a}\|_{\mathfrak{p}}$ for all $\mathfrak{p}$. Put $\beta = 1/\alpha$; then $1 \leqq \|\beta\mathfrak{a}\|_{\mathfrak{p}}$. Now for each $\mathfrak{q}$

$$\|\beta\mathfrak{a}\|_{\mathfrak{q}} = \frac{V(\beta\mathfrak{a})}{\prod_{\mathfrak{p}\neq\mathfrak{q}}\|\beta\mathfrak{a}\|_{\mathfrak{p}}} \leqq V(\beta\mathfrak{a}) = V(\mathfrak{a}).$$

LEMMA 11. *Let $\mathfrak{a}$ be any idèle and $\mathfrak{q}$ a fixed prime; then there is a β in k such that*

$$1 \leqq \|\beta\mathfrak{a}\|_{\mathfrak{p}} \leqq N\mathfrak{q}/C \quad \textit{for} \quad \mathfrak{p} \neq \mathfrak{q};$$
$$(C/N\mathfrak{q})V(\mathfrak{a}) \leqq \|\beta\mathfrak{a}\|_{\mathfrak{q}} \leqq V(\mathfrak{a}).$$

For an archimedean prime $\mathfrak{q}$ we mean by $N\mathfrak{q}$ the number 1. C is the constant of the preceding corollary.

PROOF. If we replace in $\mathfrak{a}$ the component $\alpha_\mathfrak{q}$ by a suitable $\alpha_\mathfrak{q}'$ and leave all other components unchanged we can achieve that the new idèle $\mathfrak{a}'$ satisfies

$$1/C \leqq V(\mathfrak{a}') \leqq N\mathfrak{q}/C.$$

Then we determine the β of our corollary and get

$$1 \leqq \|\beta\mathfrak{a}\|_\mathfrak{p} \leqq V(\mathfrak{a}') \leqq N\mathfrak{q}/C \quad \text{for} \quad \mathfrak{p} \neq \mathfrak{q}$$

and

$$1 \leqq \|\beta\mathfrak{a}'\|_\mathfrak{q} \leqq V(\mathfrak{a}').$$

Now

$$\|\beta\mathfrak{a}\|_\mathfrak{q} = \frac{V(\beta\mathfrak{a})}{V(\beta\mathfrak{a}')} \cdot \|\beta\mathfrak{a}'\|_\mathfrak{q} = \frac{V(\mathfrak{a})}{V(\mathfrak{a}')} \|\beta\mathfrak{a}'\|_\mathfrak{q}.$$

Hence

$$(C/N\mathfrak{q})V(\mathfrak{a}) \leqq V(\mathfrak{a})/V(\mathfrak{a}') \leqq \|\beta\mathfrak{a}\|_\mathfrak{q} \leqq V(\mathfrak{a}).$$

Let now U be the multiplicative group of all absolute units, that is, the set of all ζ of k satisfying $\|\zeta\|_\mathfrak{p} = 1$ for all $\mathfrak{p}$. In case there is a constant field k_0, our group consists of the elements not equal to 0 of k_0. In case order means number of elements, U must be a finite group since it is contained in the parallelotope of size 1; so U consists in this case of all roots of unity of k and is a finite cyclic group.

We select a finite non-empty set S of primes $\mathfrak{p}$ that contains at least all archimedean primes. By $\mathfrak{a}_S$ we mean the idèles satisfying $\|\mathfrak{a}_S\|_\mathfrak{p} = 1$ for all $\mathfrak{p}$ not in S. An element ϵ_S of k that belongs to $\mathfrak{a}_S$ is called an S-unit.

Let $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_s$ be the primes of S. If ϵ_S is an S-unit and we know the s positive numbers $\|\epsilon_S\|_{\mathfrak{p}_1}, \|\epsilon_S\|_{\mathfrak{p}_2}, \cdots, \|\epsilon_S\|_{\mathfrak{p}_s}$, then we know $\|\epsilon_S\|_\mathfrak{p}$ for all $\mathfrak{p}$, so $\|\epsilon_S\|$ is known except for a factor in U. Let us call two S-units equivalent if they differ only by a factor in U. The product formula gives

$$\prod_{\nu=1}^{s} \|\epsilon_S\|_{\mathfrak{p}_\nu} = 1$$

and shows that it suffices to know the $s-1$ numbers $\|\epsilon_S\|_{\mathfrak{p}_1}, \|\epsilon_S\|_{\mathfrak{p}_2}, \cdots, \|\epsilon_S\|_{\mathfrak{p}_{s-1}}$. (Should $s=1$ then ϵ_S is already in U as the product formula shows.)

It is more convenient to take the logarithms of our numbers so we map the unit ϵ_S onto the following vector $v(\epsilon_S)$ of an ordinary space R_{s-1} of $s-1$ dimensions:

$$v(\epsilon_S) = (\log \|\epsilon_S\|_{\mathfrak{p}_1}, \log \|\epsilon_S\|_{\mathfrak{p}_2}, \cdots, \log \|\epsilon_S\|_{\mathfrak{p}_{s-1}}).$$

We have then for two units ϵ_S and η_S the relation

$$v(\epsilon_S\eta_S) = v(\epsilon_S) + v(\eta_S).$$

So the maps $v(\epsilon_S)$ form an additive group of vectors in R_{s-1}.

The product formula gives

$$\log \|\epsilon_S\|_{\mathfrak{p}_s} = -\sum_{\nu=1}^{s-1} \log \|\epsilon_S\|_{\mathfrak{p}_\nu}.$$

Let us consider a bounded region in R_{s-1} that gives bounds for $\log \|\epsilon_S\|_{\mathfrak{p}_\nu}$ $(\nu = 1, 2, \cdots, s-1)$, say

$$-K \leqq \log \|\epsilon_S\|_{\mathfrak{p}_\nu} \leqq K \quad (\nu = 1, 2, \cdots, s-1).$$

Then we get for $\log \|\epsilon_S\|_{\mathfrak{p}_s}$ the bounds $-(s-1)K \leqq \log \|\epsilon_S\|_{\mathfrak{p}_s} \leqq (s-1)K$.

In case all the $\mathfrak{p}_\nu$ of S are discrete this gives only a finite number of possibilities for the ordinal number at each $\mathfrak{p}_\nu$; hence only a finite number of units inequivalent mod U. If there are archimedean primes in S then all ϵ_S of our region are contained in a parallelotope, so their order is finite. But order means number in this case. So we have proved:

LEMMA 12. *There are only a finite number of vectors $v(\epsilon_S)$ in a bounded region of R_{s-1}.*

The following lemma is well known; we repeat its proof here for the convenience of the reader.

LEMMA 13. *Let G be an additive group of vectors in an ordinary euclidean n-space R_n, such that no bounded region of R_n contains an infinite number of vectors of G. Assume that we can find m but not more vectors of G that are linearly independent with respect to real numbers. Then these m vectors may be selected in such a fashion that any vector of G is a linear combination of them with integral coefficients. In other words: G is a lattice of dimension m.*

PROOF. The proof is by induction according to m.

Let $v_1, v_2, \cdots, v_m$ be a maximal set of independent vectors and G_0 be the subgroup of G contained in the subspace spanned by the vectors $v_1, v_2, \cdots, v_{m-1}$. Because of induction we may already assume that any vector in G_0 is a linear integral combination of $v_1, v_2, \cdots, v_{m-1}$.

Consider the subset $\mathfrak{S}$ of all v of G of the form

$$v = x_1v_1 + x_2v_2 + \cdots + x_{m-1}v_{m-1} + x_mv_m$$

with real coefficients $x_1, x_2, \cdots, x_m$ that satisfy

$$0 \leqq x_i < 1 \qquad \text{for } i = 1, 2, \cdots, m-1$$

and

$$0 \leqq x_m \leqq 1.$$

It is a bounded set. Let v_m' be a vector of S with the smallest possible $x_m \neq 0$, say

$$v_m' = \xi_1 v_1 + \xi_2 v_2 + \cdots + \xi_m v_m.$$

Starting now with any vector v of G we can select integral coefficients $y_1, y_2, \cdots, y_m$ in such a way that

$$v' = v - y_m v_m' - y_1 v_1 - y_2 v_2 - \cdots - y_{m-1} v_{m-1}$$

is in $\mathfrak{S}$ and the coefficient of v_m is even less than ξ_m. So this coefficient of v_m is 0, that is, v' is in G_0. So v' is an integral linear combination of $v_1, v_2, \cdots, v_{m-1}$ and therefore v is an integral linear combination of $v_1, v_2, \cdots, v_{m-1}$ and v_m'.

THEOREM 5. *The vectors $v(\epsilon_S)$ form a lattice of at most $s-1$ dimensions. The ϵ_S themselves form* mod *U a free abelian group with at most $s-1$ generators.*

5. **A more restrictive axiom.** If we wish to derive stronger theorems as for instance that of the existence of enough units, we must replace Axiom 2 by a stronger axiom. So we assume from now on that we have in k besides Axiom 1 also

AXIOM 2a. *There is at least one prime in $\mathfrak{M}$ that is either archimedean, with the real field or the complex field as its completed field, or else discrete with residue class field having only a finite number of elements.*

Since Axiom 2 is a consequence of Axiom 2a we can assume all the results we derived thus far and thus we see that k is either a number field or else a function-field where k_0 has only a finite number of elements. We see immediately that Axiom 2a holds for all primes of $\mathfrak{M}$.

LEMMA 14. *To any integer M there are only a finite number of primes $\mathfrak{p}$ with $N\mathfrak{p} \leqq M$.*

PROOF. Since there are only a finite number of archimedean primes we are concerned only with the nonarchimedean ones. Consider $M+1$ integers α_ν of R and let $\mathfrak{p}$ be a prime with $N\mathfrak{p} \leqq M$. Two α_i are in the same residue class, say α_1 and α_2; hence $|\alpha_1 - \alpha_2|_\mathfrak{p} < 1$. So our $\mathfrak{p}$'s are contained among the primes for which one of the differences $\alpha_i - \alpha_k$ $(i \neq k)$ has an absolute value $|\alpha_i - \alpha_k|_\mathfrak{p} < 1$. Because of Axiom 1 our lemma holds.

Now let S be again a finite and non-empty set of primes.

LEMMA 15. *There is a constant E such that to any idèle $\mathfrak{a}_S$ and any prime $\mathfrak{q}$ of S we can find an S-unit ϵ_S such that*

$$\|\epsilon_S \mathfrak{a}_S\|_{\mathfrak{p}} \leqq E \quad \textit{for all } \mathfrak{p} \neq \mathfrak{q} \textit{ of } S.$$

PROOF. Select β according to Lemma 11. Then $1 \leqq \|\beta \mathfrak{a}_S\|_{\mathfrak{p}} \leqq N\mathfrak{q}/C$ for $\mathfrak{p} \neq \mathfrak{q}$. So

$$1 \leqq \|\beta\|_{\mathfrak{p}} \leqq N\mathfrak{q}/C \quad \text{for all } \mathfrak{p} \text{ not in } S.$$

If $\|\beta\|_{\mathfrak{p}} \neq 1$, then $\|\beta\|_{\mathfrak{p}} \geqq N\mathfrak{p}$. Since there are only a finite number $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_l$ of primes with $N\mathfrak{p}_i \leqq N\mathfrak{q}/C$ we get $\|\beta\|_{\mathfrak{p}} = 1$ for all $\mathfrak{p} \neq \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_l$ and $\mathfrak{p}$ not in S. Since $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_l$ are discrete we get only a finite number of possibilities for each $\|\beta\|_{\mathfrak{p}_i}$.

Assume that $\beta_1, \beta_2, \cdots, \beta_r$ already realize any possible distribution of values for $\|\beta\|_{\mathfrak{p}_i}$. Then to any of our β there is a β_k with $\|\beta\|_{\mathfrak{p}} = \|\beta_k\|_{\mathfrak{p}}$ for all $\mathfrak{p}$ not in S, or $\beta = \beta_k \epsilon_S$. Substituting back we get

$$\|\beta_k \epsilon_S \mathfrak{a}_S\|_{\mathfrak{p}} \leqq N\mathfrak{q}/C \quad \text{for} \quad \mathfrak{p} \neq \mathfrak{q}.$$

So $\|\epsilon_S \mathfrak{a}_S\|_{\mathfrak{p}} \leqq E$ for all $\mathfrak{p} \neq \mathfrak{q}$ of S where

$$E = \max_{\nu=1,2,\cdots,r;\ \mathfrak{p} \in S} \left(\frac{N\mathfrak{q}}{C\|\beta_\nu\|_{\mathfrak{p}}} \right).$$

Now select an $\mathfrak{a}_S$ so that $\|\mathfrak{a}_S\|_{\mathfrak{p}} > E$ for all $\mathfrak{p}$ of S. If ϵ_S is the corresponding unit then $\|\epsilon_S\|_{\mathfrak{p}} < 1$ for all $\mathfrak{p} \neq \mathfrak{q}$ of S.

Assume now that $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_s$ are all the primes in S. Then $\mathfrak{q}$ could be any of the primes $\mathfrak{p}_i$. We get in this fashion s S-units $\epsilon_1, \epsilon_2, \cdots, \epsilon_s$, where ϵ_i satisfies $\|\epsilon_i\|_{\mathfrak{p}_k} < 1$ for $k \neq i$. Because of the product formula we also get

$$\|\epsilon_i\|_{\mathfrak{p}_i} > 1.$$

The first $s-1$ of these S-units are mapped onto vectors

$$v_i = (a_{i1}, a_{i2}, \cdots, a_{i,s-1}), \qquad i = 1, 2, \cdots, s-1,$$

where $a_{ik} = \log \|\epsilon_i\|_{\mathfrak{p}_k}$. Then $a_{ii} > 0$ and $a_{ik} < 0$ for $i \neq k$, but $\sum_{\nu=1}^{s-1} a_{i\nu} = \sum_{\nu=1}^{s-1} \log \|\epsilon_i\|_{\mathfrak{p}_\nu} = -\log \|\epsilon_i\|_{\mathfrak{p}_s} > 0$.

We prove now that the vectors v_i are linearly independent, that is, that the homogeneous equations

$$\sum_{\nu=1}^{s-1} x_\nu a_{\nu k} = 0, \qquad k = 1, 2, \cdots, s-1,$$

have only the trivial solution. To that effect it suffices to show that the homogeneous equations

$$\sum_{\nu=1}^{s-1} a_{i\nu}y_\nu = 0, \qquad i = 1, 2, \cdots, s-1,$$

have only the trivial solution.

Assume indeed that $y_1, y_2, \cdots, y_{s-1}$ is a non-trivial solution and that y_i has the greatest absolute value. It is no restriction to assume $y_i > 0$ so that $y_i \geqq y_j$ for all $j \neq i$. Since $a_{ij} < 0$ we get $a_{ij}y_i \leqq a_{ij}y_j$. Now

$$\begin{aligned} a_{i1}y_1 + a_{i2}y_2 + \cdots + a_{in}y_n &\geqq a_{i1}y_i + a_{i2}y_i + \cdots + a_{in}y_i \\ &\geqq (a_{i1} + a_{i2} + \cdots + a_{in})y_i. \end{aligned}$$

The left side of the inequality should be 0 but on the right side both factors are positive.

This proves:

THEOREM 6 (UNIT THEOREM).[6] *If Axioms* 1 *and* 2a *hold then the dimension mentioned in Theorem* 5 *is precisely* $s-1$, *so the S-units form* mod *U a free abelian group with* $s-1$ *generators.*

Another consequence of Axiom 2a is the following: If we go back to Lemma 11 and select in it for $\mathfrak{q}$ one of the primes of S then the inequalities show just as in the proof of Lemma 15 that $\|\beta\mathfrak{a}\|_\mathfrak{p} = 1$ for all $\mathfrak{p}$ with $N\mathfrak{p} > N\mathfrak{q}/C$ and that outside of S there are only a finite number of possibilities for the value distribution of $\|\beta\mathfrak{a}\|_\mathfrak{p}$. Assume that the idèles $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_m$ realize any possible case; then there is always an i such that $\|\beta\mathfrak{a}\|_\mathfrak{p} = \|\mathfrak{a}_i\|_\mathfrak{p}$ for all p not in S or $\beta\mathfrak{a} = \mathfrak{a}_i \cdot \mathfrak{a}_S$. This proves:

THEOREM 7 (FINITENESS OF CLASS NUMBER). *There is a finite set of idèles* $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_m$ *such that any idèle* $\mathfrak{a}$ *is of the form*

$$\mathfrak{a} = \alpha\mathfrak{a}_i\mathfrak{a}_S$$

for a suitable i, $\alpha \in k$ *and* $\mathfrak{a}_S$.

We mention the special case, important for class field theory:

THEOREM 8. *If the set S is big enough then* $\mathfrak{a} = \alpha\mathfrak{a}_S$ *for all idèles* $\mathfrak{a}$.

PROOF. Add to the previous set S also the primes $\mathfrak{p}$ where any $\|\mathfrak{a}_i\|_\mathfrak{p} \neq 1$.

---

[6] The unit theorem in this form is due to Hasse. It is proved by Chevalley in [4].

References

1. E. Artin, *Über die Bewertungen algebraischer Zahlkörper*, Journal für Mathematik vol. 167 (1932) pp. 157–159.

2. C. Chevalley, *Sur la théorie du corps de classes dans les corps finis et les corps locaux*, Journal of College of Sciences, Tokyo, 1933, II, part 9.

3. ———, *Généralization de la théorie de corps de classes pour les extensions infinies*, Journal de mathématiques pures et appliquées (9) vol. 15 (1936) pp. 359–371.

4. ———, *La théorie du corps de classes*, Ann. of Math. vol. 41 (1940) pp. 394–418.

5. A. Ostrowski, *Über einige Lösungen der Funktionalgleichung* $\phi(x)\phi(y) = \phi(xy)$, Acta Math. vol. 41 (1918) pp. 271–284.

6. ———, *Untersuchung in der arithmetische Theorie der Körper*, Parts I, II, and III, Math. Zeit. 39 (1935) pp. 269–321.

7. B. L. van der Waerden, *Moderne Algebra*, vol. 1, 2d ed., Berlin, 1937.

8. G. Whaples, *Non-analytic class field theory and Grunwald's theorem*, Duke Math. J. vol. 9 (1942) pp. 455–473.

Indiana University and
University of Pennsylvania