VI. Reinterpretation with Adeles and Ideles, 313-402

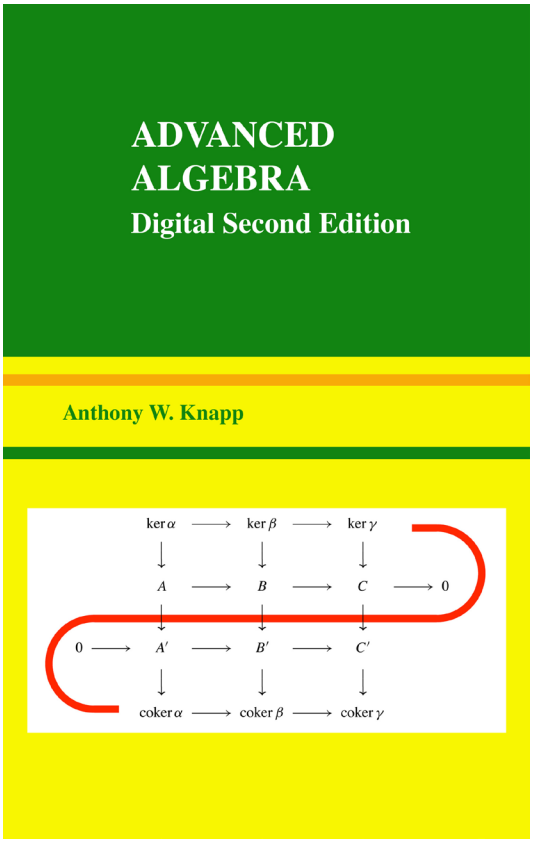
DOI: 10.3792/euclid/9781429799928-6

from

Advanced Algebra
Digital Second Edition

Anthony W. Knapp

Full Book DOI: 10.3792/euclid/9781429799928
ISBN: 978-1-4297-9992-8



Anthony W. Knapp
81 Upper Sheep Pasture Road
East Setauket, N.Y. 11733–1729, U.S.A.
Email to: aknapp@math.stonybrook.edu
Homepage: www.math.stonybrook.edu/~aknapp

Title: Advanced Algebra
Cover: Content of the Snake Lemma; see page 185.

Mathematics Subject Classification (2010): 11–01, 13–01, 14–01, 16–01, 18G99, 55U99, 11R04, 11S15, 12F99, 14A05, 14H05, 12Y05, 14A10, 14Q99.

First Edition, ISBN-13 978-0-8176-4522-9

Published by Birkhäuser Boston

Digital Second Edition, not to be sold, no ISBN

Published by the Author

CHAPTER VI

Reinterpretation with Adeles and Ideles

Abstract. This chapter develops tools for a more penetrating study of algebraic number theory than was possible in Chapter V and concludes by formulating two of the main three theorems of Chapter V in the modern setting of "adeles" and "ideles" commonly used in the subject.

Sections 1–5 introduce discrete valuations, absolute values, and completions for fields, always paying attention to implications for number fields and for certain kinds of function fields. Section 1 contains a prototype for all these notions in the construction of the field $\mathbb{Q}_p$ of p-adic numbers formed out of the rationals. Discrete valuations in Section 2 are a generalization of the order-of-vanishing function about a point in the theory of one complex variable. Absolute values in Section 3 are real-valued multiplicative functions that give a metric on a field, and the pair consisting of a field and an absolute value is called a valued field. Inequivalent absolute values have a certain independence property that is captured by the Weak Approximation Theorem. Completions in Section 4 are functions mapping valued fields into their metric-space completions. Section 5 concerns Hensel's Lemma, which in its simplest form allows one to lift roots of polynomials over finite prime fields $\mathbb{F}_p$ to roots of corresponding polynomials over p-adic fields $\mathbb{Q}_p$.

Section 6 contains the main theorem for investigating the fundamental question of how prime ideals split in extensions. Let K be a finite separable extension of a field F, let R be a Dedekind domain with field of fractions F, and let T be the integral closure of R in K. The question concerns the factorization of an ideal $\mathfrak{p}T$ in T when $\mathfrak{p}$ is a nonzero prime ideal in R. If $F_{\mathfrak{p}}$ denotes the completion of F with respect to $\mathfrak{p}$, the theorem explains how the tensor product $K \otimes_F F_{\mathfrak{p}}$ splits uniquely as a direct sum of completions of valued fields. The theorem in effect reduces the question of the splitting of $\mathfrak{p}T$ in T to the splitting of $F_{\mathfrak{p}}$ in a complete field in which only one of the prime factors of $\mathfrak{p}T$ plays a role.

Section 7 is a brief aside mentioning additional conclusions one can draw when the extension K/F is a Galois extension.

Section 8 applies the main theorem of Section 6 to an analysis of the different of K/F and ultimately to the absolute discriminant of a number field. With the new sharp tools developed in the present chapter, including a Strong Approximation Theorem that is proved in Section 8, a complete proof is given for the Dedekind Discriminant Theorem; only a partial proof had been accessible in Chapter V.

Sections 9–10 specialize to the case of number fields and to function fields that are finite separable extensions of $\mathbb{F}_q(X)$, where $\mathbb{F}_q$ is a finite field. The adele ring and the idele group are introduced for each of these kinds of fields, and it is shown how the original field embeds discretely in the adeles and how the multiplicative group embeds discretely in the ideles. The main theorems are compactness theorems about the quotient of the adeles by the embedded field and about the quotient of the normalized ideles by the embedded multiplicative group. Proofs are given only for number fields. In the first case the compactness encodes the Strong Approximation Theorem of Section 8 and the Artin product formula of Section 9. In the second case the compactness encodes both the finiteness of the class number and the Dirichlet Unit Theorem.

1. p-adic Numbers

This chapter will sharpen some of the number-theoretic techniques used in Chapter V, finally arriving at the setting of "adeles" and "ideles" in which many of the more recent results in number theory have tidy formulations. Although Chapter V dealt only with number fields, the present chapter will allow a greater degree of generality that includes results in the algebraic geometry of curves. This greater degree of generality will not require much extra effort, and it will allow us to use each of the subjects of number theory and algebraic geometry to motivate the other.

The first section of Chapter V returned to the idea that one can get some information about the integer solutions of a Diophantine equation by considering the equation as a system of congruences modulo each prime number. However, we lose information by considering only primes for the modulus, and this fact lies behind the failure of Chapter V to give a complete proof of the Dedekind Discriminant Theorem (Theorem 5.5). The proof that we did give was of a related result, Kummer's criterion (Theorem 5.6), which concerns a field $\mathbb{Q}(\xi)$, where ξ is a root of an irreducible monic polynomial $F(X)$ in $\mathbb{Z}[X]$. The statement of Theorem 5.6 involves the reduction of $F(X)$ modulo certain prime numbers p and no other congruences.

The Chinese Remainder Theorem tells us that a congruence modulo any integer can be solved by means of congruences modulo prime powers, and the formulation of Theorem 5.6 uses only congruences modulo primes raised to the first power. Let us strip away the complicated setting from such congruences and see some examples of how the use of prime powers can make a difference.

EXAMPLES.

(1) Consider the problem of finding a square root of 5 modulo powers of 2. For the first power, we have

$$x^2 - 5 = (x-1)^2 + 2x - 6 \equiv (x-1)^2 \bmod 2,$$

i.e., $x^2 - 5$ is the square of a linear factor modulo 2. For the second power, the computation is

$$x^2 - 5 = (x-1)(x+1) - 4 \equiv (x-1)(x+1) \bmod 4,$$

and $x^2 - 5$ is the product of two distinct linear factors modulo 4. For the third power, $x^2 - 5$ is irreducible modulo 8 because the only odd squares modulo 8 are ± 1. Thus the polynomial $x^2 - 5$ exhibits a third kind of behavior when considered modulo 8. For higher powers of 2, the irreducibility persists because a nontrivial factorization modulo 2^k with $k > 3$ would imply a nontrivial factorization modulo 8.

(2) Consider the problem of finding a square root of 17 modulo powers of 2. We readily compute that

$$\begin{aligned}
x^2 - 17 &= (x-1)^2 + 2x - 18 \equiv (x-1)^2 \bmod 2,\\
x^2 - 17 &= (x-1)(x+1) - 16 \equiv (x-1)(x+1) \bmod 4,\\
x^2 - 17 &= (x-1)(x+1) - 16 \equiv (x-1)(x+1) \bmod 8,\\
x^2 - 17 &= (x-1)(x+1) - 16 \equiv (x-1)(x+1) \bmod 16,\\
x^2 - 17 &= (x-7)(x+7) + 32 \equiv (x-7)(x+7) \bmod 32,\\
x^2 - 17 &= (x-9)(x+9) + 64 \equiv (x-9)(x+9) \bmod 64,
\end{aligned}$$

i.e., that the factorization of $x^2 - 17$ begins in the same way as for $x^2 - 5$ but that $x^2 - 17$ continues to factor as the product of two distinct linear factors modulo 2^3, 2^4, 2^5, and 2^6. We can argue inductively that this pattern persists through all higher powers. In fact, suppose that $x^2 - 17 = (x - m)(x + m) \bmod 2^k$ for an integer $k \geq 3$. Then

$$x^2 - 17 = x^2 - m^2 + a2^k,$$

and m must be odd. Then we can write

$$x^2 - 17 = x^2 - (m - a2^{k-1})^2 + a2^k(1 - m + a2^{k-2}).$$

The factor $(1 - m + a2^{k-2})$ is even, and this equality shows that $x^2 - 17$ is the product of two distinct linear factors modulo 2^{k+1}. This completes the induction.

One immediate observation from the two examples is that the factorizations of $x^2 - 5$ and $x^2 - 17$ are the same modulo 2 and modulo 2^2 but are qualitatively distinct modulo higher powers of 2. Another observation is the nature of the data produced by the inductive argument in Example 2: For each k, we obtain an odd integer m_k such that $m_k^2 \equiv 17 \bmod 2^k$, and the m_k's are constructed in such a way that $m_{k+1} = m_k - a_k 2^{k-1}$ if $m_k^2 = 17 + a_k 2^k$. It follows that if $l \geq k$, then $m_k - m_l$ is divisible by 2^{k-1}, i.e., by higher and higher powers of 2 as k increases.

A first conclusion is that we get additional information by using congruences modulo prime powers. A second and more subtle conclusion is that it would be desirable to regard the sequence $\{m_k\}$ as stabilizing in some sense; then we could regard the system of congruences modulo all powers 2^k as having a single pair of solutions that we can consider as square roots of 17. In this case we would not have to think about infinitely many solutions to infinitely many unrelated congruences.

The construction that is to follow in this section, which is due to K. Hensel, will capture this information as a single "2-adic number." Conversely the 2-adic number carries with it the congruence information modulo 2^k for all positive integers k.

Thus the revised method of considering congruences prime by prime will be a two-step process, first a step of "localization" and then a step of "completion." In our application in Chapter V, we did not explicitly make use of localization in the sense of Chapter VIII of *Basic Algebra*, but it was there implicitly—in Proposition 5.2 for example and in the proof of Theorem 5.6. Carrying out the details of setting up the theory behind the two-stage process will take some work and will occupy the first four sections of this chapter. Let us get started.

Let p be a prime number. We define a real-valued function $|\cdot|_p$ on the field $\mathbb{Q}$ of rationals as follows: we take $|0|_p = 0$, and for any rational $r = p^m ab^{-1}$ with a and b equal to integers relatively prime to p, we define $|r|_p = p^{-m}$. The function $|\cdot|_p$ is called the **p-adic absolute value** on $\mathbb{Q}$. It has the following properties:

(i) $|x|_p \geq 0$ with equality if and only if $x = 0$,
(ii) $|x + y|_p \leq \max(|x|_p, |y|_p)$,
(iii) $|xy|_p = |x|_p |y|_p$,
(iv) $|-1|_p = |1|_p = 1$, and
(v) $|-x|_p = |x|_p$.

In fact, with (ii), equality holds if $|x|_p \neq |y|_p$, and the case with $|x|_p = |y|_p$ comes down to the observation that $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ has no factor of p in its denominator if b and d are relatively prime to p. Property (iii) comes down to the fact that if a, b, c, d are relatively prime to p, then so are ac and bd. The other properties follow from the first three: To see that $|1|_p = 1$ in (iv), we observe from (iii) that $|1|_p$ is a nonzero solution of $x^2 = x$ and thus has to be 1. This conclusion and (iii) together show that $|-1|_p$ is a positive solution of $x^2 = 1$ and thus has to be 1. Property (v) follows immediately by combining (iii) and (iv).

Inequality (ii) is called the **ultrametric inequality**. It implies that $|x + y|_p \leq |x|_p + |y|_p$, and consequently the function $d(x, y) = |x - y|_p$ satisfies the triangle inequality

$$d(x, y) \leq d(x, z) + d(z, y).$$

Since (i) shows that $d(x, y) \geq 0$ with equality exactly when $x = y$ and since (v) implies that $d(x, y) = |x - y|_p = d(y, x)$, the function d on $\mathbb{Q} \times \mathbb{Q}$ is a metric. It is called the **p-adic metric** on $\mathbb{Q}$.

The field $\mathbb{Q}_p$ of **p-adic numbers** will be obtained by completing this metric and extending the field operations to the completion. Let us see to the details. Regard the space $\prod_{j=1}^{\infty} \mathbb{Q}$ of sequences $\{q_j\}_{j=1}^{\infty}$ of rational numbers as the direct product of copies of the ring $\mathbb{Q}$, the operations being taken coordinate by coordinate. Then $\prod_{j=1}^{\infty} \mathbb{Q}$ is a commutative ring with identity, the identity being the sequence whose terms are all equal to 1.

As is usual for metric spaces, we say that a sequence of rationals, i.e., a member $\{q_j\}$ of $\prod_{j=1}^{\infty}\mathbb{Q}$, is **convergent** to $q \in \mathbb{Q}$ in the p-adic metric if for any real $\epsilon > 0$, there exists an integer N such that $|q_n - q|_p < \epsilon$ for all $n \geq N$. Convergence in this metric is quite different from what one might expect; for example the sequence $\{2^j\}_{j=1}^{\infty}$ is convergent to 0 when $p = 2$. The sequence $\{q_j\}$ is a **Cauchy sequence** in the p-adic metric if for any real $\epsilon > 0$, there exists an integer N such that $|q_m - q_n|_p < \epsilon$ for all $m \geq N$ and all $n \geq N$. Convergent sequences are Cauchy, as follows from the inequality $|q_m - q_n|_p \leq |q_m - q|_p + |q - q_n|_p$. Cauchy sequences need not be convergent, but every Cauchy sequence $\{q_n\}$ is **bounded** in the sense that there is some real C with $|q_n|_p \leq C$ for all n.

EXAMPLE 2, CONTINUED. We obtained a sequence $\{m_k\}$ of odd integers such that $l \geq k$ implies that $m_k - m_l$ is divisible by 2^{k-1} and $m_k^2 - 17$ is divisible by 2^k. In terms of the 2-adic absolute value, $|m_k - m_l|_p \leq 2^{-(k-1)}$ and $|m_k^2 - 17|_p \leq 2^{-k}$. The sequence $\{m_k\}$ is therefore a Cauchy sequence in the 2-adic metric, and the sequence $\{m_k^2\}$ is convergent in the 2-adic metric to 17.

It follows from the ultrametric inequality that the sum and difference of Cauchy sequences is bounded, and (ii) and the boundedness of Cauchy sequences implies that the product of two Cauchy sequences is Cauchy. Therefore the subset $\mathcal{R}$ of Cauchy sequences is a subring with identity within $\prod_{j=1}^{\infty}\mathbb{Q}$.

In the theory of metric spaces, one defines a suitable notion of equivalence of Cauchy sequences, and the set of equivalence classes becomes a complete metric space,[1] any member q of $\mathbb{Q}$ being identified with the constant Cauchy sequence whose terms all equal q. With the p-adic metric, one can then prove that the field operations extend to the completion, and the completion is the field of p-adic numbers. This verification is a little tedious when done directly, and we can proceed more expeditiously by using some elementary ring theory.

Since convergent sequences are Cauchy, the set $\mathcal{I}$ of sequences convergent to 0 is a subset of the ring $\mathcal{R}$. The sum or difference of two such sequences is again convergent to 0, and $\mathcal{I}$ is an additive subgroup. We shall show that $\mathcal{I}$ is in fact an ideal in $\mathcal{R}$. Thus let $\{z_n\}$ be convergent to 0, and let $\{q_n\}$ be Cauchy. Since $\{q_n\}$ is Cauchy, it is bounded, say with $|q_n|_p \leq M$ for all n. If $\epsilon > 0$ is given, choose N such that $n \geq N$ implies $|z_n|_p \leq \epsilon/M$. Then $n \geq N$ implies that $|z_n q_n|_p = |z_n|_p |q_n|_p \leq (\epsilon/M)M = \epsilon$. Hence $\{z_n q_n\}$ is convergent to 0, and $\mathcal{I}$ is an ideal in $\mathcal{R}$.

Proposition 6.1. With the p-adic absolute value imposed on $\mathbb{Q}$, let $\mathcal{R}$ be the subring of $\prod_{j=1}^{\infty}\mathbb{Q}$ consisting of all Cauchy sequences, and let $\mathcal{I}$ be the ideal in

[1] This construction is carried out in detail in Section II.11 of the author's *Basic Real Analysis.*

$\mathcal{R}$ consisting of all sequences convergent to 0. Then $\mathcal{I}$ is a maximal ideal in $\mathcal{R}$, and the quotient $\mathcal{R}/\mathcal{I}$ is a field. Consequently the Cauchy completion of $\mathbb{Q}$ in the p-adic metric is a topological field $\mathbb{Q}_p$ into which $\mathbb{Q}$ embeds via a field mapping. If $|\cdot|_p$ denotes the function $d(\cdot, 0)$ on $\mathbb{Q}_p$, then $|\cdot|_p$ is a continuous extension of the p-adic absolute value from $\mathbb{Q}$ to $\mathbb{Q}_p$, and it satisfies

(a) $|x|_p \geq 0$ with equality if and only if $x = 0$,
(b) $|x + y|_p \leq \max(|x|_p, |y|_p)$, and
(c) $|xy|_p = |x|_p |y|_p$.

The subset $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$ is an open closed subring of $\mathbb{Q}_p$ in which $\mathbb{Z}$ is dense, and $\mathbb{Z}_p$ is compact. Consequently the topological field $\mathbb{Q}_p$ is locally compact.

REMARKS. The field $\mathbb{Q}_p$ is called the field of **p-adic numbers**, and the ring $\mathbb{Z}_p$ is called the ring of **p-adic integers**. The ring $\mathbb{Z}_p$ contains the identity of $\mathbb{Q}_p$.

PROOF. First let us prove that $\mathcal{I}$ is a maximal ideal. Arguing by contradiction, let $\{q_n\}$ be a Cauchy sequence that is not in $\mathcal{I}$, i.e., is not convergent to 0. Then there exists an $\epsilon_0 > 0$ such that $|q_n|_p \geq \epsilon_0$ for infinitely many n. Choose N such that $|q_n - q_m| < \epsilon_0/2$ whenever $n \geq N$ and $m \geq N$, and find some $n_0 \geq N$ with $|q_{n_0}|_p \geq \epsilon_0$. Then $n \geq N$ implies that $|q_n|_p \geq \epsilon_0/2$ because otherwise we would have $\epsilon_0 \leq |q_{n_0}|_p \leq |q_n - q_{n_0}|_p + |q_n|_p < \epsilon_0/2 + \epsilon_0/2 = \epsilon_0$, contradiction. Let $\{r_n\}$ be the sequence with $r_n = 0$ for $n < N$ and $r_n = q_n^{-1}$ for $n \geq N$. For $n \geq N$ and $m \geq N$, we have

$$\begin{aligned} |r_n - r_m|_p &= |q_n^{-1} - q_m^{-1}|_p = |(q_m - q_n)/(q_m q_n)|_p \\ &= |q_m - q_n|_p |q_m|_p^{-1} |q_n|_p^{-1} \leq 4\epsilon_0^{-2} |q_m - q_n|_p, \end{aligned}$$

and it follows that $\{r_n\}_p$ is Cauchy and hence lies in $\mathcal{R}$. Since $\mathcal{I}$ is an ideal in $\mathcal{R}$, $\{r_n q_n\}$ is Cauchy. The terms of the sequence $\{r_n q_n\}$ are all equal to 1 for $n \geq N$, and hence $\{r_n q_n\}$ differs from the identity of $\mathcal{R}$ by a member of $\mathcal{I}$. Consequently the identity is in $\mathcal{I}$. This is a contradiction, since the members of the constant sequence $\{1\}$ are at distance $|1 - 0|_p = 1$ from 0. Hence $\mathcal{I}$ is a maximal ideal, and $\mathcal{R}/\mathcal{I}$ is necessarily a field.

Meanwhile, the Cauchy completion $\mathbb{Q}_p$ of $\mathbb{Q}$ is the set of equivalence classes from $\mathcal{R}$, two members of $\mathcal{R}$ being equivalent if they differ by a sequence convergent to 0. Consequently the Cauchy completion $\mathbb{Q}_p$ is precisely $\mathcal{R}/\mathcal{I}$ as a set. The mapping $\mathbb{Q} \to \mathcal{R} \to \mathcal{R}/\mathcal{I}$ carrying a member q of $\mathbb{Q}$ to the constant sequence $\{q_n\}$ with all $q_n = q$ and then from $\mathcal{R}$ to the quotient $\mathcal{R}/\mathcal{I} = \mathbb{Q}_p$ evidently respects the operations and hence is a field mapping. This mapping identifies $\mathbb{Q}$ with a subset of $\mathbb{Q}_p$. The metric d on $\mathbb{Q}$ extends uniquely to a continuous function on

the completion $\mathbb{Q}_p \times \mathbb{Q}_p$, and therefore the p-adic absolute value $|\cdot|_p = d(\cdot, 0)$ extends to a continuous function on $\mathbb{Q}_p$.

Property (a) for the function $|\cdot|_p$ on $\mathbb{Q}_p$ follows from the fact that the continuous extension of d is a metric on $\mathbb{Q}_p$. To see that (b) and (c) hold on $\mathbb{Q}_p$, let x and y be members of $\mathbb{Q}_p = \mathcal{R}/\mathcal{I}$, and let $\{q_n\}$ and $\{r_n\}$ be respective coset representatives of them in $\mathcal{R}$. Then $\{q_n + r_n\}$ and $\{q_n r_n\}$ are representatives of $x + y$ and xy by definition, and the continuity of the p-adic absolute value on $\mathbb{Q}_p$ implies that $\lim_n |q_n + r_n|_p = |x + y|_p$ and $\lim_n |q_n r_n|_p = |xy|_p$. From the first of these limit formulas and from (b) on $\mathbb{Q}$, we obtain

$$|x + y|_p = \limsup_n |q_n + r_n|_p \le \limsup_n \max(|q_n|_p, |r_n|_p) = \max(|x|_p, |y|_p),$$

since $\lim_n |q_n|_p = |x|_p$ and $\lim_n |r_n|_p = |y|_p$. This proves (b) on $\mathbb{Q}_p$. Similarly

$$|xy|_p = \lim_n |q_n r_n|_p = \lim_n |q_n|_p |r_n|_p = (\lim_n |q_n|_p)(\lim_n |r_n|_p) = |x|_p |y|_p,$$

and this proves (c) on $\mathbb{Q}_p$.

To see that addition, subtraction, and multiplication are continuous on $\mathbb{Q}_p \times \mathbb{Q}_p$, let $\{x_n\}$ and $\{y_n\}$ be convergent sequences in $\mathbb{Q}_p$ with respective limits x and y. Use of (b) on $\mathbb{Q}_p$ gives

$$|(x_n + y_n) - (x + y)|_p = |(x_n - x) + (y_n - y)|_p \le \max(|x_n - x|_p, |y_n - y|_p).$$

The right side has limit 0 in $\mathbb{R}$, and therefore $x_n + y_n$ has limit $x + y$ in $\mathbb{Q}_p$. A completely analogous argument, making use also of the equality $|-1|_p = |1|_p$, shows that subtraction is continuous. Consider multiplication. If M is an upper bound for the absolute values $|x_n|_p$ and $|y_n|_p$, then use of (c) on $\mathbb{Q}_p$ gives

$$\begin{aligned} |x_n y_n - xy|_p &= |x_n(y_n - y) + y(x_n - x)|_p \\ &\le \max(|x_n(y_n - y)|_p, |y(x_n - x)|_p) \\ &= \max(|x_n|_p |y_n - y|_p, |y|_p |x_n - x|_p) \\ &\le \max(M|y_n - y|_p, |y|_p |x_n - x|_p). \end{aligned}$$

The right side has limit 0 in $\mathbb{R}$, and therefore $x_n y_n$ has limit xy in $\mathbb{Q}_p$.

To see that inversion $x \mapsto x^{-1}$ is continuous on $\mathbb{Q}_p^\times$, let $\{x_n\}$ be a sequence in $\mathbb{Q}_p^\times$ with limit x in $\mathbb{Q}_p^\times$. Since $\lim_n |x_n|_p = |x|_p$, we can find an integer N such that $|x_n|_p \ge \frac{1}{2}|x|_p$ for $n \ge N$. The computation

$$|x_n^{-1} - x^{-1}|_p = |(x - x_n)/(x_n x)|_p = |x - x_n|_p / (|x_n|_p |x|_p) \le 2|x|_p^{-1} |x - x_n|_p,$$

valid for $n \geq N$, shows that $\lim x_n^{-1} = x^{-1}$, and inversion is continuous. Consequently $\mathbb{Q}_p$ is a topological field.

It follows immediately from properties (b) and (c) and from the equality $|-x|_p = |x|_p$ that $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$. Since $\mathbb{Z}_p$ is defined in terms of a continuous function and an inequality, it is closed. It can also be defined as the subset with $|x|_p < p$ because the p-adic absolute value takes no values between 1 and p, and therefore $\mathbb{Z}_p$ is open. The most general nonzero member of $\mathbb{Q} \cap \mathbb{Z}_p$ is of the form $q = a/b$, where a and b are relatively prime nonzero integers with $|a/b|_p \leq 1$. Here $|b|_p = 1$, and p cannot divide b. If $k > 0$ is given, then it follows that there exists n with $bn - a \equiv 0 \bmod p^k$. This n has $|n - \frac{a}{b}|_p = |bn - a|_p \leq p^{-k}$. So q is in the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$. In other words, the closure of $\mathbb{Z}$ contains $\mathbb{Q} \cap \mathbb{Z}_p$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.

For each integer $n \geq 0$, the set $\mathbb{Z}_p$ is covered by the closed balls of radius p^{-n} centered at the integers $0, 1, 2, \ldots, p^n - 1$. In fact, every integer z has $z \equiv k \bmod p^n$ for some integer $k \in \{0, 1, 2, \ldots, p^n - 1\}$. For this k, $|z - k|_p \leq p^{-n}$. Thus $\mathbb{Z}$ is contained in the union of the closed balls of radius p^{-n} centered at $0, 1, 2, \ldots, p^n - 1$. This union is closed; since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, $\mathbb{Z}_p$ is contained in this union. In turn, these closed balls are contained in the open balls of radius p^{-n+1} centered at the integers $0, 1, 2, \ldots, p^n - 1$. Thus for any positive radius, there exists a finite collection of open balls of that radius or less such that the union of the open balls covers $\mathbb{Z}_p$. This means that $\mathbb{Z}_p$ is totally bounded in the metric space $\mathbb{Q}_p$. A totally bounded closed subset of a complete metric space is compact, and consequently $\mathbb{Z}_p$ is compact.

Thus the 0 element of $\mathbb{Q}_p$ has $\mathbb{Z}_p$ as a compact neighborhood. Since addition is continuous, $x + \mathbb{Z}_p$ is a compact neighborhood of x, and therefore $\mathbb{Q}_p$ is locally compact. □

2. Discrete Valuations

The construction of the p-adic absolute value on $\mathbb{Q}$ seemingly made use of unique factorization of the members of $\mathbb{Z}$, but actually the unique factorization of the ideals in $\mathbb{Z}$ would have been sufficient. Thus we shall see in a moment that the construction extends to apply to any number field F as soon as we specify a nonzero prime ideal P in the ring R of algebraic integers of F. In fact, there is nothing special about a number field. If R is any Dedekind domain and F is its field of fractions, then the construction extends to F as soon as we specify a nonzero prime ideal P in R.

Before describing the extended construction, let us look at the definition of the p-adic absolute value on $\mathbb{Q}$ more closely. Recall that if $x = p^m a b^{-1}$ for integers a and b relatively prime to p, then $|x|_p = p^{-m}$. Actually, the base p in this exponential is not very important at this point, and we could have used

any real number $r > 1$ in place of p in p^{-m}. With this adjustment the p-adic absolute value would have been given by $|x|_p = r^{-v_p(x)}$, where $v_p(x)$ is the exact net power of p that occurs when the prime factorizations of the numerator and denominator of x are used. The exponent $v_p(x)$ is what is important; the base r is unimportant.

The expression $v_p(x)$ for $\mathbb{Q}$ is analogous to the order of vanishing of a polynomial in one complex variable at a point, and Hensel was led to the p-adic absolute value by carrying the notion for $\mathbb{C}[X]$ to the setting with $\mathbb{Q}$. In setting up a generalization, we shall work first with the generalization of the order of vanishing $v_p(x)$, since it is the more primitive notion, and in Section 3 we shall exponentiate to obtain a generalization of the absolute value for which we can form a completion.

To make the definitions, it is convenient to make use of fractional ideals, which were the subject of a set of problems in Chapter VIII of *Basic Algebra*. Let us recall the definition and the relevant properties. Again let R be a Dedekind domain, and let F be its field of fractions. A **fractional ideal** of F is any finitely generated R module M. For such an R module, there exists some $a \in R$ with $aM \subseteq R$, and then aM is an ideal of R. If M is any nonzero fractional ideal, then $M^{-1} = \{x \in F \mid xM \in R\}$ is a nonzero fractional ideal, and $MM^{-1} = R$. With this definition and property, it readily follows from the unique factorization of ideals in R that any nonzero fractional ideal M of F is of the form

$$M = \prod_{j=1}^{l} P_j^{k_j},$$

for a suitable set $\{P_1, \dots, P_l\}$ of distinct nonzero prime ideals of R and for suitable nonzero integer exponents k_j. This expansion is unique up to the order of the factors, and every such expression is a fractional ideal. It follows that the nonzero fractional ideals form a group under multiplication. At the end of this section, we shall mention how this group is related to the ideal class group of F as defined in Section V.6.

If $x \neq 0$ is in F, then the **principal fractional ideal** $(x) = xR$ has a factorization as above. If P is a nonzero prime ideal of R, we let $v_P(x)$ be the negative of the integer exponent of P in the prime factorization of (x). For example, if x is a nonzero element of R, then $v_P(x)$ is a nonnegative integer. To make $v_P(\cdot)$ be everywhere defined on F, we define $v_P(0) = +\infty$. Then $v_P(\cdot)$ is function from F onto $\mathbb{Z} \cup \{+\infty\}$ such that

(i) $v_P(x) = +\infty$ if and only if $x = 0$,
(ii) $v_P(x + y) \geq \min(v_P(x), v_P(y))$ for all x and y, and
(iii) $v_P(xy) = v_P(x) + v_P(y)$ for all x and y.

We shall see in Proposition 6.4 below that the effect of $v_P(\cdot)$ is to pick out from F the localization of R at P.

To proceed further, we abstract the above construction and see what information we can recover from it. Let F be any field. A **discrete valuation** of F is a function $v(\cdot)$ from F onto $\mathbb{Z} \cup \{\infty\}$ such that

(i) $v(x) = +\infty$ if and only if $x = 0$,
(ii) $v(x + y) \geq \min(v(x), v(y))$ for all x and y, and
(iii) $v(xy) = v(x) + v(y)$ for all x and y.

Observe as a consequence that

(iv) $v(-1) = v(1) = 0$,
(v) $v(-x) = v(x)$ for all x, and
(vi) $v(x + y) = v(x)$ if $v(y) > v(x)$.

In fact, $v(1) = 0$ follows by taking $x = y = 1$ in (iii), and then $v(-1) = 0$ follows by taking $x = y = -1$ in (iii). This proves (iv), and (v) follows by combining (iv) with (iii) for $x = -1$. For (vi), we have $v(x + y) \geq v(x)$ by (ii). In the reverse direction, $v(x) \geq \min(v(x + y), v(y))$ by (ii) and (v); since $v(y) > v(x)$, the minimum must be the first of the two, and thus $v(x) \geq v(x+y)$.

Define $R_v = \{x \in F \mid v(x) \geq 0\}$. Property (i) shows that 0 is in R_v, (ii) and (v) show that R_v is closed under addition and subtraction, (iii) shows that R_v is closed under multiplication, and (iv) shows that 1 is in R_v. Consequently R_v is an integral domain. The ring R_v is called the **valuation ring** of v in F.

If x is in F but is not in R_v, then $v(x) < 0$. This inequality forces $v(x^{-1}) > 0$, and x^{-1} is in R_v. As a consequence, F can be regarded as the field of fractions of R_v.

Let $P_v = \{x \in F \mid v(x) > 0\}$. Arguing in similar fashion, we see that P_v is an ideal in R_v. Any x in R_v that is not in P_v has $v(x) = v(x^{-1}) = 0$ and is thus a unit in R_v. In other words, R_v is a local ring with P_v as its unique maximal ideal. The ideal P_v is called the **valuation ideal** of v in F. We write $\Bbbk_v$ for the field R_v/P_v; it is called the **residue class field** of v.

Proposition 6.2. Let v be a discrete valuation of a field F, let R_v be the valuation ring, and let P_v be the valuation ideal. Then

(a) R_v is a principal ideal domain,
(b) there exists an element π in P_v with $v(\pi) = 1$, and any such π has $P_v = (\pi)$,
(c) the nonzero ideals of R_v are exactly the nonnegative integer powers of P_v and are given by $P_v^n = (\pi^n) = \{x \in R_v \mid v(x) \geq n\}$ for $n \geq 0$,
(d) the nonzero fractional ideals of R_v are exactly the integer powers of P_v and are given by $P_v^n = (\pi^n) = \{x \in R_v \mid v(x) \geq n\}$ for $n \in \mathbb{Z}$.

REMARKS. When F equals $\mathbb{Q}$ and v counts the net power of a prime number p dividing a rational number, we see by inspection that the ring R_v is the localization of $\mathbb{Z}$ at p, consisting of all rational numbers with no factor of p in their

denominators. The choices[2] for π in (b) are the elements rp, where r is any nonzero rational whose numerator and denominator are both prime to p, and the nonzero ideals are of the form (p^n) with $n \geq 0$.

PROOF. The ideal P_v contains an element π with $v(\pi) = 1$ because $v(\cdot)$ is assumed to be onto $\mathbb{Z} \cup \{+\infty\}$. Suppose that x is a nonzero member of P_v and that $v(x) = n > 0$. Then $v(\pi^{-n}x) = 0$, and the elements $\pi^{-n}x$ and $x^{-1}\pi^n$ lie in R_v. Hence $x = \pi^n(\pi^{-n}x)$ exhibits x as a member of (π^n), and $\pi^n = x(x^{-1}\pi^n)$ exhibits π^n as a member of (x). Consequently $(x) = (\pi^n)$. If I is a nonzero proper ideal in R_v, then it follows that $I = \pi^{n_0}R_v$, where n_0 is the smallest integer such that some element x_0 of I has $v(x_0) = n_0$. This proves (a), (b), and (c).

Since R_v is a principal ideal domain, it is a Dedekind domain, and the theory of fractional ideals is applicable. Since (c) shows the nonzero ideals to be all P_v^n with $n \geq 0$, it follows that the fractional ideals are all P_v^n with n an arbitrary integer. For any integer $n > 0$, we have $(\pi^{-n})P_v^n = \pi^{-n}R_v\pi^n R_v = R_v = P_v^{-n}P_v^n$, and thus $P_v^{-n} = (\pi^{-n})$. The latter ideal equals $\pi^{-n}R_v = \{x \in R_v \mid v(x) \geq -n\}$, and this proves (d). □

From property (vi) it follows for $n > 0$ that the members x of the set $1 + P_v^n$ all have $v(x) = 0$. The product of two such elements is again in the set because P_v^n is an ideal. Let us see that the multiplicative inverse x^{-1} of a member x of the set is in the set. We calculate that $v(x^{-1} - 1) = v(x^{-1}) + v(1-x) = 0 + v(1-x) = v(1-x) \geq n$. Hence x^{-1} is in $1 + P_v^n$, and $1 + P_v^n$ is a group under multiplication. It is a subgroup of the group $R_v^\times$ of units in R_v.

EXAMPLE. When $F = \mathbb{Q}$ and v counts the net power of a prime number p dividing a rational number, the residue class field $\Bbbk_v$ has p elements, with the integers $0, 1, \ldots, p-1$ being coset representatives. The group $R_v^\times$ is the multiplicative group of rationals having numerators and denominators prime to p. The members of $1 + P_v^n$ are rationals of the form $1 + p^n ab^{-1}$, where a and b are integers and b is prime to p. If we write this as $b^{-1}(b + p^n a)$, we see that the condition on a rational to be in $1 + P_v^n$ is that its numerator and denominator be prime to p and be congruent to each other modulo p^n.

Now we return to our first example of a discrete valuation, which was constructed from a nonzero prime ideal P in a Dedekind domain R. We called the valuation $v_P(\cdot)$. We asserted earlier that the construction via $v_P(\cdot)$ picks out the localization of R at P and the associated data. This assertion will be proved in Proposition 6.4 below. We begin with a handy lemma.

[2]Some books use the term "uniformizer" or "uniformizing element" for any generator π of the principal ideal P_v. The generators are exactly the prime elements of the ring R_v.

Lemma 6.3. Let R be a Dedekind domain regarded as a subring of its field of fractions F, let P be a nonzero prime ideal in R, and let v_P be the valuation of F defined by P. Then any element x of F with $v_P(x) = 0$ is of the form $x = ab^{-1}$ with a and b in R and $v_P(a) = v_P(b) = 0$.

PROOF. If x is an element of F with $v_P(x) = 0$, write $x = a'b'^{-1}$ with $a' \in R$ and $b' \in R$. Then $v_P(a') = v_P(b') = n$ for some integer $n \geq 0$. Since a' and b' are in R, (a') and (b') are ordinary ideals, and their prime factorizations are into ordinary ideals. Let the factorizations be $(a') = P^n Q_1$ and $(b') = P^n Q_2$, where Q_1 and Q_2 are products of prime ideals not involving P. Since we are dealing with ordinary ideals, a' and b' lie in P^n. Choose an element z in the fractional ideal P^{-n} that is not in P^{-n+1}. By definition of P^{-n}, zP^n is contained in R. Hence za' and zb' lie in R. Write $(za') = P^m Q_3$ and $(zb') = P^{m'} Q_4$, where $m \geq 0$ and where Q_3 and Q_4 are ordinary ideals whose prime factorizations do not involve P. Substituting for (a'), we obtain $(z)P^n Q_1 = P^m Q_3$ and hence $(z)P^n = P^m Q_3 Q_1^{-1}$. From this expression we see that $Q_3 Q_1^{-1}$ is an ordinary ideal. By definition of P^{-n+1}, $(z)P^{n-1}$ is not contained in R. Since $(z)P^{n-1} = P^{m-1} Q_3 Q_1^{-1}$, it follows that $m = 0$. Similarly $m' = 0$. Consequently $v_P(za') = v_P(zb') = 0$, and the lemma follows with $a = za'$ and $b = zb'$. □

Proposition 6.4. Let R be a Dedekind domain regarded as a subring of its field of fractions F, let P be a nonzero prime ideal in R, and let $v_P(\cdot)$ be the corresponding valuation of F. If S denotes the multiplicative system in R consisting of the complement of P and if the localization $S^{-1}R$ is regarded as a subring of F, then the valuation ring R_{v_P} coincides with $S^{-1}R$ and the valuation ideal P_{v_P} coincides with $S^{-1}P$.

PROOF. The set S consists exactly of the members x of R with $v_P(x) \leq 0$. Since v_P is nonnegative on R, these are the members x of R with $v_P(x) = 0$. Thus each x in $S^{-1}R$ has $v_P(x) \geq 0$, and $S^{-1}R$ is a subset of R_{v_P}.

For the reverse inclusion, fix a member π of P that is not in P^2. This element has $v_P(\pi) = 1$. If x is given in R_{v_P} with $v_P(x) = n \geq 0$, then we can write $x = \pi^n u$ for some member u of F with $v_P(u) = 0$. By Lemma 6.3 we can decompose u as $u = ab^{-1}$ with a and b in R and $v_P(a) = v_P(b) = 0$. The members of R on which v_P takes the value 0 are exactly the members of S. Thus u is exhibited as the quotient of two members of S, and u is in $S^{-1}R$. Since π is in the ideal P of R, $x = \pi^n u$ is in $S^{-1}R$. Hence $R_{v_P} = S^{-1}R$.

The ideal $S^{-1}P$ is a maximal ideal of $S^{-1}R = R_{v_P}$, and we observed just before Proposition 6.2 that P_{v_P} is the unique maximal ideal of R_{v_P}. Therefore $S^{-1}P = P_{v_P}$. □

Let us investigate the nature of an arbitrary discrete valuation in various settings involving a Dedekind domain. The main general result of this section is as follows.

Theorem 6.5. Let R be a Dedekind domain regarded as a subring of its field of fractions F, and let v be a discrete valuation of F such that $R \subseteq R_v$. Then

(a) $P = R \cap P_v$ is a nonzero prime ideal of R,
(b) the associated discrete valuation v_P defined by P coincides with v,
(c) $PR_v = P_v$,
(d) $R + P_v = R_v$, and in fact $R + P_v^n = R_v$ for every integer $n \geq 1$, and
(e) the inclusion of R into R_v induces a field isomorphism $R/P \cong R_v/P_v$.

PROOF. Since 1 is not in P_v, the ideal P in (a) is proper. If a and b are members of R such that ab is in P, then ab is in P_v, one of a and b is in P_v as well as R, and $P = R \cap P_v$ is a prime ideal. The ideal P cannot be 0 because otherwise every nonzero element x of R would have $v(x) = 0$, in contradiction to the fact that F is the field of fractions of R. Thus P is a nonzero prime ideal of R. This proves (a).

For (b) and (c), let us begin by showing that $v_P(x) = 0$ implies $v(x) = 0$. By Lemma 6.3 we can write $x = ab^{-1}$ with a and b in R and with $v_P(a) = v_P(b) = 0$. The values of v_P show that the members a and b of R are not in P. Since $P = R \cap P_v$, neither a nor b is in P_v. Therefore $v(a) \leq 0$ and $v(b) \leq 0$. Since $R \subseteq R_v$ by assumption, $v(a) \geq 0$ and $v(b) \geq 0$. We conclude that $v(a) = v(b) = 0$ and that $v(x) = v(ab^{-1}) = v(a) - v(b) = 0$.

Now we can show that $v = v_P$ and that $PR_v = P_v$. The ideal PR_v of R_v has to be of the form P_v^e for some integer $e \geq 0$ by Proposition 6.2c, and the integer e has to be > 0 because 1 is not in PR_v. If a nonzero $x \in R$ has $v_P(x) = n$ for some integer $n \geq 0$, then $xR = P^nQ$, where Q is an ideal of R whose prime factorization does not involve P. The function v_P is 0 on Q, and the result of the previous paragraph shows that v is 0 on Q. Hence the members of Q are units in R_v, and $QR_v = R_v$. Therefore $xR_v = xRR_v = P^nQR_v = P^nR_v = (PR_v)^n = P_v^{en}$, and $v(x) = en = ev_P(x)$. Since F is the field of fractions of R, $v = ev_P$ everywhere. The image of v_P is $\mathbb{Z} \cup \{+\infty\}$, and we conclude that $e = 1$. In other words, $v = v_P$ and $PR_v = P_v$. This proves (b) and (c).

For the first conclusion in (d), we certainly have $R + P_v \subseteq R_v$. In the reverse direction, let $x \in R_v$ be given. If $v(x) > 0$, then x is in P_v, and there is nothing to prove. If $v(x) = 0$, then (b) and Lemma 6.3 together show that we can write $x = ab^{-1}$, where a and b are members of R but not P. Since R/P is a field, we can choose c in R with bc in $1 + P$. Then

$$x - ac = a(b^{-1} - c) = ab^{-1}(1 - bc) = x(1 - bc).$$

The right side is a member of R_vP, and (c) showed that $R_vP = P_v$. Therefore x is exhibited as the sum of the member ac of R and the member $x(1 - bc)$ of P_v, and we conclude that $R + P_v = R_v$. This proves the first conclusion in (d).

For the second conclusion in (d), we show inductively for $n \geq 1$ that $P^{n-1} + P_v^n = P_v^{n-1}$, the case $n = 1$ being what has already been proved in (d). Assume that case n has been proved. Multiplying the equality by P and using (c), we obtain $P^n + PP_v^n = (PR_v)P_v^{n-1} = P_vP_v^{n-1} = P_v^n$. Since $P \subseteq P_v$, the term PP_v^n is contained in P_v^{n+1}, but increasing the left side in this way does not increase the right side. Thus $P^n + P_v^{n+1} = P_v^n$. This completes the induction. Using a second induction, we show that $R + P_v^n = R_v$. We have already proved this equality for $n = 1$. If we assume it for n and substitute from what has just been proved, we obtain $R + (P^n + P_v^{n+1}) = R_v$, and this proves case $n + 1$ since $P^n \subseteq R$. The second conclusion of (d) thus follows by induction.

For (e), we are assuming that $R \subseteq R_v$, and we have defined $P = R \cap P_v$. Thus the inclusion $R \to R_v$, when followed by the passage to the quotient R_v/P_v, descends to the quotient as a field map $R/P \to R_v/P_v$. By (d), any member x of R_v is the sum of a member y of R and a member z of P_v; then $y + P$ is the member of R/P that maps to $x + P_v$ in R_v/P_v. Thus the field map $R/P \to R_v/P_v$ is onto, and (e) is proved. □

Corollary 6.6. Let R be a Dedekind domain regarded as a subring of its field of fractions F. If x is a member of $\mathbb{F}$ such that $v(x) \geq 0$ for every discrete valuation v of F satisfying $R \subseteq R_v$, then x lies in R.

PROOF. We may assume that $x \neq 0$. Write $x = ab^{-1}$ with a and b in R. Theorem 6.5 shows that the valuations in question are the ones determined by the nonzero prime ideals of R. If the principal ideals (a) and (b) factor as $(a) = P_1^{j_1} \cdots P_r^{j_r}$ and $(b) = P_1^{k_1} \cdots P_r^{k_r}$, then $0 \leq v_{P_i}(x) = v_{P_i}(ab^{-1}) = j_i - k_i$ for $1 \leq i \leq r$. Thus $j_i \geq k_i$ for all i, and the fractional ideal (ab^{-1}) equals the product $P_1^{j_1-k_1} \cdots P_r^{j_r-k_r}$, which is contained in R. Hence $x = ab^{-1}$ lies in R. □

A finite field has no discrete valuations because of the requirement that the image of a discrete valuation be $\mathbb{Z} \cup \{+\infty\}$. If we drop this requirement in the definition and let a be a multiplicative generator of a finite field, then any discrete valuation v would have $v(a^k) = kv(a)$ by property (ii). Taking k equal to the order of a and using that $v(1) = 0$, we obtain $v(a) = 0$. Thus if we drop the requirement about the image of a discrete valuation, the only possibility has $v(0) = +\infty$ and $v(x) = 0$ for all $x \neq 0$. Thus this setting is not very interesting.

The settings in which discrete valuations v are of most interest to us are the following:

(i) number fields,

(ii) "function fields in one variable" over a base field,[3]

[3]This notion has not been defined thus far in the book but will be treated in Chapter VII. The fields in question are finite algebraic extensions of a field $\Bbbk(X)$, where X is an indeterminate and $\Bbbk$

(iii) fields obtained from (i) or (ii) by a process of completion similar to that used in forming the field of p-adic numbers.

The first of these are the initial subject matter of algebraic number theory, and the second of these are the initial subject matter of algebraic geometry—the geometry of curves. The third of these are used as a tool in studying the other two. Section VIII.7 of *Basic Algebra* explained parts of the analogy between the first two kinds of fields, and that is why we treat them together. We shall use Proposition 6.7 below to determine their discrete valuations. In the case of (ii), the members of the base field $\Bbbk$ are regarded as constants, and the interest is only in valuations that are 0 on $\Bbbk^\times$.

Proposition 6.7. Let R be a Dedekind domain, let F be its field of fractions, let K be a finite algebraic extension of F, and let T be the integral closure of R in K. If a discrete valuation v of K is ≥ 0 on R, then it is ≥ 0 on T.

REMARKS. We make repeated use in this chapter of the fact that T is a Dedekind domain in this situation. This fact was proved as Theorem 8.54 of *Basic Algebra* for the case that K is a finite *separable* extension of F, but it is valid without the hypothesis of separability. The result without the hypothesis of separability will be proved in Chapter VII as part of an investigation of separable and "purely inseparable" extensions.

PROOF. If $x \neq 0$ is in T, then the minimal polynomial of x over R is a monic polynomial in $T[X]$, and thus there exist an integer n and coefficients $a_{n-1}, \dots, a_0$ in R such that

$$x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Properties (ii) and (iii) of discrete valuations show from this equation that

$$nv(x) \geq \min_{0 \leq j \leq n-1} \big(v(a_j) + jv(x)\big).$$

Since $v(a_j) \geq 0$, we obtain $nv(x) \geq \min_{0 \leq j \leq n-1} jv(x)$, and it follows that $v(x) \geq 0$. Thus v is nonnegative on T. □

Corollary 6.8. The only discrete valuations of the field $\mathbb{Q}$ of rationals are the ones leading to the p-adic absolute value for each prime number p. If K is a number field and T is its the ring of algebraic integers, then the only discrete valuations of K are the valuations v_P corresponding to each nonzero prime ideal P of T.

---

is a field called the **base field**. At times later in the chapter, we shall be interested only in the case that the algebraic extension is separable. It will be proved in Chapter VII that for perfect fields $\Bbbk$, this separability can always be arranged by adjusting the indeterminate X suitably.

PROOF. If v is an arbitrary discrete valuation of $\mathbb{Q}$, then property (iv) of discrete valuations shows that $v(-1) = v(1) = 0$, and property (ii) allows us to conclude that v is nonnegative on all of $\mathbb{Z}$. Thus $\mathbb{Z}$ is contained in the valuation ring of v, and Theorem 6.5 applies. By (a) in the theorem, the intersection of $\mathbb{Z}$ with the valuation ideal is a nonzero prime ideal of $\mathbb{Z}$, hence is $p\mathbb{Z}$ for some prime number p. Part (b) in the theorem then identifies v as the valuation corresponding to $p\mathbb{Z}$. This proves the first conclusion.

For the second conclusion, let v be a discrete valuation of K. The restriction to $\mathbb{Q}$ has to be a positive integral multiple of a discrete valuation of $\mathbb{Q}$ or else a function that is identically 0 on $\mathbb{Q}^\times$. In either case, v is ≥ 0 on $\mathbb{Z}$, and Proposition 6.7 shows that v is ≥ 0 on T. If R_v denotes the valuation ring of v and P_v denotes the valuation ideal, then this says that $T \subseteq R_v$. We can therefore apply Theorem 6.5. If P is defined by $P = T \cap P_v$, then (a) in the theorem shows that P is a nonzero prime ideal, and (b) shows that $v = v_P$. □

Let us now consider the field $\mathbb{C}(X)$, regarding it as having some properties in common with the number field $\mathbb{Q}$. We want to know whether some analog of Corollary 6.8 is valid for $\mathbb{C}(X)$. The ring $\mathbb{C}[X]$ of polynomials is a principal ideal domain with $\mathbb{C}(X)$ as field of fractions, and the prime ideals of $\mathbb{C}[X]$ are all of the form $(X - c)$ with $c \in \mathbb{C}$ because $\mathbb{C}$ is algebraically closed. For each such c, we therefore obtain a discrete valuation $v_{(X-c)}$. Are there any other discrete valuations? If we think geometrically about this question, we can regard $\mathbb{C}(X)$ as the rational functions on the Riemann sphere, and each discrete valuation addresses the order of vanishing of rational functions at some point of the sphere. For the points of the sphere that correspond to points c of $\mathbb{C}$, such a valuation picks out the power of $(X - c)$ by which the rational function should be divided in order to be regular and nonvanishing at c. The point ∞ on the Riemann sphere behaves differently. The usual technique in complex-variable theory is to replace X by $1/X$ and examine the behavior at 0. Following that prescription, we are led to a discrete valuation v_∞ that is not of the form v_P for some prime ideal P of $\mathbb{C}[X]$. The definition of v_∞ on the quotient $f(X)/g(X)$ of nonzero polynomials is

$$v_\infty(f(X)/g(X)) = \deg g - \deg f$$

with $v_\infty(0) = +\infty$ as usual. The next proposition, which extends one of Liouville's theorems in complex-variable theory[4] from $\mathbb{C}$ to a general field $\Bbbk$, says that there are no other discrete valuations of interest for this example.

Proposition 6.9. Let $\Bbbk$ be any field, and let $F = \Bbbk(X)$ be the field of rational expressions in one indeterminate over $\Bbbk$. Regard F as the field of fractions of

[4]For a meromorphic function on the Riemann sphere, the sum of the orders of the poles equals the sum of the orders of the zeros.

the principal ideal domain $\Bbbk[X]$. Then the only discrete valuations of F that are 0 on the multiplicative group $\Bbbk^\times$ of nonzero constant polynomials are the various valuations $v_{(p)}$, where $p(X)$ is a monic prime polynomial in $\Bbbk[X]$, and the valuation v_∞ that is defined on nonzero elements of F by

$$v_\infty(f(X)/g(X)) = \deg g - \deg f$$

if f and g are polynomials. Moreover, any nonzero $h(X)$ in F has

$$v_\infty(h) + \sum_{\substack{p(X) \text{ monic} \\ \text{prime in } R}} (\deg p) v_{(p)}(h) = 0.$$

PROOF. Let v be a discrete valuation of F that is 0 on $\Bbbk^\times$. First suppose that $v(X) \geq 0$. Being 0 on the coefficients, v is nonnegative on all polynomials. Thus $\Bbbk[X]$ is contained in the valuation ring of v, and Theorem 6.5 applies. By (a) in the theorem, the intersection of $\Bbbk[X]$ with the valuation ideal is a nonzero prime ideal of $\Bbbk[X]$, hence is $(p(X))$ for some monic prime polynomial $p(X)$. Part (b) in the theorem then identifies v as the valuation corresponding to $(p(X))$.

Next suppose that $v(X) < 0$. Since $\Bbbk[X^{-1}]$ has $\Bbbk(X)$ as field of fractions, the argument in the previous paragraph is applicable, and we find that v is the valuation determined by the prime ideal (X^{-1}) in $\Bbbk[X^{-1}]$. In particular, $v(X) = -1$. To find $v(f)$ for a general polynomial $f(X) = a_n X^n + \cdots + a_1 X + a_0$ in $\Bbbk[X]$ under the assumption that $a_n \neq 0$, we write f as $X^n(a_n + \cdots + a_1 X^{1-n} + a_0 X^{-n})$. The member $a_n + \cdots + a_1 X^{1-n} + a_0 X^{-n}$ of $\Bbbk[X^{-1}]$ is not divisible by X^{-1}, and thus v is 0 on it. Consequently $v(f) = v(X^n) = nv(X) = -n = -\deg f$. If f and g are both nonzero in $\Bbbk[X]$, then it follows that $v(f/g) = v(f) - v(g) = -\deg f + \deg g = v_\infty(f/g)$. That is, $v = v_\infty$.

To prove the displayed formula, write a given nonzero member $h(X)$ of F as the quotient of two relatively prime polynomials, thus as $h(X) = f(X)/g(X)$. Factor the numerator as $f(X) = c\prod_{i=1}^m p_i(X)^{k_i}$ with $c \in \Bbbk^\times$, and factor the denominator similarly. If $p(X)$ is a monic prime polynomial, then inspection of the formula for $f(X)$ shows that $v_{(p)}(f)$ is k_i if $p = p_i$ and is 0 otherwise. Hence $\sum_p (\deg p) v_{(p)}(f) = \sum_{i=1}^m k_i \deg p_i = \deg f$. Subtracting this formula and a corresponding formula for g, we obtain

$$\sum_p (\deg p) v_{(p)}(f/g) = \deg f - \deg g = -v_\infty(h),$$

and the result follows. □

Corollary 6.10. Let $\Bbbk$ be a field, let $F = \Bbbk(X)$ be the field of rational expressions in one indeterminate over $\Bbbk$, let K be a finite algebraic extension of

$\Bbbk[X]$, let T be the integral closure of $\Bbbk[X]$ in K, and let v be a discrete valuation of K that is 0 on the multiplicative group $\Bbbk^\times$. Then the only possibilities for v are as follows:

(a) $v(X) \geq 0$, and there exists a unique nonzero prime ideal P in T such that $v = v_P$,

(b) $v(X) < 0$, and there exists a prime ideal P in the integral closure T' of $\Bbbk[X^{-1}]$ in K such that $P \cap \Bbbk[X^{-1}] = X^{-1}\Bbbk[X^{-1}]$ and such that v is the valuation of K determined by P.

REMARK. The ideals P that occur in (b) are the ones in the prime factorization of the ideal $X^{-1}T'$ in T'. There is at least one, and there are only finitely many.

PROOF. The argument is similar to the one for Corollary 6.8, except that we have to take into account what Proposition 6.9 says when $v(X) < 0$. The conclusion is that either v is ≥ 0 on $\Bbbk[X]$, and then Proposition 6.7 and Theorem 6.5 show that v is as in (a), or else $v(X) < 0$, and then Proposition 6.7 and Theorem 6.5 show that v is as in (b). □

To conclude, let us complete the remarks about fractional ideals begun early in this section. In the context that R is a Dedekind domain and F is its field of fractions, we mentioned that the nonzero fractional ideals of F form a group. We denote this group by $\mathcal{I}$. The nonzero principal fractional ideals form a subgroup $\mathcal{P}$, and $\mathcal{P}$ is isomorphic to the multiplicative group $F^\times$.

The point of the present discussion is that the group $\mathcal{I}/\mathcal{P}$ is isomorphic to the ideal class group of F as defined in the number-field setting in Section V.6. Recall the nature of this group. Two nonzero ideals I and J of R are equivalent if there exist nonzero members a and b of R with $aI = bJ$. Proposition 5.18 showed in the number-field setting that multiplication of such ideals descends to a multiplication on the set of equivalence classes and that the result is a group. This result holds for any Dedekind domain. The group is called the **ideal class group** of F; we denote it here by $\mathcal{C}$.

To verify that $\mathcal{C} \cong \mathcal{I}/\mathcal{P}$, we map each ideal I of R to its coset in $\mathcal{I}/\mathcal{P}$. If I and J are equivalent ideals of R and $aI = bJ$, then $(ab^{-1})I = J$, and I and J map to the same coset. Thus $\mathcal{C}$ maps homomorphically into $\mathcal{I}/\mathcal{P}$. If I maps into the identity coset, then $xI = R$ for some $x \in F^\times$. Writing x as ab^{-1} with a and b in R shows that $aI = bR = (b)$, hence that I is equivalent to a principal ideal. Thus the homomorphism $\mathcal{C} \to \mathcal{I}/\mathcal{P}$ is one-one. Finally if M is any nonzero fractional ideal of F, then we can find some $x \in F^\times$ with $xM \subseteq R$. Here xM is an ideal of R, and the equivalence of M and xM exhibits the class of M in $\mathcal{I}/\mathcal{P}$ as in the image of $\mathcal{C}$. Consequently $\mathcal{C} = \mathcal{I}/\mathcal{P}$, as asserted.

3. Absolute Values

The next step in analyzing and generalizing the construction of the p-adic absolute value is to pass from the valuation, which appears in the exponent, to the absolute value itself. If F is a field, an **absolute value** on F is a function $|\cdot|$ from F to $\mathbb{R}$ such that

(i) $|x| \geq 0$ with equality if and only if $x = 0$,
(ii) $|x + y| \leq |x| + |y|$ for all x and y in F,
(iii) $|xy| = |x||y|$ for all x and y in F.

It follows directly that

(iv) $|-1| = |1| = 1$ and that
(v) $|-x| = |x|$ for all x in F.

In fact, (iv) follows by combining (i) with (iii) for $x = y = 1$ and then with (iii) for $x = y = -1$; then (v) follows by combining (iii) and (iv). The absolute value $|\cdot|$ on F is said to be **nonarchimedean** if the following strong form of (ii) holds:[5]

(ii′) $|x + y| \leq \max(|x|, |y|)$ for all x and y in F.

Otherwise it is called **archimedean**. The inequality in (ii′) is called the **ultrametric inequality**. When the ultrametric inequality holds, then the following additional condition holds:

(vi) $|x + y| = |x|$ whenever x and y in F have $|y| < |x|$.

In fact, when $|y| < |x|$, (ii′) immediately gives $|x + y| \leq |x|$. But also (ii′) and (v) give $|x| \leq \max(|x + y|, |-y|) = \max(|x + y|, |y|)$. On the right side, the maximum cannot be $|y|$ because $|x| \leq |y|$ is false. Thus $|x| \leq |x + y|$, and (vi) holds.

Although it might seem counterintuitive, it turns out that the archimedean absolute values are easier to understand than the nonarchimedean ones in the number fields and function fields of interest to us.

Because of (iii), any absolute value of F when restricted to $F^\times$ is a multiplicative homomorphism into the positive real numbers. The image in the positive reals is therefore a group.

EXAMPLES OF NONARCHIMEDEAN ABSOLUTE VALUES.

(1) Let F be any field, and define $|x| = 0$ for $x = 0$ and $|x| = 1$ for $x \neq 0$. The result is a nonarchimedean absolute value called the **trivial absolute value**. It is of no interest, and we shall tend to exclude consideration of it from our results.

[5]Some authors refer to a nonarchimedean absolute value as a "valuation," using the same term as for the functions $v(\cdot)$ in Section 2. There is little danger of confusing the two notions, but we shall use the two distinct names anyway.

Any other absolute value will be said to be **nontrivial**. Observe for a finite field F that the fact that $x \mapsto |x|$ is a homomorphism from $F^\times$ to the positive reals implies that the only absolute value on a finite field is the trivial one.

(2) Let F be any field, let v be a discrete valuation on F, and fix a real number $r > 1$. Then $|x| = r^{-v(x)}$ defines a nonarchimedean absolute value on F. Property (i) of absolute values follows because $v(x)$ takes values in $\mathbb{Z} \cup \{+\infty\}$ and is infinite if and only if $x = 0$, property (ii′) follows because $v(x + y) \geq \min(v(x), v(y))$, and property (iii) follows because $v(xy) = v(x) + v(y)$. In particular, the p-adic absolute value is obtained in this way when we take $r = p$, and we obtain corresponding examples for any number field F by taking $v = v_P$ and fixing $r > 1$, where P is any nonzero prime ideal in the ring of algebraic integers in F. For the function field $F = \Bbbk(X)$, we obtain corresponding examples by taking $v = v_{(p)}$ and fixing $r > 1$, where $p(X)$ is any monic prime polynomial in $\Bbbk(X)$. The choice $v = v_\infty$ gives us another example. In all of these cases, the image of $F^\times$ in $\mathbb{R}^\times$ under the absolute value is discrete in the sense that each one-point set of the image is open in the relative topology from the positive reals. Corollary 6.17 will show conversely that any absolute value for which the image in $\mathbb{R}^\times$ of the nonzero elements is discrete and nontrivial is obtained in this way from a discrete valuation. It is worth pausing to interpret some of the conclusions of Theorem 6.5 in terms of absolute values and metrics.

Proposition 6.11. Let R be a Dedekind domain regarded as a subring of its field of fractions F, suppose that $|\cdot|$ is an absolute value on F defined by means of a discrete valuation v, and suppose that the subset R_v of F for which $|x| \leq 1$ contains R. If P_v denotes the subset of F with $|x| < 1$, then $P = R \cap P_v$ is a nonzero prime ideal of R, and also

(a) R is dense in R_v,
(b) P^n is dense in P_v^n for every $n \geq 1$,
(c) $R/P \cong R_v/P_v$.

PROOF. In terms of v, the set R_v is the valuation ring, and the set P_v is the valuation ideal. The hypothesis $R \subseteq R_v$ is the hypothesis of Theorem 6.5. Part (a) of that theorem shows that $P = R \cap P_v$ is a prime ideal in R. Conclusions (a) and (b) here follow from Theorem 6.5d. In fact, let $|x| = r^{-v(x)}$ with $r > 1$. Suppose that x is given in P_v^n with $n \geq 0$ and that a positive number r^{-N} is specified. We may assume that $N \geq n$. The condition for x to be in P_v^n is that $|x| \leq r^{-n}$. Theorem 6.5d shows that we can find an x_0 in R such that $x_0 + y = x$ with y in P_v^N, hence with $|y| \leq r^{-N}$. Then x_0 is in R and has $|x_0 - x| = |y| \leq r^{-N}$. Hence x_0 is within r^{-N} of x. Since $|x_0| \leq \max(|x|, |y|) = \max(r^{-n}, r^{-N}) = r^{-n}$, x_0 is in $R \cap P_v^n = P^n$. Conclusion (c) is immediate from Theorem 6.5e. □

EXAMPLES OF ARCHIMEDEAN ABSOLUTE VALUES. If F is any subfield of $\mathbb{R}$ or $\mathbb{C}$ and if $|\cdot|$ is defined as the restriction to F of the ordinary absolute value function, then $|\cdot|$ is an archimedean absolute value. Remarkably it turns out that there are no other archimedean absolute values, apart from "equivalent" ones in the sense to be defined below. We return to this matter at the end of Section 4. Actually, we shall be interested in archimedean absolute values only when F is a number field or is all of $\mathbb{R}$ or all of $\mathbb{C}$, and we will not need to invoke any deep theorem for the cases of interest to us.

Properties (i), (ii), and (v) of absolute values show that the function d with $d(x, y) = |x-y|$ is a metric on F, and the next section will examine what happens when this metric is completed. The resulting fields will be generalizations of the field of p-adic numbers and will useful as tools in investigating number fields and function fields in one variable.

Two absolute values $|\cdot|_1$ and $|\cdot|_2$ on the same field are said to be **equivalent** if there is a positive number α such that $|\cdot|_1 = (|\cdot|_2)^\alpha$. In our passage from a discrete valuation v to a nonarchimedean absolute value $|\cdot|$, we fixed $r > 1$ and defined $|x| = r^{-v(x)}$. Changing r changes the absolute value to an equivalent absolute value. In the archimedean case a positive power of an absolute value need not be an absolute value, since the triangle inequality may fail. For example the ordinary absolute value on $\mathbb{R}$ satisfies the triangle inequality; so does its α^{th} power for $\alpha < 1$ but not for $\alpha > 1$.

Equivalent absolute values yield the same topology on F and in fact the same Cauchy sequences.[6] Conversely two absolute values that yield the same topology are equivalent, according to the following proposition.

Proposition 6.12. Two nontrivial absolute values on a field F are equivalent if and only if

$$\{x \in F \mid |x|_1 > 1\} \subseteq \{x \in F \mid |x|_2 > 1\},$$

if and only if they induce the same topology on F.

REMARKS. If $|\cdot|_1$ is the trivial absolute value, then the stated inclusion holds for all $|\cdot|_2$, but the equivalence may fail; that is why the statement has to exclude this case. The statement of the proposition remains true if the inequalities $|x|_1 > 1$ and $|x|_2 > 1$ are replaced by $|x|_1 < 1$ and $|x|_2 < 1$, as we see by replacing x by x^{-1}.

PROOF. If the two absolute values are equivalent, then it is immediate from the definition of equivalent that equality holds in the stated inclusion. Conversely

[6] In many books an equivalence class of absolute values on a field is called a "place" of the field. We shall use this term in Sections 9 and 10 of this chapter,

suppose that the inclusion holds. Fix $x \in F$ with $|x|_1 > 1$. Such an x exists because $|\cdot|_1$ is nontrivial. Since $|x|_2 > 1$, there exists a real $s > 0$ with $|x|_1 = |x|_2^s$. We shall show that $|\cdot|_1 = |\cdot|_2^s$.

Let $y \in F$ be arbitrary with $|y|_1 \geq 1$. Find the number $r \geq 0$ depending on y such that $|y|_1 = |x|_1^r$. Let $\{a_n/b_n\}$ be a sequence of positive rationals strictly decreasing to r such that a_n and b_n are both positive. Then $|y|_1 = |x|_1^r < |x|_1^{a_n/b_n}$, from which we obtain $|y^{b_n}|_1 < |x^{a_n}|_1$ and $|x^{a_n} y^{-b_n}|_1 > 1$. By assumption, $|x^{a_n} y^{-b_n}|_2 > 1$, and therefore $|y|_2 < |x|_2^{a_n/b_n}$. Passing to the limit, we obtain $|y|_2 \leq |x|_2^r$.

Now suppose that $|y|_1 > 1$. Arguing similarly with a sequence of positive rationals strictly increasing to r, we obtain $|y|_2 \geq |x|_2^r$. Thus $|y|_2 = |x|_2^r$. Then we have

$$|y|_1 = |x|_1^r = |x|_2^{rs} = |y|_2^s \qquad \text{whenever } |y|_1 > 1. \tag{$*$}$$

If instead $|y|_1 = 1$, then the number r in the second paragraph of the proof is 0, and we obtain $|y|_2 \leq |x|_2^r = 1$. Replacing y by y^{-1} shows also that $|y|_2 \geq 1$. Thus $|y|_1 = 1$ implies $|y|_2 = 1$.

The remaining case is that $|y|_1 < 1$. Then we apply $(*)$ to y^{-1} and conclude that $|y|_1 = |y|_2^s$ in this case as well. This completes the proof of the first conclusion of the proposition.

For the final statement we know that equivalent absolute values lead to the same topology. Conversely suppose that the absolute values are not equivalent. By what we have just shown, there exists $x \in F$ with $|x|_1 > 1$ and $|x|_2 \leq 1$. Then $\{x^{-n}\}$ is a sequence convergent to 0 in the topology from $|\cdot|_1$ but not convergent to 0 in the topology from $|\cdot|_2$. Therefore the topologies are different. □

Proposition 6.13. If $|\cdot|$ is an absolute value on the field F, then the topology on F induced by the associated metric makes F into a topological field.

REMARK. The proof is similar to part of the argument that proves Proposition 6.1 except that the general triangle inequality has to be used in place of the ultrametric inequality.

PROOF. To see that addition, subtraction, and multiplication are continuous on F, let $\{x_n\}$ and $\{y_n\}$ be convergent sequences in F with respective limits x and y. Use of the triangle inequality on F gives

$$|(x_n + y_n) - (x + y)| = |(x_n - x) + (y_n - y)| \leq |x_n - x| + |y_n - y|.$$

The right side has limit 0 in $\mathbb{R}$, and therefore $x_n + y_n$ has limit $x + y$ in F. A completely analogous argument, making use also of the equality $|-1| = |1|$, shows that subtraction is continuous. Consider multiplication. If M is an upper

bound for the absolute values $|x_n|$, then use of the multiplicative property of the absolute value on F gives

$$\begin{aligned}|x_n y_n - xy| &= |x_n(y_n - y) + y(x_n - x)| \le |x_n(y_n - y)| + |y(x_n - x)| \\ &= |x_n||y_n - y| + |y||x_n - x| \le M|y_n - y| + |y||x_n - x|.\end{aligned}$$

The right side has limit 0 in $\mathbb{R}$, and therefore $x_n y_n$ has limit xy in F.

To see that inversion $x \mapsto x^{-1}$ is continuous on $F^\times$, let $\{x_n\}$ be a sequence in $F^\times$ with limit x in $F^\times$. Since $\lim_n |x_n| = |x|$, we can find an integer N such that $|x_n| \ge \frac{1}{2}|x|$ for $n \ge N$. The computation

$$|x_n^{-1} - x^{-1}| = |(x - x_n)/(x_n x)| = |x - x_n|/(|x_n||x|) \le 2|x|^{-1}|x - x_n|,$$

valid for $n \ge N$, then shows that $\lim x_n^{-1} = x^{-1}$, and inversion is continuous. Consequently F is a topological field. □

We now give a few results that limit the kinds of absolute values that can arise in particular situations.

Proposition 6.14. If $|\cdot|$ is an absolute value on the field F for which there is some c with $|n| \le c$ for all integers $n \in \mathbb{Z}$, i.e., for all additive multiples of 1, then $|\cdot|$ is nonarchimedean. In particular, $|\cdot|$ is necessarily nonarchimedean if F has characteristic different from 0.

REMARK. When c exists, then c can be taken to be 1, since the image of $F^\times$ under the absolute value is a subgroup of the positive reals and the only bounded such subgroup is $\{1\}$.

PROOF. If x and y are in F and if n is any positive integer, then the Binomial Theorem gives $(x + y)^n = \sum_{j=0}^n \binom{n}{j} x^{n-j} y^j$. Therefore

$$\begin{aligned}|x + y|^n &= \sum_{j=0}^n \left|\tbinom{n}{j}\right| |x|^{n-j} |y|^j \\ &\le c \sum_{j=0}^n \max(|x|, |y|)^{n-j} \max(|x|, |y|)^j \\ &= c(n + 1) \max(|x|, |y|)^n.\end{aligned}$$

Extraction of the n^{th} root gives $|x + y| \le c^{1/n}(n + 1)^{1/n} \max(|x|, |y|)$. Passing to the limit, we obtain $|x + y| \le \max(|x|, |y|)$. □

Theorem 6.15 (Ostrowski's Theorem). If $|\cdot|$ is a nontrivial absolute value on the field $\mathbb{Q}$, then $|\cdot|$ is equivalent either to the p-adic absolute value $|\cdot|_p$ for some prime number p or to the ordinary absolute value $|\cdot|_{\mathbb{R}}$.

REMARKS. No two of these are equivalent because $\{p^n\}$ tends to 0 relative to the p-adic absolute value, $\{p^{-n}\}$ tends to 0 relative to the ordinary absolute value, and p^n has absolute value 1 relative to the ℓ-adic absolute value for all prime numbers $\ell \neq p$.

PROOF. First suppose that every integer n has $|n| \leq 1$. Proposition 6.14 shows that $|\cdot|$ is nonarchimedean. Since $|\cdot|$ is nontrivial, we must have $|n| < 1$ for some n, and we may take n to be positive. Since $|n|$ is the product of $|p|$ over all primes dividing n, multiplicities included, some prime number p has $|p| < 1$. Let us see that p is unique. If, on the contrary, $|q| < 1$ for a second prime number q, choose integers a and b with $ap + bq = 1$. Then $1 = |1| = |ap + bq| \leq \max(|ap|, |bq|) = \max(|a||p|, |b||q|) \leq \max(|p|, |q|) < 1$, contradiction. If we now define a positive real α by $|p| = p^{-\alpha}$, then it follows that $|n| = (|n|_p)^\alpha$ for all integers n. Therefore $|\cdot| = (|\cdot|_p)^\alpha$ on all of $\mathbb{Q}$.

Now suppose that n is some integer with $|n| > 1$. We may assume that n is positive. For any positive integer m, the triangle inequality gives

$$|m| = |1 + \cdots + 1| \leq |1| + \cdots + |1| = m.$$

In particular we have $|n| = n^\alpha$ for some real α with $0 < \alpha \leq 1$.

We shall prove that

$$|m| \leq m^\alpha \tag{$*$}$$

for all positive integers m. We start by expanding m to the base n, writing

$$m = c_0 + c_1 n + c_2 n^2 + \cdots + c_{k-1} n^{k-1},$$

where k is the integer such that $n^{k-1} \leq m < n^k$ and where each c_j satisfies $0 \leq c_j < n$. The triangle inequality gives

$$\begin{aligned}
|m| &\leq |c_0| + |c_1||n| + |c_2||n|^2 + \cdots + |c_{k-1}||n|^{k-1} \\
&\leq (n-1)(1 + n^\alpha + n^{2\alpha} + \cdots + n^{\alpha(k-1)}) && \text{by definition of } \alpha \\
&= \frac{(n-1)n^{\alpha k}}{n^\alpha - 1} = \frac{(n-1)n^\alpha}{n^\alpha - 1}\, n^{\alpha(k-1)} \\
&\leq \frac{(n-1)n^\alpha}{n^\alpha - 1}\, m^\alpha && \text{since } n^{k-1} \leq m.
\end{aligned}$$

In other words, there is a positive number C independent of m such that $|m| \leq Cm^\alpha$ for every positive integer m. For every positive integer N, we then have

$|m|^N = |m^N| \le Cm^{\alpha N}$, and thus $|m| \le C^{1/N} m^\alpha$. Letting N tend to infinity, we obtain $(*)$.

Let us now improve $(*)$ to the equality

$$|m| = m^\alpha \qquad \text{for every positive integer } m. \tag{$**$}$$

The integer k above has $n^{k-1} \le m < n^k$. Put $d = n^k - m$; this satisfies $0 < d \le n^k - n^{k-1}$. Then

$$n^{\alpha k} = |n|^k = |n^k| \le |m| + |d| \le |m| + d^\alpha \le |m| + (n^k - n^{k-1})^\alpha,$$

and consequently

$$|m| \ge n^{\alpha k} - (n^k - n^{k-1})^\alpha = n^{\alpha k}\big(1 - \big(1 - \tfrac{1}{n}\big)^\alpha\big) \ge m^\alpha\big(1 - \big(1 - \tfrac{1}{n}\big)^\alpha\big).$$

Thus $|m| \ge C' m^\alpha$ for some positive constant C' independent of m. For every positive integer N, we then have $|m|^N = |m^N| \ge C' m^{\alpha N}$ and hence $|m| \ge C'^{1/N} m^\alpha$. Letting N tend to infinity, we obtain $|m| \ge m^\alpha$. In combination with $(*)$, this proves $(**)$.

Since $|-m| = |m|$, the equality $(**)$ implies $|m| = (|m|_{\mathbb{R}})^\alpha$ for every integer m. Taking quotients, we obtain $|q| = (|q|_{\mathbb{R}})^\alpha$ for every rational q. □

Corollary 6.16. If $|\cdot|$ is a nontrivial absolute value on a number field F, then the restriction of $|\cdot|$ to $\mathbb{Q}$ is nontrivial.

REMARK. In view of Ostrowski's Theorem (Theorem 6.15), the restriction to $\mathbb{Q}$ therefore has to be equivalent to the p-adic absolute value for some p or to the ordinary absolute value.

PROOF. Since $|\cdot|$ is nontrivial, there exists x with $|x| > 1$. Raising x to a power if necessary, we may assume that $|x| \ge 2$. Arguing by contradiction, suppose that $|q| = 1$ for all nonzero q in $\mathbb{Q}$. Since x is algebraic over $\mathbb{Q}$, there exist an integer $n \ge 1$ and rational coefficients $q_{n-1}, \dots, q_0$ such that

$$x^n = q_{n-1}x^{n-1} + \cdots + q_1 x + q_0.$$

Applying $|\cdot|$ to both sides and using that $|q_j| \le 1$ for all j gives

$$|x|^n \le |x|^{n-1} + \cdots + |x| + 1 = \frac{|x|^n - 1}{|x| - 1} \le |x|^n - 1,$$

the right-hand inequality holding because $|x| \ge 2$. We have thus obtained $|x|^n \le |x|^n - 1$ and have arrived at a contradiction. □

An absolute value $|\cdot|$ on a field F such that the image of $F^\times$ is discrete is called a **discrete absolute value**. The p-adic absolute values on $\mathbb{Q}$ and on $\mathbb{Q}_p$ furnish examples.

Corollary 6.17. If $|\cdot|$ is a nontrivial discrete absolute value on the field F, then $|\cdot|$ is nonarchimedean, and $|x| = r^{-v(x)}$ for some discrete valuation of F.

REMARKS. Example 1 of nonarchimedean absolute values shows that discrete valuations always lead to discrete absolute values. This corollary is a converse. The trivial absolute value is of course nonarchimedean, but it does not arise from a discrete valuation. We shall not be interested in any nonarchimedean absolute values that do not arise from discrete valuations.

PROOF. First we show that $|\cdot|$ is nonarchimedean. Proposition 6.14 immediately handles the case that F has nonzero characteristic, and we may therefore take the characteristic to be 0. Let D be the discrete image subgroup of $F^\times$. This D in particular must contain the image of $\mathbb{Q}^\times$. Meanwhile, Theorem 6.15 says that the restriction of $|\cdot|$ to $\mathbb{Q}$ has to be trivial, or equivalent to the p-adic absolute value for some p, or equivalent to the ordinary absolute value. Under the ordinary absolute value, the image of $\mathbb{Q}^\times$ cannot be contained in D, and the restriction must be one of the other kinds. For all of the other kinds, the image of $\mathbb{Z}$ is bounded, and Proposition 6.14 allows us to conclude that $|\cdot|$ is nonarchimedean.

Now that $|\cdot|$ is nonarchimedean, we set $v(0) = +\infty$ and $v(x) = -\log_r |x|$ for $x \neq 0$. Properties (i), (ii′), and (iii) of nonarchimedean absolute values immediately imply the three defining properties of a discrete valuation. □

Corollary 6.18. If $|\cdot|$ is a nontrivial discrete absolute value on a field F, then the corresponding valuation ring $R = \{x \in F \mid |x| \leq 1\}$ and the valuation ideal $P = \{x \in F \mid |x| < 1\}$ are open and closed in F.

REMARK. Corollary 6.17 shows that $|\cdot|$ is defined by a discrete valuation.

PROOF. The definitions of R and P in the statement show that R is closed and P is open. Let D be the image of $F^\times$ under $|\cdot|$. A discrete subgroup of positive reals has to be equal[7] to $\{1\}$ or to the subgroup $r^{\mathbb{Z}}$ for a unique real $r > 1$. The nontriviality of $|\cdot|$ implies that the correct alternative is $r^{\mathbb{Z}}$. Then the equality $R = \{x \in F \mid |x| < r\}$ shows that R is open, and the equality $P = \{x \in F \mid |x| \leq r^{-1}\}$ shows that P is closed. □

Next we prove a general result applicable to number fields and to function fields in one variable that yields the conclusion that nonarchimedean absolute values in these cases are automatically discrete. The general result is obtained in two parts, stated as Lemma 6.19 and Proposition 6.20.

[7]One can invoke Lemma 5.14, for example.

Lemma 6.19. If R is a Dedekind domain regarded as a subring of its field of fractions F, and if $|\cdot|$ is a nonarchimedean absolute value on F that is ≤ 1 on R, then $|\cdot|$ is discrete. Hence either $|\cdot|$ is trivial or else it is defined by the valuation relative to a nonzero prime ideal of R.

PROOF. The subset of $x \in R$ for which $|x| < 1$ is a proper ideal I in R, and we let P be a prime ideal containing I. Since R is a Dedekind domain, P defines a corresponding discrete valuation v_P. Let $|x|_P = 2^{-v_P(x)}$. Then

$$\big\{x \in R \,\big|\, |x| < 1\big\} = I \subseteq P = \big\{x \in R \,\big|\, |x|_P < 1\big\},$$

and hence

$$\big\{x \in R \,\big|\, |x|_P = 1\big\} \subseteq \big\{x \in R \,\big|\, |x| = 1\big\}. \tag{$*$}$$

Let π be an element of R with $|\pi|_P = \frac{1}{2}$. If x is an arbitrary nonzero member of F with $|x|_P < 1$, then Proposition 6.4 shows that we can write $x = \pi^k x'$ with $k > 0$, x' in R, and $|x'|_P = 1$. Then $|x'| = 1$ by $(*)$, and it follows that $|x| = |\pi|^k$. Since $|x|_P = |\pi|_P^k$ also, there are only two possibilities. One possibility is that $|x| = |\pi| = 1$ for all $x \neq 0$, and then $|\cdot|$ is trivial. The other possibility is that the subsets of F for which $|x| < 1$ and for which $|x|_P < 1$ coincide. In this case we apply Proposition 6.12 and conclude that $|\cdot|$ and $|\cdot|_P$ are equivalent. □

Proposition 6.20. Let R be a Dedekind domain regarded as a subring of its field of fractions F, let K be a finite algebraic extension of F, and let T be the integral closure of R in K. If $|\cdot|$ is a nonarchimedean absolute value on K that is ≤ 1 on R, then it is ≤ 1 on T. Hence $|\cdot|$ is discrete, and either $|\cdot|$ is trivial or else it is defined by the valuation relative to a nonzero prime ideal of T.

PROOF. As with Proposition 6.7, T is a Dedekind domain. If $x \neq 0$ is in T, then the minimal polynomial of x over R is a monic polynomial in $R[X]$, and thus there exist an integer n and coefficients $a_{n-1}, \dots, a_0$ in R such that

$$x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Taking the absolute value of both sides and using the nonarchimedean property, we obtain

$$|x|^n \le \max_{0 \le j \le n-1} (|a_j||x|^j) \le \max_{0 \le j \le n-1} (|x|^j) = \max(1, |x|^{n-1}),$$

the inequality holding because $|\cdot|$ is assumed to be ≤ 1 on R. If we could have $|x| > 1$, then this inequality would read $|x|^n \le |x|^{n-1}$, which is a contradiction. We conclude that $|x| \le 1$ for all $x \in T$. The conclusions in the last sentence of the proposition now follow from Lemma 6.19. □

Corollary 6.21. If K is a number field, then every nontrivial nonarchimedean absolute value $|\cdot|$ on K comes from the valuation v_P relative to some nonzero prime ideal P in the ring of algebraic integers in K.

REMARK. Proposition 6.27 below will classify the archimedean absolute values on a number field.

PROOF. Since $|\cdot|$ is nonarchimedean, its restriction to $\mathbb{Q}$ is nonarchimedean. By Ostrowski's Theorem (or by inspection), it is ≤ 1 on $\mathbb{Z}$. The result now follows from Proposition 6.20 if we take R to be $\mathbb{Z}$ and F to be $\mathbb{Q}$. □

Corollary 6.22. Let $\Bbbk$ be a field, let $F = \Bbbk(X)$ be the field of rational expressions in one indeterminate over $\Bbbk$, let K be a finite algebraic extension of $\Bbbk[X]$, let T be the integral closure of $\Bbbk[X]$ in K, and let $|\cdot|$ be a nontrivial nonarchimedean absolute value on K that is 1 on the multiplicative group $\Bbbk^\times$. Then $|\cdot|$ is discrete, and the only possibilities for it are as follows:

(a) $|X| \le 1$, and there exists a unique nonzero prime ideal P in T such that $|\cdot|$ comes from the valuation determined by P,

(b) $|X| > 1$, and there exists a prime ideal P in the integral closure T' of $\Bbbk[X^{-1}]$ in K such that $P \cap \Bbbk[X^{-1}] = X^{-1}\Bbbk[X^{-1}]$ and such that $|\cdot|$ comes from the valuation of K determined by P.

REMARKS. As with Proposition 6.7, T and T' are Dedekind domains. If $\Bbbk$ has nonzero characteristic, then Proposition 6.14 shows that every absolute value is nonarchimedean. For the case that $\Bbbk$ has characteristic zero, remarks at the end of Section 4 will indicate why every absolute value that is 1 on $\Bbbk^\times$ is nonarchimedean; we shall not need to make use of this fact, however. In any event, just as with Corollary 6.10, the ideals P that occur in (b) are the ones in the prime factorization of the ideal $X^{-1}T'$ in T'; there is at least one, and there are only finitely many.

PROOF. The argument is similar to the one for Corollary 6.21, except that we have to take into account what happens when $|X| > 1$. We apply Proposition 6.20 either with $R = \Bbbk[X]$ or with $R = \Bbbk[X^{-1}]$.

Since $|\cdot|$ is 1 on $\Bbbk^\times$, an inequality $|X| \le 1$ implies that $|\cdot|$ is ≤ 1 on $\Bbbk[X]$, $|\cdot|$ being assumed to be nonarchimedean. Then Proposition 6.20 and Corollary 6.10 show that (a) holds. Similarly an inequality $|X| > 1$ implies that $|\cdot|$ is ≤ 1 on $\Bbbk[X^{-1}]$ because $|\cdot|$ is assumed nonarchimedean. Then Proposition 6.20 and Corollary 6.10 show that (b) holds. □

Theorem 6.23 (Weak Approximation Theorem). Let $|\cdot|_1, \dots, |\cdot|_n$ be inequivalent nontrivial absolute values on a field F. If $\epsilon > 0$ is a real number and $x_1, \dots, x_n$ are elements of F, then there exists y in F such that

$$|y - x_j|_j < \epsilon \qquad \text{for } 1 \le j \le n.$$

REMARKS. The special case of this theorem in which F is a number field and the absolute values are defined by n distinct nonzero prime ideals in the ring of algebraic integers follows from the Chinese Remainder Theorem (Theorem 8.27 of *Basic Algebra*, restated in the present book on page xxv). In fact, it is enough to handle the case that all the x_j's are algebraic integers in F. Let the prime ideals be $P_1, \dots, P_n$, and let $|\cdot|_j = r_j^{-v_{P_j}(\cdot)}$ with $r_j > 1$. If we specify any positive integers $k_1, \dots, k_n$, then the Chinese Remainder Theorem produces an algebraic integer y in F such that $y \equiv x_j \bmod P_j^{k_j}$ for $1 \le j \le n$. These congruences say that $v_{P_j}(y - x_j) \ge k_j$, hence that $|y - x_j|_j \le r_j^{-k_j}$. Thus we have only to choose $k_1, \dots, k_n$ large enough to make $r_j^{-k_j} < \epsilon$ for all j, and the inequalities of the theorem will hold.

PROOF. First let us prove that we can find an element z in F with

$$|z|_1 > 1 \qquad \text{and} \qquad |z|_j < 1 \ \text{ for } 2 \le j \le n. \tag{$*$}$$

We do so by induction on n, the case $n = 2$ being Proposition 6.12. Assuming the result for $n-1$, find u with $|u|_1 > 1$ and $|u|_j < 1$ for $2 \le j \le n-1$. Then by the result for $n = 2$, find v with $|v|_1 > 1$ and $|v|_n < 1$. Let $k > 0$ be an integer to be specified, and put

$$z = \begin{cases} v & \text{if } |u|_n < 1, \\ u^k v & \text{if } |u|_n = 1, \\ \frac{u^k v}{1+u^k} & \text{if } |u|_n > 1. \end{cases}$$

In the second case, k is to be chosen large enough to make $|u|_j^k |v|_j < 1$ for $2 \le j \le n-1$. In the third case, k is to be chosen large enough to make $|u|_1^k (1 + |u|_1^k)^{-1} |v|_1 > 1$, $|u|_j^k (1 - |u|_j^k)^{-1} |v|_j < 1$ for $2 \le j \le n-1$, and $|u|_n^k (|u|_n^k - 1)^{-1} |v|_n < 1$. Then z satisfies the conditions in $(*)$, and the inductive proof of $(*)$ is complete.

Applying $(*)$, find z_j such that $|z_j|_j > 1$ and $|z_j|_i < 1$ for $i \ne j$. Let l be a positive integer to be specified, and put

$$y = \sum_{i=0}^{n} \tfrac{x_i z_i^l}{1+z_i^l}.$$

Since $y - x_j = -x_j(1 + z_j^l)^{-1} + \sum_{i \ne j} x_i z_i^l (1 + z_i^l)^{-1}$, we obtain

$$|y - x_j|_j \le |x_j|_j \big(|z_j|_j^l - 1\big)^{-1} + \sum_{i \ne j} |x_i|_j \big(|z_i|_j^l (1 - |z_i|_j^l)^{-1}\big). \tag{$**$}$$

For l large enough, the coefficients $(|z_j|_j^l - 1)^{-1}$ and $|z_i|_j^l (1 - |z_i|_j^l)^{-1}$ for $i \ne j$ can be made as small as we please, and thus the right side of $(**)$ can be made to be $< \epsilon$. □

4. Completions

In this section we finish our project of establishing an abstract theory that generalizes the construction of the field of p-adic numbers. A little care is appropriate in stating the results. Here is an example of the cost of imprecision: We know that the field $\mathbb{Q}_p$ is obtained by completing $\mathbb{Q}$ with respect to the p-adic absolute value. We shall see in Section 5 that $\mathbb{Q}_p$ for $p = 5$ is obtained also by completing the field $\mathbb{Q}(i)$ with respect to a certain absolute value and that in fact there are two distinct equivalence classes of absolute values on $\mathbb{Q}(i)$ for which $\mathbb{Q}_5$ results in this way. Thus a completion process is not well specified unless we include all the data—the original field, the absolute value on it (or at least the equivalence class of absolute values), and the mapping into the completed space.

For this reason we introduce the notions of a **valued field**, namely a pair $(F, |\cdot|_F)$ consisting of a field and an absolute value on it, and a **homomorphism of valued fields**. If $(F, |\cdot|_F)$ and $(K, |\cdot|_K)$ are the two valued fields in question, a homomorphism from the first to the second is a field map $\varphi : F \to K$ such that $|x|_F = |\varphi(x)|_K$ for all x in F. We write φ^* for the corresponding operation of restriction: $\varphi^*(|\cdot|_K) = |\cdot|_F$. If φ carries F onto K, then φ is called an **isomorphism of valued fields**.

A **completion** of a valued field $(F, |\cdot|_F)$ is defined to be a homomorphism of valued fields $\varphi : (F, |\cdot|_F) \to (K, |\cdot|_K)$ such that $(K, |\cdot|_K)$ is complete as a metric space and $\varphi(F)$ is dense in K. The first theorem establishes existence.

Theorem 6.24. Let F be a field with a nontrivial absolute value $|\cdot|_F$, let d be the associated metric on F, let $\mathcal{R}$ be the subring of $\prod_{j=1}^{\infty} F$ consisting of all Cauchy sequences relative to d, and let $\mathcal{I}$ be the ideal in $\mathcal{R}$ consisting of all sequences convergent to 0. Then $\mathcal{I}$ is a maximal ideal in $\mathcal{R}$, and the quotient $\mathcal{R}/\mathcal{I}$ is a field. Consequently the Cauchy completion of F relative to d is a topological field $\overline{F} = \mathcal{R}/\mathcal{I}$. Let $i : F \to \overline{F}$ be the natural map $F \to \mathcal{R} \to \mathcal{R}/\mathcal{I}$ of F into the Cauchy completion given by carrying members of F into constant sequences in $\mathcal{R}$, followed by passage to the quotient. The metric $\bar{d}$ on the Cauchy completion is the unique continuous function $d : \overline{F} \times \overline{F} \to \mathbb{R}$ such that $\bar{d}(i(x), i(y)) = d(x, y)$. If a real-valued function $|\cdot|_{\overline{F}}$ is defined on $\overline{F}$ by $|x|_{\overline{F}} = \bar{d}(x, 0)$ for $x \in \overline{F}$, then $|\cdot|_{\overline{F}}$ is an absolute value on $\overline{F}$, and $i : (F, |\cdot|_F) \to (\overline{F}, |\cdot|_{\overline{F}})$ is a homomorphism of valued fields. Moreover, the absolute value on $\overline{F}$ is nonarchimedean if the absolute value on F is nonarchimedean.

REMARKS. The usual construction of the Cauchy completion embeds the original metric subspace as a dense subset of a complete metric space, and therefore this theorem is showing that $i : (F, |\cdot|_F) \to (\overline{F}, |\cdot|_{\overline{F}})$ is a completion of $(F, |\cdot|_F)$.

PROOF. The proof of this theorem is almost the same as the first part of the proof of Proposition 6.1, apart from notational changes. The differences occur in spots where the ultrametric inequality was invoked in the proof of Proposition 6.1 and only the triangle inequality is available here. The main such difference is the argument that the validity of the triangle inequality on F implies the validity of the triangle inequality on $\overline{F}$, and we give that argument in a moment. Correspondingly it is unnecessary for us to prove that the validity of the ultrametric inequality on F implies the validity of the ultrametric inequality on $\overline{F}$, because that argument does occur in the proof of Proposition 6.1.

The other places in the proof of Proposition 6.1 where the ultrametric inequality was used are in the proof that the completion is a topological field. It is not necessary to modify that proof here, however, since we can invoke Proposition 6.13.

Thus let us see that the validity of the triangle inequality on F implies the validity of the triangle inequality on $\overline{F}$. To proceed, let x and y be members of $\overline{F} = \mathcal{R}/\mathcal{I}$, and let $\{q_n\}$ and $\{r_n\}$ be respective coset representatives of them in $\mathcal{R}$. Then $\{q_n + r_n\}$ is a representative of $x + y$, by definition, and the continuity of $|\cdot|_{\overline{F}}$ on $\overline{F}$ implies that $\lim_n |q_n + r_n|_p = |x + y|_p$. From this limit formula and the triangle inequality for F, we obtain

$$\begin{aligned} |x + y|_{\overline{F}} &= \lim_n |q_n + r_n|_{\overline{F}} \le \limsup_n (|q_n|_{\overline{F}} + |r_n|_{\overline{F}}) \\ &\le \limsup_n |q_n|_{\overline{F}} + \limsup_n |r_n|_{\overline{F}} = |x|_{\overline{F}} + |y|_{\overline{F}}, \end{aligned}$$

since $\lim_n |q_n|_{\overline{F}} = |x|_{\overline{F}}$ and $\lim_n |r_n|_{\overline{F}} = |y|_{\overline{F}}$. This proves the triangle inequality on $\overline{F}$. □

A valued field $(L, |\cdot|_L)$ is said to be **complete** if L is Cauchy complete in the metric defined by $|\cdot|_L$. In Section 6 we shall make crucial use of a universal mapping property of the completion of a valued field.

Theorem 6.25. If $\iota : (F, |\cdot|_F) \to (K, |\cdot|_K)$ is a completion of the valued field $(F, |\cdot|_F)$ and if $\varphi : (F, |\cdot|_F) \to (L, |\cdot|_L)$ is a homomorphism of valued fields with $(L, |\cdot|_L)$ complete, then there exists a unique homomorphism of valued fields $\Phi : (K, |\cdot|_K) \to (L, |\cdot|_L)$ such that $\varphi = \Phi \circ \iota$.

REMARKS. As usual with universal mapping properties, this theorem implies a uniqueness result: any two completions of a valued field are canonically isomorphic. It is not necessary to write out the details. Making a small adjustment to the proof below, we see also that if a field has two equivalent absolute values on it, then the corresponding two completions are canonically isomorphic by a field map that respects the topologies.

PROOF. The theory of completion of a metric space produces a unique continuous function $\Phi : K \to L$ such that $\varphi = \Phi \circ \iota$, and this continuous function respects the metrics. It is necessary to check only that Φ respects addition and multiplication.

The argument is the same for the two operations, and we check only addition. Let x and y be given in K, and choose sequences $\{x_n\}$ and $\{y_n\}$ in F with $\lim \iota(x_n) = x, \lim \iota(y_n) = y$. Since addition is continuous in K, $\lim \iota(x_n + y_n) = x + y$. Since Φ is a continuous function with $\varphi = \Phi \circ \iota$,

$$\begin{aligned}\Phi(x) + \Phi(y) &= \Phi(\lim \iota(x_n)) + \Phi(\lim \iota(y_n)) \\ &= \lim(\Phi(\iota(x_n))) + \lim(\Phi(\iota(y_n))) = \lim(\varphi(x_n)) + \lim(\varphi(y_n)) \\ &= \lim(\varphi(x_n) + \varphi(y_n)) = \lim(\varphi(x_n + y_n)) \\ &= \lim(\Phi\iota(x_n + y_n)) = \Phi(\lim \iota(x_n + y_n)) = \Phi(x + y),\end{aligned}$$

and Φ respects addition. □

Theorem 6.24 generalizes the parts of Proposition 6.1 concerning $\mathbb{Q}_p$ but not those concerning $\mathbb{Z}_p$. The arguments concerning $\mathbb{Z}_p$ transparently made use of the ultrametric inequality, and they used a little more. The extra fact used is that the p-adic absolute value is defined from a discrete valuation. In view of Corollary 6.17 and Example 1 of nonarchimedean absolute values in the previous section, a necessary and sufficient condition for a nontrivial absolute value on a field F to be obtained from a discrete valuation is that the image of $F^\times$ under the valuation be a discrete subset of the positive reals. Such an absolute value is automatically nonarchimedean.

Theorem 6.26. Let $\iota : (F, |\cdot|_F) \to (\overline{F}, |\cdot|_{\overline{F}})$ be a completion of a valued field, and suppose that $|\cdot|_F$ is nontrivial and discrete. Let $v(\cdot)$ be the discrete valuation that defines $|\cdot|$ on F. Then

(a) the image $|\overline{F}^\times|_{\overline{F}}$ equals the image $|F^\times|_F$, and $|\cdot|_{\overline{F}}$ on $\overline{F}$ is therefore defined by a discrete valuation $\bar{v}(\cdot)$ on $\overline{F}$ such that $\bar{v} \circ \iota = v$,
(b) the image $\iota(R)$ of the valuation ring R of v is dense in the valuation ring $\overline{R}$ of $\bar{v}$,
(c) for every integer $n > 0$, the image $\iota(P^n)$ of the n^{th} power P^n of the valuation ideal P of v is dense in the n^{th} power $\overline{P}^n$ of the valuation ideal $\overline{P}$ of $\bar{v}$,
(d) the residue class fields of F and $\overline{F}$ coincide in the sense that the mapping $\iota : R \to \overline{R}$ descends to a field isomorphism of R/P onto $\overline{R}/\overline{P}$,
(e) for every integer $n > 0$, the mapping $\iota : R \to \overline{R}$ descends to a ring isomorphism of R/P^n onto $\overline{R}/\overline{P}^n$,
(f) $\overline{R}$ is compact if R/P is finite, and in this case the topological field $\overline{F}$ is locally compact.

REMARK. No assertion is made in (d) and (e) about whether the topologies match under the constructed isomorphisms. Our interest will be mostly in the case that R/P is finite, in which case the topologies match because they are discrete.

PROOF. Write $|F^\times|_F$ in the form $r^{\mathbb{Z}}$ for a unique real number $r > 1$. For (a), since $|\iota(x)|_{\overline{F}} = |x|_F$ and since $\iota(F)$ is dense in $\overline{F}$, the continuity of the absolute value $|\cdot|_{\overline{F}}$ implies that the image of $\overline{F}^\times$ is contained in the closure of $r^{\mathbb{Z}}$ within the positive reals, which is $r^{\mathbb{Z}}$. The formula $\bar{v} \circ \iota = v$ follows from the computation $r^{-v(x)} = |x|_F = |\iota(x)|_{\overline{F}} = r^{-\bar{v}(\iota(x))}$ by taking the logarithm to the base r.

For (b) and (c), we use that $\iota(F)$ is dense in $\overline{F}$, and we treat (b) as the case $n = 0$ of (c). Fix $n \geq 0$ and consider $\overline{P}^n$. Choose a sequence $\{x_k\}$ in F with $\{\iota(x_k)\}$ converging to a point x in $\overline{P}^n$. Since $|x|_{\overline{F}} \leq r^{-n}$, we must have $|x_k|_F < r^{-n+1}$ for all sufficiently large k. The elements x_k satisfying this condition are in P^n, and thus $\iota(P^n)$ is dense in $\overline{P}^n$.

For (d) and (e), the mapping $R \to \overline{R}/\overline{P}^n$ descends to R/P^n, since $\iota(P) \subseteq \overline{P}$. The descended map is one-one, since if $x \in R$ maps to the 0 coset, then x is in $\iota^{-1}(\overline{P}^n) = P^n$. To see that the descended map is onto, let a coset $\bar{x} + \overline{P}^n$ be given. Since $\iota(R)$ is dense in $\overline{R}$, we can choose $x \in R$ with $|\iota(x) - \bar{x}|_{\overline{F}} < r^{-n}$. Since $\overline{P}^n = \{y \in \overline{F} \,|\, |y| < r^{-n+1}\}$, $\iota(x) - \bar{x}$ is in $\overline{P}^n$. Hence $\iota(x)$ is exhibited as in $\bar{x} + \overline{P}^n$, and the coset $x + P^n$ maps to the coset $\bar{x} + \overline{P}^n$.

In (f), Corollary 8.60 of *Basic Algebra* shows that P^n/P^{n+1} is a 1-dimensional vector space over R/P. The First Isomorphism Theorem gives an R module isomorphism $(R/P^{n+1})\big/(R/P^n) \cong P^n/P^{n+1}$, and it follows by induction on n that the finiteness of R/P implies the finiteness of R/P^n. In view of (e), $\overline{R}/\overline{P}^n$ is finite for every $n > 0$.

For each $n > 0$, the set $\overline{R}$ is covered by the cosets of $\overline{P}^n$, which are closed balls in $\overline{F}$ of radius r^{-n} and open balls of radius r^{-n+1}. Thus for any positive radius, there exists a finite collection of open balls of that radius or less such that the union of the open balls covers $\overline{R}$. This means that $\overline{R}$ is totally bounded in the metric space $\overline{F}$. A totally bounded closed subset of a complete metric space is compact, and consequently $\overline{R}$ is compact.

Thus the 0 element of $\overline{F}$ has $\overline{R}$ as a compact neighborhood. Since addition is continuous, each member x of $\overline{F}$ has $x + \overline{R}$ as a compact neighborhood of x, and therefore $\overline{F}$ is locally compact. □

Let us review briefly. We start with an absolute value on a field F. The cases of initial interest are that F is a number field or is a function field in one variable, namely a finite algebraic extension of a field $\Bbbk(X)$, where $\Bbbk$ is a given base field; in the latter case we assume that the absolute value is identically 1 on $\Bbbk^\times$. A number field can have archimedean absolute values, and we come

to them in a moment. In the function-field case we know that every absolute value is nonarchimedean if $\Bbbk$ has nonzero characteristic; this remains true for characteristic zero but we did not prove it. For our cases of interest the nonarchimedean nontrivial absolute values are always given by a discrete valuation.

Thus let us summarize what happens for a nonarchimedean nontrivial absolute value that is given by a discrete valuation. Within the given field F we have singled out a Dedekind domain R for which F is the field of fractions,[8] and the absolute value is ≤ 1 on R. For example, in the number-field case R is the ring of algebraic integers in F. In all cases the discrete valuation v is determined by a nonzero prime ideal $\mathfrak{p}$ of R, and the absolute value on F is given by $|x|_F = r^{-v(x)}$ for some number $r > 1$. Our two-step process consists in a step of localization and a step of completion. The step of localization passes to the principal ideal domain $S^{-1}R$ with maximal ideal $S^{-1}\mathfrak{p}$, where S is the complement of $\mathfrak{p}$ in R. The domain $S^{-1}R$ coincides with the valuation ring of v, and the ideal $S^{-1}\mathfrak{p}$ coincides with the valuation ideal of v. The absolute value on F does not change during this process of localization. The ideal $S^{-1}\mathfrak{p}$ is principal in $S^{-1}R$, say with π as a generator. The element π can be chosen to be in $\mathfrak{p}$, and it has $v(\pi) = 1$. Theorem 6.5 and Proposition 6.11 govern relationships between R and $S^{-1}R$. Briefly the powers of $\mathfrak{p}$ are dense in the powers of $S^{-1}\mathfrak{p}$, and the natural map of residue class fields $R/\mathfrak{p} \to S^{-1}R/S^{-1}\mathfrak{p}$ is a field isomorphism onto.

The second step is a step of completion with respect to the absolute value. The completion of a valued field $(F, |\cdot|_F)$ is a homomorphism of valued fields $\iota : (F, |\cdot|_F) \to (L, |\cdot|_L)$ such that $(L, |\cdot|_L)$ is complete as a metric space and ι carries F onto a dense subfield of L. This exists by Theorem 6.24. In the situation with a nonarchimedean nontrivial absolute value that is given by a discrete valuation, one often writes $F_\mathfrak{p}$ for the completed field L. The eventual interest is partly in what happens to R and $\mathfrak{p}$, but we first consider $S^{-1}R$ and $S^{-1}\mathfrak{p}$. The completed absolute value $|\cdot|_{F_\mathfrak{p}}$ is given by a discrete valuation $\bar{v}$ with $\bar{v} \circ \iota = v$. Let us write $R_\mathfrak{p}$ for its valuation ring and $\mathfrak{p}_\mathfrak{p}$ for its valuation ideal. Theorem 6.26 governs the relationships between $S^{-1}R$ and $R_\mathfrak{p}$. Briefly the images under ι of the powers of $S^{-1}\mathfrak{p}$ are dense in the powers of $\mathfrak{p}_\mathfrak{p}$, and the natural map of residue class fields $S^{-1}R/S^{-1}\mathfrak{p} \to R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$ induced by ι is a field isomorphism onto.

The case of most interest for number theory is the case of a number field F and the absolute value determined by a nonzero prime ideal $\mathfrak{p}$ in the ring of algebraic integers of F. The field $F_\mathfrak{p}$ is called the field of **$\mathfrak{p}$-adic numbers**, and the ring $R_\mathfrak{p}$ is called the ring of **$\mathfrak{p}$-adic integers**. When $F = \mathbb{Q}$ and $\mathfrak{p} = p\mathbb{Z}$ for a prime number p, the element π can be taken to be p.

[8]The case $R = F$ is excluded; this is the case that produces the trivial absolute value, which does not interest us.

In the case of a function field in one variable that is most analogous to a number field, one starts from a field F that is a finite algebraic extension of $\mathbb{F}_q(X)$, where $\mathbb{F}_q$ is a finite field with q elements. According to Corollary 6.22, all but finitely many of the nonarchimedean absolute values are defined in terms of nonzero prime ideals in the integral closure of $\mathbb{F}_q[X]$ in F; the others are the prime constituents of the ideal $X^{-1}\mathbb{F}_q[X^{-1}]$ in $\mathbb{F}_q[X^{-1}]$. One can show that the ring in the completion analogous to $R_{\mathfrak{p}}$ is always a **ring of formal power series** $\mathbb{F}_{q'}[[X]]$ in one indeterminate X and with coefficients in a finite extension $\mathbb{F}_{q'}$ of $\mathbb{F}_q$. Elements of this ring are arbitrary formal power series of the form $\sum_{k=0}^{\infty} c_k X^k$ with all c_k in $\mathbb{F}_{q'}$. The field of fractions analogous to $F_{\mathfrak{p}}$ is always a **field of formal Laurent series** $\mathbb{F}_q((X))$ in one indeterminate; nonzero elements of this field are arbitrary expressions of the form $\sum_{k=-N}^{\infty} c_k X^k$ with all c_k in $\mathbb{F}_{q'}$, with $c_{-N} \neq 0$, and with N depending on the element.

Let us now examine archimedean completions. We shall discuss what happens when we start from a number field, and then we make some remarks without proof about the general case. Thus let F be a number field, and let an archimedean absolute value be given on it. To have notation parallel to the nonarchimedean case, it is customary to index the absolute value[9] by a symbol like v, writing $|\cdot|_v$ for it. Corollary 6.16 shows that the restriction of $|\cdot|_v$ to $\mathbb{Q}$ is nontrivial, and the combination of Proposition 6.14 and Ostrowski's Theorem (Theorem 6.15) shows that the restriction to $\mathbb{Q}$ is equivalent to the ordinary absolute value. Adjusting $|\cdot|_v$ within its equivalence class, we may assume that its restriction to $\mathbb{Q}$ matches the ordinary absolute value. Using Theorem 6.24, we form the completion of F with respect to $|\cdot|_v$, writing F_v for the completed space. The limits of Cauchy sequences from $\mathbb{Q}$ itself show that $\mathbb{R}$ lies in the completed space, since $|\cdot|_v$ matches the ordinary absolute value on $\mathbb{Q}$. Thus we can regard $\mathbb{R}$ as a subfield of F_v, and F is a subfield as well. Consequently the set $\mathbb{R}F$ of sums of products is a subring of F_v. The multiplication mapping of $\mathbb{R} \times F$ into F_v is $\mathbb{Q}$ bilinear and has a linear extension $\mathbb{R} \otimes_{\mathbb{Q}} F \to F_v$ whose image is $\mathbb{R}F$. The $\mathbb{R}$ dimension of $\mathbb{R} \otimes_{\mathbb{Q}} F$ is $[F : \mathbb{Q}]$, and consequently the $\mathbb{R}$ dimension of $\mathbb{R}F$ is $\leq [F : \mathbb{Q}]$, hence finite. Being a finite-dimensional $\mathbb{R}$ algebra embedded in a field, $\mathbb{R}F$ is a subfield[10] of F_v. It is therefore a finite algebraic extension of $\mathbb{R}$ and must be $\mathbb{R}$ or $\mathbb{C}$. Thus F lies in $\mathbb{R}$ or $\mathbb{C}$. The fields $\mathbb{R}$ and $\mathbb{C}$ are complete relative to the ordinary absolute value, and hence $\mathbb{R}F$ is a closed subset of F_v. Since F is dense, we conclude that F_v is $\mathbb{R}$ or $\mathbb{C}$.

Visualize having a standard copy of $\mathbb{C}$ available, with $\mathbb{R}$ embedded in it. From the above remarks, any archimedean absolute value of the number field F, after

[9] Or the equivalence class of the absolute value.

[10] Within a field if a nonzero element is algebraic over a base field, then the smallest ring containing the base field and the element contains also the inverse of the element.

adjustment within its equivalence class, yields a completion that takes one of the two forms

$$\sigma : (F, |\cdot|_v) \to (\mathbb{R}, |\cdot|) \qquad \text{and} \qquad \sigma : (F, |\cdot|_v) \to (\mathbb{C}, |\cdot|),$$

where $|\cdot|$ is ordinary absolute value on $\mathbb{R}$ or $\mathbb{C}$. Conversely any field mapping σ of F into $\mathbb{R}$ or $\mathbb{C}$ has dense image either in $\mathbb{R}$ or in $\mathbb{C}$ and defines an archimedean absolute value on F by $|\cdot|_v = \sigma^*(|\cdot|)$. Then $\sigma : (F, |\cdot|_v) \to (\mathbb{R}$ or $\mathbb{C}, |\cdot|)$ is a completion by Theorem 6.25.

To classify the archimedean absolute values up to equivalence, we recall from Section V.2 that the number of distinct field maps σ into $\mathbb{C}$ of a number field F of degree $[F : \mathbb{Q}] = n$ is exactly n, with a certain number r_1 of them having image in $\mathbb{R}$ and with the remainder $2r_2$ having image in $\mathbb{C}$ but not $\mathbb{R}$ and occurring in complex conjugate pairs. Each such field map σ gives us a completion. The members of a complex conjugate pair result in the same absolute value on F when the ordinary absolute value of $\mathbb{C}$ is restricted to F. We shall show that there are no other equivalences.

Proposition 6.27. Let F be a number field with $[F : \mathbb{Q}] = n$, and let there be r_1 distinct field maps of F into $\mathbb{R}$ and r_2 complex conjugate pairs of distinct field maps of F into $\mathbb{C}$, with $r_1 + 2r_2 = n$. Each such field map σ induces an archimedean absolute value on F by restriction from $\mathbb{R}$ or $\mathbb{C}$, the only equivalences are the ones from pairs of field maps related by complex conjugation, and the resulting collection of $r_1 + r_2$ absolute values exhausts the archimedean absolute values on F, up to equivalence.

PROOF. The remarks above show everything except that these $r_1 + r_2$ absolute values are mutually inequivalent. To prove this fact, suppose that σ and σ' are two field maps of F into the same field, $\mathbb{R}$ or $\mathbb{C}$, such that $x \mapsto |\sigma(x)|$ is equivalent to $x \mapsto |\sigma'(x)|$. Then $\varphi = \sigma'\sigma^{-1}$ is a field isomorphism from image σ onto image σ' that respects the absolute value, up to a power. It is therefore uniformly continuous from image σ onto image σ'. Consequently φ extends to all of $\mathbb{R}$ or $\mathbb{C}$, and the continuous extension respects the field operations. On $\mathbb{Q}$, φ is the identity, and hence its continuous extension to $\mathbb{R}$ must be the identity. Thus the continuous extension is an automorphism of $\mathbb{R}$ or $\mathbb{C}$ that fixes $\mathbb{R}$, and consequently it must be the identity or complex conjugation. □

It is of some interest to know what archimedean absolute values can occur in other situations, besides number fields, and Theorem 6.24 shows that it is enough to classify the complete ones. Ostrowski did so, and the result is that $\mathbb{R}$ and $\mathbb{C}$, with their ordinary absolute values, are the only complete archimedean fields up to equivalence.[11]

[11] A proof of the Ostrowski result may be found in Hasse's *Number Theory*, pp. 191–194. Gelfand

5. Hensel's Lemma

Hensel's Lemma is a device that in its simplest forms allows one to solve polynomial equations in the field $\mathbb{Q}_p$ of p-adic numbers by using congruence information modulo some power of p. It has a number of distinct formulations, all of which work within any complete nonarchimedean valued field, not limited to $\mathbb{Q}_p$. We shall give a fairly simple formulation and obtain a handy special case as a corollary, using an adaptation of Newton's method of iterations in calculus for finding roots of polynomials. At the end of the section, we shall state without proof a version of Hensel's Lemma that works to factor polynomials rather than to find their roots. Yet another formulation of Hensel's Lemma, whose precise statement we omit, applies to systems of polynomial equations in several variables.

No overarching result of this chapter actually makes use of any version of Hensel's Lemma. Instead, versions of Hensel's Lemma are indispensable in analyzing the fine structure of complete valued fields and in handling examples. Thus the applications of Hensel's Lemma in this book will occur in the examples of this section and the next and also in problems at the end of the chapter. Problem 16 is one such problem.

Theorem 6.28 (Hensel's Lemma). Let F be a field with a nontrivial discrete absolute value $|\cdot|$, necessarily nonarchimedean, and assume that F is complete. Let R be the valuation ring, and let $f(X)$ be a polynomial in $R[X]$. Suppose that a_0 is a member of R such that

$$|f(a_0)| < |f'(a_0)|^2.$$

Then the sequence $\{a_n\}$ recursively given by

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$$

is well defined in R and converges to a root a of $f(X)$ that satisfies $|a - a_0| < 1$.

PROOF. Put $c = |f(a_0)|/|f'(a_0)|^2 < 1$. We prove the following three statements together by induction on n:

(i) a_n is well defined and is in R,
(ii) $|f'(a_n)| = |f'(a_0)| \neq 0$, and
(iii) $|f(a_n)|/|f'(a_n)| \leq c^{2^n}|f'(a_0)|$.

---

and Tornheim proved a more general result, with the same conclusion, that allows the multiplicative property of absolute values to be relaxed somewhat. A proof of this result appears in Artin's *Theory of Algebraic Numbers*, pp. 45–51.

The base case for the induction is the case $n = 0$, and the three statements are true by hypothesis in this case.

Assume that the three statements hold for n. From (ii), a_{n+1} is defined, and then (iii) shows that a_{n+1} satisfies

(iii′) $|a_{n+1} - a_n| = |f(a_n)|/|f'(a_n)| \le c^{2^n}|f'(a_0)|$.

The fact that a_n and $f'(a_0)$ are in R, in combination with (iii′), shows that a_{n+1} is in R. This proves (i) for $n + 1$.

For (ii) and (iii), we make use of the following Taylor expansions of $f(X)$ and $f'(X)$ about b:

$$f(X) = f(b) + (X - b)f'(b) + (X - b)^2 g(X) \qquad \text{with } g(X) \in R[X]$$

and

$$f'(X) = f'(b) + (X - b)h(X) \qquad \text{with } h(X) \in R[X].$$

To check that these expansions are valid in any characteristic, it is enough to check the first one, since the second one follows by differentiation. For the first one, it is enough to treat the special case X^k. Dividing $X^k - b^k$ by $X - b$, we see that we are to produce $g(X)$ such that

$$(X - b)g(X) = \sum_{j=0}^{k-1} b^{k-1-j}X^j - kb^{k-1} = \sum_{j=0}^{k-1} b^{k-1-j}(X^j - b^j).$$

Every term on the right side is divisible by $X - b$, and thus the quotient $g(X)$ is in $R[X]$.

Put $Q_n = a_{n+1} - a_n = -f(a_n)/f'(a_n)$. By (iii) for n, $|Q_n| \le |f'(a_n)|c^{2^n}$; in particular, $|Q_n| < |f'(a_n)|$. In the expansion of $f'(X)$, we take $b = a_n$ and evaluate at $X = a_{n+1}$ to obtain

$$f'(a_{n+1}) = f'(a_n) + Q_n h(a_{n+1}).$$

Since $|Q_n| < |f'(a_n)|$ and $|h(a_{n+1})| \le 1$, we see that $|f'(a_{n+1})| = |f'(a_n)|$. This proves (ii) for $n + 1$.

In the expansion of $f(X)$, we take $b = a_n$ and evaluate at $X = a_{n+1}$ to obtain

$$f(a_{n+1}) = f(a_n) + (a_{n+1} - a_n)f'(a_n) + (a_{n+1} - a_n)^2 g(a_{n+1}).$$

But $(a_{n+1} - a_n)f'(a_n) = -f(a_n)$, and hence this equation simplifies to

$$f(a_{n+1}) = Q_n^2 g(a_{n+1}).$$

Since $g(a_{n+1})$ is in R, application of (iii) for n and (ii) for $n+1$ gives

$$\frac{|f(a_{n+1})|}{|f'(a_{n+1})|^2} = \frac{|Q_n|^2|g(a_{n+1})|}{|f'(a_n)|^2} \le \Big(\frac{|f(a_n)|}{|f'(a_n)|^2}\Big)^2 \le (c^{2^n})^2 = c^{2^{n+1}},$$

and this proves (iii) for $n+1$. This completes the induction.

Now we can prove the theorem. If $n < m$, then (iii′) and the ultrametric inequality imply that

$$|a_m - a_n| \le \max_{n\le k<m} |a_{k+1} - a_k| \le |f'(a_0)| \max_{n\le k<m} c^{2^k} \le |f'(a_0)|c^{2^n}. \qquad (*)$$

Consequently $\{a_n\}$ is a Cauchy sequence. Let a be its limit. Substituting into the definition of a_{n+1}, using (ii), and passing to the limit, we obtain $a = a - f(a)/f'(a)$. Thus $f(a) = 0$. Taking $n = 0$ in $(*)$ and letting m tend to infinity gives $|a - a_0| \le |f'(a_0)|c$, and this is $\le c < 1$ because $f'(a_0)$ is in R. □

Corollary 6.29 (Hensel's Lemma). Let F be a field with a nontrivial discrete absolute value, necessarily nonarchimedean, and assume that F is complete. Let R be the valuation ring, let $\mathfrak{p}$ be the unique maximal ideal, and let $f(X)$ be a polynomial in $R[X]$. If $\overline{f}(X)$ is the reduced polynomial with coefficients in $R/\mathfrak{p}$ and if $\bar{a}$ is a simple root of $\overline{f}(X)$, then $f(X)$ has a simple root $a \in R$ whose image in $R/\mathfrak{p}$ is $\bar{a}$.

PROOF. Let a_0 be any member of R whose image in $R/\mathfrak{p}$ is $\bar{a}$. The assumptions imply that $f(a_0)$ is in $\mathfrak{p}$ and that $f'(a_0)$ is in R but not $\mathfrak{p}$. Thus the hypotheses of Theorem 6.28 are satisfied, and the theorem produces a root a of $f(X)$ with $a - a_0$ in $\mathfrak{p}$. □

EXAMPLES WITH $F = \mathbb{Q}_p$ AND $R = \mathbb{Z}_p$.

(1) Suppose that p is an odd prime and that n is an integer for which the Legendre symbol $\left(\frac{n}{p}\right)$ is $+1$, i.e., for which $\mathrm{GCD}(n, p) = 1$ and n has a square root modulo p. Then n has a square root in $\mathbb{Z}_p$. This is immediate from Corollary 6.29 with $f(X) = X^2 - n$.

(2) Suppose that $p = 2$ and that n is an integer[12] having the form $8k + 1$. The maximal ideal in $\mathbb{Z}_2$ is (2). Corollary 6.29 is not applicable to $f(X) = X^2 - n$, since evaluation of the derivative $f'(X) = 2X$ at any point of $\mathbb{Z}_2$ leads to a member of the ideal (2). However, we can apply Theorem 6.28. Let $a_0 = 1$, so that $f(a_0) = 1 - n$ and $f'(a_0) = 2$. The theorem produces a root a in $\mathbb{Z}_2$ if $|1 - n|_2/|2|_2^2 < 1$, i.e., if $|1 - n|_2 < \frac{1}{4}$. Since $|1 - n|_2 = |-8k|_2 = \frac{1}{8}|k|_2 < \frac{1}{4}$, the theorem indeed applies. The resulting root a in $\mathbb{Z}_2$ has $a \equiv 1 \bmod (2)$.

[12] In fact, n could be a 2-adic integer in this argument.

(3) Suppose that $p > 3$. Every nonzero residue $\bar{a}$ in $\mathbb{Z}/p\mathbb{Z}$ has $\bar{a}^{p-1} \equiv 1 \bmod p$. Corollary 6.29 shows immediately that the polynomial $X^{p-1} - 1$ has a root a whose image in $\mathbb{Z}_p/p\mathbb{Z}_p$ is $\bar{a}$. Since the elements $\bar{a}$ are distinct, we conclude that $\mathbb{Z}_p$ contains all $p-1$ of the $(p-1)^{\text{st}}$ root of unity.

(4) As promised at the beginning of Section 4, we show that $\mathbb{Q}_p$ for $p = 5$ is obtained also by completing the field $\mathbb{Q}(i)$ with respect to a certain absolute value and that in fact there are two distinct equivalence classes of absolute values on $\mathbb{Q}(i)$ for which $\mathbb{Q}_5$ results. Thus let $F = \mathbb{Q}$, $K = \mathbb{Q}(i)$, and $\mathfrak{p} = (5)$. The prime factorization of $(5)\mathbb{Z}[i]$ is as $(2+i)(2-i)$. If we put $P_1 = (2+i)$ and $P_2 = (2-i)$, then K_{P_1} and K_{P_2} are both equal to $\mathbb{Q}_5$ because Example 1 above shows that the square roots of -1 already appear in $\mathbb{Q}_5$. If a is one of the square roots, then $\big|2+a\big|_5 \big|2-a\big|_5 = \big|(2+a)(2-a)\big|_5 = |5|_5 = \frac{1}{5}$. Thus one of $\big|2+a\big|_5$ and $\big|2-a\big|_5$ equals $\frac{1}{5}$ and the other equals 1. What is happening is that there are two field mappings $\mathbb{Q}(i) \to \mathbb{Q}_5$. For each of them, the effect on the base field $\mathbb{Q}$ is the same; however, one field mapping sends i in $\mathbb{Q}(i)$ to a in $\mathbb{Q}_5$, and the other sends i to $-a$. For definiteness, let us say that $\big|2+a\big|_5 = \frac{1}{5}$. Then the valuation of $\mathbb{Q}(i)$ with respect to $P_1 = (2+i)$ is consistent with the 5-adic valuation of $\mathbb{Q}_5$, but the valuation of $P_2 = (2-i)$ is not. This example shows why the definition of completion insists on a mapping of valued fields (respecting absolute values), not merely a mapping of fields.

(5) Suppose that $p = 2$. The question is the prime factorization of $f(X) = X^3 + X^2 - 2X + 8$ in $\mathbb{Z}_2$. This polynomial was studied at length toward the end of Section V.4 in connection with common index divisors. It is irreducible over $\mathbb{Q}$, but we are to factor it over $\mathbb{Q}_2$. We shall show that it splits into first-degree factors. Considering the polynomial modulo 2, we find that $f(X) \equiv (X-1)X^2 \bmod 2$. Since 1 is a simple root modulo 2, Corollary 6.29 says that there exists an element θ_1 in $\mathbb{Z}_2$ such that $f(\theta_1) = 0$ and $\theta_1 \equiv 1 \bmod 2$. Dividing $f(X)$ by $X - \theta_1$, we obtain

$$f(X) = (X-\theta_1)\big(X^2 + (\theta_1+1)X + (\theta_1(\theta_1+1) - 2)\big).$$

To show that the quadratic factor splits over $\mathbb{Q}_2$, it is necessary and sufficient to show that its discriminant is a square, since $\mathbb{Q}_2$ has characteristic 0. The discriminant is

$$(\theta_1+1)^2 - 4(\theta_1(\theta_1+1) - 2) = 4\big((\tfrac{1}{2}(\theta_1+1))^2 - (\theta_1(\theta_1+1) - 2)\big),$$

and we can ignore the square factor of 4. We know that $\theta_1 \equiv 1 \bmod 2$. Let us compute θ_1 modulo $8\mathbb{Z}_2$ by writing $\theta_1 = 8\varphi + c$ with $\varphi \in \mathbb{Z}_2$ and with $c = \pm 1$ or ± 3. Substituting into $f(X)$ and computing modulo $8\mathbb{Z}_2$, we have

$$0 = f(\theta_1) \equiv c^3 + c^2 - 2c \bmod 8\mathbb{Z}_2.$$

Since c is odd, $c^3 \equiv c$ and $c^2 \equiv 1 \bmod 8$. Thus $0 \equiv c + 1 - 2c \bmod 8$ and $c \equiv 1 \bmod 8$. Consequently

$$(\tfrac{1}{2}(\theta_1 + 1))^2 - (\theta_1(\theta_1 + 1) - 2) \equiv 1 \bmod 8.$$

By Example 2 any 2-adic integer that is $\equiv 1 \bmod 8\mathbb{Z}_2$ is a square in $\mathbb{Z}_2$, and thus $f(X)$ indeed factors over $\mathbb{Z}_2$ as the product of three first-degree factors.

We conclude this section with a version of Hensel's Lemma that we state without proof.[13] This version deals with factorizations rather than roots. Briefly it says that we can lift a *relatively prime* factorization modulo $\mathfrak{p}$ to a factorization in $R[X]$ if at least one of the two factors modulo $\mathfrak{p}$ has leading coefficient 1. This theorem certainly implies Corollary 6.29.

Theorem 6.30 (Hensel's Lemma). Let F be a field with a nontrivial discrete absolute value, necessarily nonarchimedean, and assume that F is complete. Let R be the valuation ring, let $\mathfrak{p}$ be the unique maximal ideal, let $\Bbbk$ be the residue class field, and let $f(X)$ be a polynomial in $R[X]$. Suppose that there exist polynomials $g_0(X)$ and $h_0(X)$ in $R[X]$ such that $g_0(X) \bmod \mathfrak{p}$ and $h_0(X) \bmod \mathfrak{p}$ are relatively prime in $\Bbbk[X]$, g_0 has leading coefficient 1, and $f(X)$ factors modulo $\mathfrak{p}$ as $f(X) \equiv g_0(X)h_0(X) \bmod \mathfrak{p}$. Then there exist polynomials $g(X)$ and $h(X)$ in $R[X]$ such that $g(X)$ has leading coefficient 1, $g(X) \equiv g_0(X) \bmod \mathfrak{p}$, $h(X) \equiv h_0(X) \bmod \mathfrak{p}$, and $f(X)$ factors in $R(X)$ as $f(X) = g(X)h(X)$.

6. Ramification Indices and Residue Class Degrees

Sections 1–4 have presented the ingredients of a two-stage process for analyzing congruence information, and now it is time to use everything together. The goal is to have techniques for extracting information about a global number-theoretic problem by seeing what the problem says about ideals, for reducing the questions about ideals to questions about powers of prime ideals, and for then assembling the results.

We give one illustration of the utility of our constructions: With the techniques we had in Chapter V, we gave only a partial proof of the Dedekind Discriminant Theorem (Theorem 5.5). By contrast, we shall see in Section 8 that the present techniques lead naturally to a complete proof.

Although we might want to work just within one number field, it is helpful to change the context so that we are comparing a number field with a finite extension. There is no loss of generality in doing so; we can always take the base field to

[13] A proof may be found in Hasse's *Number Theory*, pp. 169–172.

be the rationals $\mathbb{Q}$, and the effect is that we consider only the finite set of prime ideals for the extension field that contain a given prime number p.

As long as we are going to consider finite extensions of fields in addressing number theory, we might as well treat also the case of function fields in one variable, at least to the extent that the two theories are quite analogous. Thus we are led to the following set-up.

Let R be a Dedekind domain considered as a subring of its field of fractions F, let K be a finite *separable*[14] extension of F with $[K : F] = n$, and let T be the integral closure of R in K. We shall work with F and K as valued fields, having some absolute value on them. The case of interest in this section will be that the absolute value is nonarchimedean and arises from a discrete valuation whose valuation ring contains R or T, respectively. Theorem 6.5 shows that the valuation is defined by means of some prime ideal $\wp$ of R or T, and the associated absolute value may thus be denoted by an expression[15] like $|\cdot|_\wp$.

We start from a prime ideal $\mathfrak{p}$ in R and form the corresponding absolute value on F as in Section 3, obtaining a valued field $(F, |\cdot|_\mathfrak{p})$. Then we complete as in Section 4, writing the completion as

$$\psi_0 : (F, |\cdot|_\mathfrak{p}) \to (F_\mathfrak{p}, |\cdot|_\mathfrak{p}).$$

We know that the ideal $\mathfrak{p}T$ in T has a prime factorization of the form $\mathfrak{p}T = P_1^{e_1} \cdots P_g^{e_g}$, where $P_1, \ldots, P_g$ are distinct prime ideals in T. The integers e_i are called **ramification indices** and the dimensions $f_i = \dim_{R/\mathfrak{p}}(T/P_i)$ are called **residue class degrees**. We are interested in saying everything we can about $P_1, \ldots, P_g$ and about the indices e_i and f_i. The fundamental relationship is given by Theorem 9.60 of *Basic Algebra*, namely

$$\sum_{i=1}^{g} e_i f_i = n.$$

We know that each P_i gives us a nonarchimedean absolute value $|\cdot|_{P_i}$ on K, unique up to equivalence, and then a completion

$$\psi_i : (K, |\cdot|_{P_i}) \to (K_{P_i}, |\cdot|_{P_i}).$$

[14]The role of separability will become apparent before the statement of Theorem 6.31 below.

[15]The number-theory case ultimately requires also a limited amount of analysis of archimedean absolute values, and that will be carried out in Section 9. In the context of passing from a Diophantine equation to congruence information, part of the role that archimedean absolute values play is in analyzing signs. Thus for example the simple-minded equation $x^2 + y^2 = -1$ has no solutions in integers; the reason for the absence of solutions is a constraint on signs, not some limitation from congruences with respect to powers of primes. Archimedean absolute values control signs.

The first important step is to establish an isomorphism involving fields such that the identity $\sum_{i=1}^{g} e_i f_i = n$ is a dimension formula that follows from the isomorphism. The identity in question concerns the ring $K \otimes_F F_{\mathfrak{p}}$, which is a commutative algebra over K or over $F_{\mathfrak{p}}$, whichever we like, and which is semisimple by Corollary 2.30 under our assumption that K is a finite separable extension of $\mathbb{F}$. The Wedderburn theory (Theorems 2.2 and 2.4) shows that $K \otimes_F F_{\mathfrak{p}}$ is isomorphic to a finite direct product of fields,[16] each of which is a finite extension of $F_{\mathfrak{p}}$. What we shall prove later in this section is the following theorem.

Theorem 6.31. Let R be a Dedekind domain considered as a subring of its field of fractions F, let K be a finite separable extension of F with $[K : F] = n$, and let T be the integral closure of R in K. If $\mathfrak{p}$ is a nonzero prime ideal of R and if the ideal $\mathfrak{p}T$ in T has a prime factorization of the form $\mathfrak{p}T = P_1^{e_1} \cdots P_g^{e_g}$, where $P_1, \ldots, P_g$ are distinct prime ideals in T and the e_j are positive integers, then

$$K \otimes_F F_{\mathfrak{p}} \cong \prod_{j=1}^{g} K_{P_j}.$$

When the formula $\sum_{j=1}^{g} e_j f_j = n$ is specialized to the field extension $K_{P_j}/F_{\mathfrak{p}}$, it becomes $e_j^* f_j^* = [K_{P_j} : F_{\mathfrak{p}}]$, where e_j^* and f_j^* are the ramification index and residue class degree associated to $K_{P_j}/F_{\mathfrak{p}}$. If we accept for the moment the result of Lemma 6.36 below that e_j^* and f_j^* coincide with the corresponding indices e_j and f_j for K/F, then $n = \sum_{j=1}^{g} e_j f_j = \sum_{j=1}^{n} e_j^* f_j^* = \sum_{j=1}^{g} [K_{P_j} : F_{\mathfrak{p}}]$ indeed counts the $F_{\mathfrak{p}}$ dimensions of both sides of the formula $K \otimes_F F_{\mathfrak{p}} \cong \prod_{j=1}^{g} K_{P_j}$ in the theorem. The theorem says much more than this, and we shall mine its consequences after giving the proof of the theorem.

For orientation, let us recall Example 4 from Section 5. In that example, we had $R = \mathbb{Z}$, $F = \mathbb{Q}$, $K = \mathbb{Q}(i)$, $T = \mathbb{Z}[i]$, $\mathfrak{p} = 5\mathbb{Z}$, and $F_{\mathfrak{p}} = \mathbb{Q}_5$. The factorization $\mathfrak{p}T = \prod P_j^{e_j}$ is $5\mathbb{Z}[i] = (2+i)(2-i)$, and the two completed versions of K are $K_{(2+i)} \cong \mathbb{Q}_5$ and $K_{(2-i)} \cong \mathbb{Q}_5$. Thus the identity in the theorem specializes to

$$\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}_5 \cong \mathbb{Q}_5 \times \mathbb{Q}_5.$$

Proving the identity on this level would be more challenging than necessary because the isomorphism cannot be unique; it can always be composed with the interchange of the two factors on the right side. For this reason the proof makes use of valued fields, and then in effect the desired isomorphism becomes a constructive one that we can write down rather explicitly.

[16] The words "direct product" in connection with finitely many fields refer to the direct sum of the additive structures, with multiplication given coordinate by coordinate.

Let us now work toward proving Theorem 6.31. Above, we mentioned the completion mapping ψ_0 for F relative to an absolute value in the equivalence class determined by $\mathfrak{p}$, as well as ψ_j for K relative to some absolute value in the class determined by P_j. In addition, we have inclusion mappings corresponding to the field extensions K/F and $K_{P_j}/F_{\mathfrak{p}}$. Figure 6.1 below is a square diagram that assigns the names φ_0 and φ_j to these as well.

$$\begin{array}{ccc} F & \xrightarrow{\psi_0} & F_{\mathfrak{p}} \\ {\scriptstyle\varphi_0}\downarrow & & \downarrow{\scriptstyle\varphi_j} \\ K & \xrightarrow{\psi_j} & K_{P_j} \end{array}$$

FIGURE 6.1. Commutativity of completion and extension as field mappings.

The diagram in Figure 6.1 commutes. In fact, $\psi_j\varphi_0$ and $\varphi_j\psi_0$ are both F homomorphisms, being compositions of F homomorphisms, and hence $x \in F$ implies $\psi_j\varphi(x) = x(\psi_j\varphi(1)) = x(1) = x(\varphi_j\psi_0(1)) = \varphi_j\psi_0(x)$.

But more is true: we are going to impose absolute values on the four fields in the diagram in such a way that the four field mappings are homomorphisms of valued fields. We have already defined $|\cdot|_{\mathfrak{p}}$ on F as any absolute value corresponding to $\mathfrak{p}$, and then $|\cdot|_{\mathfrak{p}}$ is defined on $F_{\mathfrak{p}}$ in such a way that the completion mapping ψ_0 preserves absolute values. Theorem 6.33 below will enable us to define an absolute value in a unique fashion on K_{P_j} such that φ_j preserves absolute values. Proposition 6.34 will give us the definition of an absolute value on K, and we shall check in Lemma 6.35 that Figure 6.1 with these absolute values in place is a commutative diagram of valued fields. Finally we use this commutativity to prove in Lemma 6.36 that the ramification index e_j^* and residue class degree f_j^* for $K_{P_j}/F_{\mathfrak{p}}$ match the corresponding parameters e_j and f_j for K/F, and then we are ready for the main part of the proof of the theorem.

We begin our preliminary work by limiting the possibilities for a finite extension of a complete valued field $(F, |\cdot|_F)$. If K is a finite extension of F, a **norm** on the F vector space K relative to $|\cdot|_F$ is a function $\|\cdot\|$ from K to $\mathbb{R}$ having

(i) $\|x\| \geq 0$ on K with equality if and only if $x = 0$,
(ii) $\|cx\| = |c|_F\|x\|$ for $c \in F$ and $x \in K$,
(iii) $\|x + y\| \leq \|x\| + \|y\|$ for all x and y in K.

Lemma 6.32. If $(F, |\cdot|_F)$ is a complete valued field, if K is a finite extension of F, and if $\|\cdot\|_1$ and $\|\cdot\|_2$ are any two norms on K relative to $|\cdot|_F$, then there exist real constants C and C' such that

$$\|x\|_1 \leq C\|x\|_2 \quad \text{and} \quad \|x\|_2 \leq C'\|x\|_1 \qquad \text{for all } x \in K.$$

Consequently K is Cauchy complete in the metric induced by either norm.

REMARK. It is not important that K be a field in this lemma, only that it be a finite-dimensional vector space over F.

PROOF. Let $n = \dim_F K$. Fixing an ordered basis $(x_1, \ldots, x_n)$ of K over F, we may express any member x of K in the form $x = \sum_{i=1}^n c_i x_i$ with all c_i in F. With the c_i's defined this way, we define $\|x\|_{\sup} = \max_{1\le i\le n} |c_i|_F$. To prove the displayed inequalities, it is enough to prove them for $\|\cdot\|_{\sup}$ and any other norm $\|\cdot\|$. For one direction of the inequality, we have

$$\|x\| = \Big\| \textstyle\sum_i c_i x_i \Big\| \le \sum_i \|c_i x_i\| = \sum_i |c_i|_F \|x_i\| \le \big(\sum_i \|x_i\|\big)\|x\|_{\sup}.$$

This proves that $\|x\| \le C\|x\|_{\sup}$ with $C = \sum_i \|x_i\|$.

For the reverse inequality we shall prove by induction on k that an inequality $\|x\|_{\sup} \le C'_k\|x\|$ holds for all x in the F linear span of at most k of the vectors $x_1, \ldots, x_n$. The base case for the induction is $k = 1$, and then $\|x\|_{\sup} = \|x_i\|^{-1}\|x\|$ whenever x is a multiple of x_i. So $C'_1 = \max_{1\le i\le n}(\|x_i\|^{-1})$.

Assume that $C'_1, \ldots, C'_k$ exist and that we are to produce C'_{k+1}. Arguing by contradiction, we may assume that there is some sequence $\{x^{(m)}\}$ in K, each term having at most $k+1$ nonzero coefficients, such that $\|x^{(m)}\| = 1$ for all m and $\|x^{(m)}\|_{\sup}$ tends to infinity. Possibly by passing to a subsequence, we may assume that the nonzero coefficients of $x^{(m)}$ all lie in a particular subset of $k+1$ of the coefficients, and there is no harm in assuming that this subset is $\{1, \ldots, k+1\}$. Passing to a further subsequence, we may assume that there is some index j such that the largest coefficient of each $x^{(m)}$, when measured by $|\cdot|_F$, is the j^{th}, and there is no harm in assuming that $j = k+1$.

Let $c_1^{(m)}, \ldots, c_{k+1}^{(m)}$ be the coefficients of $x^{(m)}$, so that $x^{(m)} = \sum_{i=1}^{k+1} c_i^{(m)} x_i$. Put $y^{(m)} = (c_{k+1}^{(m)})^{-1} x^{(m)} = \sum_{i=1}^k d_i^{(m)} x_i + x_{k+1}$, where $d_i^{(m)} = (c_{k+1}^{(m)})^{-1} c_i^{(m)}$. Here $|d_i^{(m)}|_F \le 1$ for $1 \le i \le k$ and for all m, and also $\|y^{(m)}\| = |c_{k+1}^{(m)}|_F^{-1}\|x^{(m)}\| = |c_{k+1}^{(m)}|_F^{-1}$ tends to 0.

For each vector $y^{(m)} - x_{k+1}$, only the first k coefficients can be nonzero, and the same thing is true of differences $y^{(m)} - y^{(m')}$ of two such vectors. The inductive hypothesis tells us that $\|y^{(m)} - y^{(m')}\|_{\sup} \le C'_k\|y^{(m)} - y^{(m')}\|$, and the right side tends to 0 as m and m' tend to infinity because $\|y^{(m)}\|$ and $\|y^{(m')}\|$ tend to 0. Therefore the i^{th} coordinate of $y^{(m)}$ forms a Cauchy sequence. Since F is given as complete, $\{y^{(m)}\}$ is convergent in the norm $\|\cdot\|_{\sup}$ to some $y = \sum_{i=1}^k d_i x_i + x_{k+1}$ in K.

By the easy direction of our inequality, $\|y^{(m)} - y\| \le C\|y^{(m)} - y\|_{\sup}$. The right side tends to 0, and hence so does the left. We know that $\|y^{(m)}\|$ tends to 0, and hence $y = 0$. But this conclusion contradicts the form of y as $\sum_{i=1}^k d_i x_i + x_{k+1}$ with coefficient 1 for x_{k+1}. We conclude that C'_{k+1} exists as asserted, and the lemma follows. □

Theorem 6.33. If $(F, |\cdot|_F)$ is a complete valued field relative to a nontrivial nonarchimedean discrete absolute value and if K is a finite separable extension of F with $[K : F] = n$, then K has a unique absolute value $|\cdot|_K$ extending $|\cdot|_F$, K is complete and nonarchimedean, and the integral closure T in K of the valuation ring R of F is the valuation ring of K. The extension is given by $|x|_K = |N_{K/F}(x)|_F^{1/n}$.

REMARKS. Since T is the valuation ring, Proposition 6.2 shows that T has a unique nonzero prime ideal. It follows that if $\mathfrak{p}$ is a nonzero prime ideal of R, then $\mathfrak{p}T = P^e$ for a single prime ideal P of T. We shall make frequent use of this fact in applications without explicit mention.

PROOF. For uniqueness, suppose that $|\cdot|_1$ and $|\cdot|_2$ are two absolute values on K that extend $|\cdot|_F$. Let us see that each of these is a norm on K relative to $|\cdot|_F$. In fact, what needs checking for $|\cdot|_1$ is that the function respects scalars from F appropriately. If c is in F and x_0 is in K, then $|cx_0|_1 = |c|_1|x_0|_1 = |c|_F|x_0|_1$, the second equality following because $|\cdot|_1$ restricts to $|\cdot|_F$ on F. A similar argument applies to $|\cdot|_2$, and thus we are dealing with two norms.

If the two given absolute values are inequivalent, then Proposition 6.12 shows in the presence of the nontriviality of $|\cdot|_F$ that we can find an $x \in K$ with $|x|_1 > 1$ and $|x|_2 \le 1$. Then $\lim_k |x^{-k}|_1 = 0$ while $|x^{-k}|_2 \ge 1$ for all k. Consequently there cannot exist a constant C such that $|y|_2 \le C|y|_1$ for all $y \in F$, in contradiction to Lemma 6.32.

We conclude that $|\cdot|_1$ and $|\cdot|_2$ are equivalent, say that $|x|_1 = |x|_2^s$ for all $x \in K$ and some $s > 0$. Since $|\cdot|_F$ is nontrivial, there exists some $x_0 \in F$ with $|x_0|_1 > 1$. The equality $|x_0|_1 = |x_0|_2^s$ then implies that $s = 1$. This proves uniqueness.

We turn to existence. Proposition 6.2 shows that the valuation ring R in F for the discrete valuation v_F corresponding to $|\cdot|_F$ on F is a local principal ideal domain and that the valuation ideal $\mathfrak{p}$ is the unique maximal ideal of R. Theorem 6.5 shows that the valuation $v_\mathfrak{p}$ determined by $\mathfrak{p}$ is the same as the given valuation v_F. Hence $|\cdot|_F$ is given for all $a \in F$ by $|a|_F = r^{-v_\mathfrak{p}(a)}$ for some $r > 1$. Let π be a generator of the principal ideal $\mathfrak{p}$ of R.

Since K/F is finite and separable, Theorem 8.54 of *Basic Algebra* shows that the integral closure T of R in K is a Dedekind domain. Let $\mathfrak{p}T = P_1^{e_1} \cdots P_g^{e_g}$ be the factorization of the ideal $\mathfrak{p}T$ of T into the product of powers of distinct prime ideals of T. Each P_j defines a nonarchimedean valuation v_{P_j} of K. If a is any element of F, then we can write $a = \pi^k u$ for some $u \in R^\times$ and some integer k. The computation $aT = aRT = \pi^k uRT = \pi^k RT = \pi^k T = \mathfrak{p}^k T = P_1^{ke_1} \cdots P_g^{ke_g}$ shows that $v_\mathfrak{p}(a) = k$ and that $v_{P_j}(a) = ke_j$. Hence $v_{P_j} = e_j v_\mathfrak{p}$ on F, and therefore the formula $|x|_{P_j} = (r^{e_j^{-1}})^{-v_{P_j}(x)}$ for $x \in K$ defines an absolute

value on K that has $|a|_F = r^{-v_{\mathfrak{p}}(a)} = r^{-e_j^{-1}v_{P_j}(a)} = (r^{e_j^{-1}})^{-v_{P_j}(a)} = |a|_{P_j}$ for all a in F. This proves existence. The absolute value $|\cdot|_{P_j}$ on K is complete by Lemma 6.32 and is nonarchimedean because it is given by a discrete valuation.

Let us show that $g = 1$. Arguing by contradiction, suppose that there are at least two distinct prime ideals P_1 and P_2 of T that contain $\mathfrak{p}$. Since $P_1 + P_2 = T$, we can choose $x_1 \in P_1$ and $x_2 \in P_2$ with $x_1 + x_2 = 1$. Then $v_{P_1}(x_1) > 0$ and $v_{P_1}(1) = 0$, from which we see that $v_{P_1}(x_2) = 0$. Since $v_{P_2}(x_2) > 0$, we obtain a contradiction to the uniqueness part of the theorem. Thus the prime ideal of T is unique. Let us write P for this ideal.

We know that $v_P(T) \geq 0$, i.e., that T is contained in the valuation ring of v_P. Proposition 6.4 shows that the valuation ring of v_P equals $S^{-1}T$, where S is the complement of P in T. The uniqueness of P means that T is local, and hence every member of S is a unit in T. Thus $S^{-1}T = T$, and T is the valuation ring.

Write $|\cdot|_K$ in place of $|\cdot|_{P_j}$. To prove the explicit formula for $|\cdot|_K$ in the statement of the proposition, choose a finite Galois extension L of F that contains K; such a field L exists because K/F is separable.[17] By the existence just proved, let $|\cdot|_L$ be an extension of $|\cdot|_K$ to L. If σ is in $\mathrm{Gal}(L/F)$, then $x \mapsto |\sigma(x)|_L$ and $x \mapsto |x|_L$ are both absolute values on L that extend $|\cdot|_F$. By the uniqueness just proved, $|\sigma(x)|_L = |x|_L$. Applying $|\cdot|_L$ to both sides of the formula $N_{L/F}(x) = \prod_{\sigma \in \mathrm{Gal}(L/F)} \sigma(x)$ gives

$$|N_{L/F}(x)|_F = |N_{L/F}(x)|_L = \prod_{\sigma \in \mathrm{Gal}(L/F)} |\sigma(x)|_L = |x|_L^{[L:F]}. \tag{$*$}$$

If x is in K, then the left side equals $(|N_{K/F}(x)|_F)^{[L:K]}$, and the right side equals $(|x|_K)^{[L:K][K:F]} = (|x|_K^{[K:F]})^{[L:K]}$. Thus the desired formula follows by extracting the positive $[L:K]^{\text{th}}$ root of both sides of $(*)$. □

Proposition 6.34. Under the hypotheses of Theorem 6.31, let $v_{\mathfrak{p}}$ be the valuation of F defined by $\mathfrak{p}$, and let v_{P_j} be the valuation of K defined by P_j, $1 \leq j \leq g$. Then $e_j v_{\mathfrak{p}} = v_{P_j}\big|_F$. Consequently if $|\cdot|_{\mathfrak{p}}$ is an absolute value on F defined by $\mathfrak{p}$, then for each j some member $|\cdot|_{P_j}$ of the equivalence class of absolute values defined on K by P_j is an extension of $|\cdot|_{\mathfrak{p}}$. In this case the inclusion of $(F, |\cdot|_{\mathfrak{p}})$ into $(K, |\cdot|_{P_j})$ is a homomorphism of valued fields.

PROOF. Let S be the multiplicative system in R given as the set-theoretic complement of $\mathfrak{p}$ in R. For the first conclusion Proposition 6.4 and Theorem 6.5 together show that it is enough to prove that

$$e_j v_{S^{-1}\mathfrak{p}} = v_{S^{-1}P_j}\big|_F. \tag{$*$}$$

[17] The field L can be taken to be a splitting field of the minimal polynomial over F of an element ξ such that $K = F(\xi)$. The extension L/F is separable by Corollary 9.30 of *Basic Algebra*.

From the identity

$$\mathfrak{p}T = P_1^{e_1} \cdots P_g^{e_g},$$

we have

$$S^{-1}\mathfrak{p}T = (S^{-1}P_1)^{e_1} \cdots (S^{-1}P_g)^{e_g}. \tag{$**$}$$

Since S is the complement of $\mathfrak{p}$ in R, $v_\mathfrak{p}$ is 0 on S. Hence $v_{S^{-1}\mathfrak{p}}$ is 0 on S. From $R \cap P_j = \mathfrak{p}$, we have $S \cap P_j \subseteq S \cap \mathfrak{p} = \varnothing$. Thus the members of S lie in $R \subseteq T$ but in no P_j, and v_{P_j} is 0 on S. Hence $v_{S^{-1}P_j}$ is 0 on S.

Let π be a generator of the principal ideal $S^{-1}\mathfrak{p}$ in $S^{-1}R$, so that $v_{S^{-1}\mathfrak{p}}(\pi) = 1$. Since $\pi S^{-1}T = S^{-1}\mathfrak{p}T$, equation $(**)$ shows that $v_{S^{-1}P_j}(\pi) = e_j$. Each element y of F is of the form $y = \pi^k u$ for some integer k and some $u \in F$ with $v_{S^{-1}\mathfrak{p}}(u) = 0$. The element u must be in $S^{-1}R$ but not $S^{-1}\mathfrak{p}$ and hence is in S^{-1}. Thus $v_{S^{-1}P_j}(u) = 0$. We have now seen that $v_{S^{-1}P_j}(x) = e_j v_{S^{-1}\mathfrak{p}}(x)$ for the element $x = u$ above and also for $x = \pi$. Therefore $v_{S^{-1}P_j}(x) = e_j v_{S^{-1}\mathfrak{p}}(x)$ for all $x \in F$, and $(*)$ is proved.

Now that $e_j v_\mathfrak{p} = v_{P_j}\big|_F$, choose $r > 1$ such that $|x|_\mathfrak{p} = r^{-v_\mathfrak{p}(x)}$ for $x \in F$. If r' is defined by $r = (r')^{e_j}$, then the definition $|x|_{P_j} = (r')^{-v_{P_j}(x)}$ for $x \in K$ restricts for $x \in F$ to $|x|_{P_j} = (r')^{-v_{P_j}(x)} = (r')^{-e_j v_\mathfrak{p}(x)} = r^{-v_\mathfrak{p}(x)} = |x|_\mathfrak{p}$, and the inclusion is indeed a homomorphism of valued fields. □

With these facts in place, let us make Figure 6.1 into a commutative diagram of valued fields. From $\mathfrak{p}$, we use any corresponding choice of $|\cdot|_\mathfrak{p}$ on F, and this uniquely determines an absolute value by the same name on $F_\mathfrak{p}$. Next we apply Theorem 6.33 to the inclusion $\varphi_j : F_\mathfrak{p} \to K_{P_j}$ to obtain a unique extension of $|\cdot|_\mathfrak{p}$ from $F_\mathfrak{p}$ to an absolute value $|\cdot|_{P_j}$ on K_{P_j}.

Meanwhile, with the index j specified, Proposition 6.34 gives us a unique absolute value $|\cdot|_{P_j}$ on K such that the inclusion $\varphi_0 : F \to K$ is a homomorphism of valued fields. The completion mapping $\psi_j : K \to K_{P_j}$ in turn gives us a second determination of $|\cdot|_{P_j}$ on K_{P_j}, and Lemma 6.35 below says that these two determinations match, i.e., that Figure 6.2 is a commutative diagram of homomorphisms of valued fields.

$$\begin{array}{ccc} (F, |\cdot|_\mathfrak{p}) & \xrightarrow{\psi_0} & (F_\mathfrak{p}, |\cdot|_\mathfrak{p}) \\ \Big\downarrow{\scriptstyle \varphi_0} & & \Big\downarrow{\scriptstyle \varphi_j} \\ (K, |\cdot|_{P_j}) & \xrightarrow{\psi_j} & (K_{P_j}, |\cdot|_{P_j}) \end{array}$$

FIGURE 6.2. Commutativity of completion and extension as homomorphisms of valued fields.

Lemma 6.35. In the above notation the two determinations of $|\cdot|_{P_j}$ on K_{P_j} coincide—one by using Theorem 6.33 to insist that $\varphi_j\psi_0$ in Figure 6.2 be the composition of homomorphisms of valued fields, and the other by using Proposition 6.34 to insist that $\psi_j\varphi_0$ in Figure 6.2 be the composition of homomorphisms of valued fields.

REMARKS. The commutativity formula $\psi_j\varphi_0 = \varphi_j\psi_0$ for field mappings is known from the discussion concerning Figure 6.1.

PROOF. Let us give two different names to the two possible absolute values on K_{P_j}, writing $|\cdot|'$ for the one that makes $|\psi_j(k)|' = |k|_{P_j}$ for $k \in K$ and writing $|\cdot|''$ for the other, which makes $|\varphi_j(x)|'' = |x|_{\mathfrak{p}}$ for $x \in F_{\mathfrak{p}}$. Let y be in F. Then the equality $\varphi_j\psi_0 = \psi_j\varphi_0$ implies that

$$|\varphi_j\psi_0(y)|' = |\psi_j\varphi_0(y)|' = |\varphi_0(y)|_{P_j} = |y|_{\mathfrak{p}} = |\psi_0(y)|_{\mathfrak{p}}. \tag{$*$}$$

If x_0 is given in $F_{\mathfrak{p}}$, then we can choose a sequence $\{x_n\}$ in F with $\{\psi_0(x_n)\}$ convergent to x_0 in $F_{\mathfrak{p}}$. Then $\{\psi_0(x_n)\}$ is Cauchy in the metric on $F_{\mathfrak{p}}$, and it follows from $(*)$ applied with $y = x_n - x_{n'}$ that $\{\varphi_j\psi_0(x_n)\}$ is Cauchy in the metric from $|\cdot|'$ on K_{P_j}. If we have a second such sequence $\{x_n'\}$ in F with $\psi_0(x_n')$ convergent to x_0 and if we alternate the terms of $\{x_n\}$ and $\{x_n'\}$ to produce a sequence $\{z_n\}$, then $\{\varphi_j\psi_0(z_n)\}$ remains Cauchy in the metric from $|\cdot|'$. Since $|\cdot|'$ is complete, it follows that $|\varphi_j(x_0)|'$ is given by a well-defined limit independently of the sequence in $\psi_0(F)$ used to approximate x_0. The formula $(*)$ shows that $|\varphi_j(x_0)|' = |x_0|_{\mathfrak{p}}$, and the definition of $|\cdot|''$ shows that this equals $|\varphi_j(x_0)|''$. By the uniqueness in Theorem 6.33, $|\cdot|' = |\cdot|''$ on K_{P_j}. □

Lemma 6.36. In the above notation and that of Theorem 6.31, the ramification index e_j^* corresponding to $K_{P_j}/F_{\mathfrak{p}}$ for the closure of the ideal $\psi_j(P_j)$ coincides with the ramification index e_j corresponding to K/F for the ideal P_j.

REMARK. In addition, the residue class degree f_j^* for $K_{P_j}/F_{\mathfrak{p}}$ coincides with the residue class degree f_j for K/F. In fact, the five paragraphs of review that follow Theorem 6.26 mention that residue class fields change neither during the localization step nor in the completion step of our two-step process. Thus $R/\mathfrak{p}$ remains the same during the two steps, and so does T/P_j. Hence the dimension of T/P_j as a vector space over $R/\mathfrak{p}$ remains the same.

PROOF. Let $v_{\mathfrak{p},F}$, $v_{P_j,K}$, $v_{\mathfrak{p},F_{\mathfrak{p}}}$, and $v_{P_j,K_{P_j}}$ be the valuations corresponding to the absolute values on F, K, $F_{\mathfrak{p}}$, and K_{P_j}, respectively. The last of these is well defined by Lemma 6.35. Proposition 6.34 shows that

$$e_j v_{\mathfrak{p},F} = v_{P_j,K}\varphi_0 \qquad \text{and} \qquad e_j^* v_{\mathfrak{p},F_{\mathfrak{p}}} = v_{P_j,K_{P_j}}\varphi_j. \tag{$*$}$$

Meanwhile, the completion mappings ψ_0 and ψ_j satisfy

$$v_{\mathfrak{p},F_{\mathfrak{p}}}\psi_0 = v_{\mathfrak{p},F} \qquad \text{and} \qquad v_{P_j,K_{P_j}}\psi_j = v_{P_j,K}. \tag{$**$}$$

Multiplying the second equation of $(*)$ on the right by ψ_0 and substituting from the first equation of $(**)$, we obtain

$$e_j^* v_{\mathfrak{p},F} = e_j^* v_{\mathfrak{p},F_{\mathfrak{p}}}\psi_0 = v_{P_j,K_{P_j}}\varphi_j\psi_0.$$

We substitute from the commutativity formula $\varphi_j\psi_0 = \psi_j\varphi_0$ and unwind the right side as

$$v_{P_j,K_{P_j}}\psi_j\varphi_0 = v_{P_j,K}\varphi_0 = e_j v_{\mathfrak{p},F}.$$

Thus $e_j^* v_{\mathfrak{p},F} = e_j v_{\mathfrak{p},F}$. Since $v_{\mathfrak{p},F}$ is not identically 0, we obtain $e_j^* = e_j$. □

PROOF OF THEOREM 6.31. As was mentioned before the statement of the theorem, it follows from Proposition 2.29 and the Wedderburn theory that $K \otimes_F F_{\mathfrak{p}}$ is isomorphic to a product $\prod_{i=1}^{g'} L_i$ of fields, each of which is a finite extension of $F_{\mathfrak{p}}$ and each of which has K embedded in it. The subfields L_i are uniquely determined within $K \otimes_F F_{\mathfrak{p}}$, and we let η_i be the projection of $K \otimes_F F_{\mathfrak{p}}$ onto L_i. Each η_i is a ring homomorphism and is given by multiplication by a specific element of $K \otimes_F F_{\mathfrak{p}}$, namely the element that is 1 in the i^{th} position and is 0 in the other positions. When restricted to $K \otimes 1$, η_i gives a field map $\alpha_i : K \to L_i$; when restricted to $1 \otimes F_{\mathfrak{p}}$, it gives a field map $\beta_i : F_{\mathfrak{p}} \to L_i$.

We shall develop a small abstract theory about these field maps α_i and β_i. Suppose that M is a field containing F, that $\alpha : K \to M$ and $\beta : F_{\mathfrak{p}} \to M$ are F algebra homomorphisms, and that M is a finite separable extension of $\beta(F_{\mathfrak{p}})$. Theorem 6.33 says that M has a unique absolute value $|\cdot|_{\mathfrak{p},\beta}$ extending $|\cdot|_{\mathfrak{p}}$ and that the valued field $(M, |\cdot|_{\mathfrak{p},\beta})$ is complete. The extension property means that $\beta : (F_{\mathfrak{p}}, |\cdot|_{\mathfrak{p}}) \to (M, |\cdot|_{\mathfrak{p},\beta})$ is a homomorphism of valued fields. The restriction $\alpha^*(|\cdot|_{\mathfrak{p},\beta})$ to K makes $(K, \alpha^*(|\cdot|_{\mathfrak{p},\beta}))$ into a valued field in such a way that

$$\alpha : (K, \alpha^*(|\cdot|_{\mathfrak{p},\beta})) \to (M, |\cdot|_{\mathfrak{p},\beta}) \tag{$*$}$$

is a homomorphism of valued fields. Let us see that

$$\alpha^*(|\cdot|_{\mathfrak{p},\beta}) \text{ is one (and only one) of the absolute values } |\cdot|_{P_j} \text{ on } K \tag{$**$}$$

and that α in $(*)$ factors as the composition of the completion mapping

$$\psi_j : (K, |\cdot|_{P_j}) \to (K_{P_j}, |\cdot|_{P_j})$$

followed by some other homomorphism of valued fields

$$\iota : (K_{P_j}, |\cdot|_{P_j}) \to (M, |\cdot|_{\mathfrak{p},\beta}).$$

To get at $(**)$ and the factorization of α, let us show that the field mapping

$$\varphi_0 : (F, |\cdot|_{\mathfrak{p}}) \to (K, \alpha^*(|\cdot|_{\mathfrak{p},\beta})) \tag{$\dagger$}$$

is a homomorphism of valued fields, i.e., that $\varphi_0^*\alpha^*(|\cdot|_{\mathfrak{p},\beta}) = |\cdot|_{\mathfrak{p}}$. The field mappings $\alpha\varphi_0$ and $\beta\psi_0$, which carry F into M via K and $F_{\mathfrak{p}}$, respectively, are compositions of F homomorphisms and hence are F homomorphisms. Therefore $x \in F$ implies that $\alpha\varphi_0(x) = x(\alpha\varphi_0(1)) = x(1) = x(\beta\psi_0(1)) = \beta\psi_0(x)$, and we see that $\alpha\varphi_0 = \beta\psi_0$ on F. For $x \in F$, this identity accounts for the third equality in the following computation proving $(\dagger)$:

$$\begin{aligned} |x|_{\mathfrak{p}} &= |\psi_0 x|_{\mathfrak{p}} = |\beta\psi_0 x|_{\mathfrak{p},\beta} \\ &= |\alpha\varphi_0 x|_{\mathfrak{p},\beta} = \alpha^*(|\cdot|_{\mathfrak{p},\beta})(\varphi_0 x) = \varphi_0^*\alpha^*(|\cdot|_{\mathfrak{p},\beta})(x). \end{aligned}$$

Returning to $(**)$ and applying $(\dagger)$, we see that $\alpha^*(|\cdot|_{\mathfrak{p},\beta})$ is ≤ 1 on R. Since T is the integral closure of R, Proposition 6.20 shows that $\alpha^*(|\cdot|_{\mathfrak{p},\beta})$ is ≤ 1 on T and that it arises from some nonzero prime ideal of T, necessarily one of the ideals $P_1, \dots, P_g$. This proves $(**)$. Then the factorization $(*)$ follows from $(**)$ and the universal mapping property of completions as given in Theorem 6.25, since $(M, |\cdot|_{\mathfrak{p},\beta})$ is complete.

Now let us specialize by taking $M = L_i$ with i fixed. As in the first paragraph of the proof, the projection $\eta_i : K \otimes_F F_{\mathfrak{p}} \to L_i$ gives us field mappings $\alpha_i : K \to L_i$ and $\beta_i : F_{\mathfrak{p}} \to L_i$ by composing η_i with $K \to K \otimes 1$ and with $F_{\mathfrak{p}} \to 1 \otimes F_{\mathfrak{p}}$. If $u_1, \dots, u_n$ is a vector-space basis of K over F, then $u_1 \otimes 1, \dots, u_n \otimes 1$ is a vector-space basis of $K \otimes_F F_{\mathfrak{p}}$ over $F_{\mathfrak{p}}$, and it follows that L_i is finite-dimensional over $F_{\mathfrak{p}}$. Let us check that L_i is separable over $F_{\mathfrak{p}}$. We are given that K is separable over F, hence that $K = F(\xi)$ for an element ξ whose minimal polynomial $g(X)$ over F is separable. Then $\xi \otimes 1$ is a root of $g(X)$ regarded as in $F_{\mathfrak{p}}[X]$, and so is $\eta_i(\xi \otimes 1)$. Therefore $L_i/F_{\mathfrak{p}}$ is separable, and the above theory is applicable. In the theory, L_i acquires an absolute value $|\cdot|_{\mathfrak{p},\beta_i}$ such that $\beta_i : (F_{\mathfrak{p}}, |\cdot|_{\mathfrak{p}}) \to (L_i, |\cdot|_{\mathfrak{p},\beta_i})$ is a homomorphism of valued fields, and then $(L_i, |\cdot|_{\mathfrak{p},\beta_i})$ is complete. The theory produces a unique index $j = j(i)$ making $\alpha_i : (K, |\cdot|_{P_j}) \to (L_i, |\cdot|_{\mathfrak{p},\beta_i})$ into a homomorphism of valued fields.

Let us see that $\alpha_i(K)$ is dense in L_i. Every member of L_i is the image under η_i of some member $\sum_{l=1}^n u_l \otimes c_l$ of $K \otimes_F F_{\mathfrak{p}}$ with each c_l in $F_{\mathfrak{p}}$. The computation

$$\eta_i(u_l \otimes c_l) = \eta_i(u_l \otimes 1)\eta_i(1 \otimes c_l) = \alpha_i(u_l)\beta_i(c_l)$$

shows that every member of L_i is of the form $\sum_{l=1}^n \alpha_i(u_l)\beta_i(c_l)$. Since F is dense in $F_\mathfrak{p}$, we can choose members c_l' of F as close as we please to c_l. Since β_i is isometric, $\sum_{l=1}^n \alpha_i(u_l)\beta_i(c_l)$ is then close to $\sum_{l=1}^n \alpha_i(u_l)\beta_i(c_l') = \sum_{l=1}^n \alpha_i(c_l'u_l)$. Consequently $\alpha_i(K)$ is indeed dense in L_i.

Recall in connection with $(*)$ that $\alpha_i : K \to L_i$ factors as a composition of homomorphisms of valued fields, namely as $\psi_j : (K, |\cdot|_{P_j}) \to (K_{P_j}, |\cdot|_{P_j})$ followed by $\iota : (K_{P_j}, |\cdot|_{P_j}) \to (L_i, |\cdot|_{\mathfrak{p},\beta_i})$. Since K_{P_j} is complete, $\iota(K_{P_j})$ is closed in L_i. The dense image $\alpha_i(K) = \iota(\psi_j(K))$ in L_i is contained in the closed subset $\iota(K_{P_j})$, and it follows that ι is onto L_i. That is, the homomorphism of valued fields

$$\iota : (K_{P_j}, |\cdot|_{P_j}) \to (L_i, |\cdot|_{\mathfrak{p},\beta_i})$$

is an isomorphism. This identifies the valued field $(L_i, |\cdot|_{\mathfrak{p},\beta_i})$ as isomorphic to $(K_{P_j}, |\cdot|_{P_j})$.

As a consequence of the argument thus far, we have constructed a choice-free function $i \mapsto j(i)$ carrying $\{1, \dots, g'\}$ into $\{1, \dots, g\}$. The function has the property that $K_{P_{j(i)}}$ is isomorphic as a valued field to L_i for each i. We are going to show that $i \mapsto j(i)$ is onto $\{1, \dots, g\}$. Thus let the completion homomorphism $\psi_j : (K, |\cdot|_{P_j}) \to (K_{P_j}, |\cdot|_{P_j})$ be given.

The F bilinear mapping $(\psi_j, \varphi_j) : K \times F_\mathfrak{p} \to K_{P_j}$ given by multiplication has a linear extension

$$\psi_j \otimes \varphi_j : K \otimes_F F_\mathfrak{p} \to K_{P_j}$$

that is a ring homomorphism. The range K_{P_j} is a field that is finite-dimensional over $\varphi_j(F_\mathfrak{p})$, and the image of $\psi_j \otimes \varphi_j$ is a $\varphi_j(F_\mathfrak{p})$ vector subspace of K_{P_j} that is closed under multiplication. Consequently the image of $\psi_j \otimes \varphi_j$ is closed under inverses[18] and is a field. The kernel of $\psi_j \otimes \varphi_j$ is therefore a maximal ideal, and it follows that there exists some i such that $\psi_j \otimes \varphi_j$ factors as a composition of $\eta_i : K \otimes_F F_\mathfrak{p} \to L_i$ followed by a field map $\gamma : L_i \to K_{P_j}$.

Having constructed a particular L_i, let us form α_i, β_i, and $P_{j(i)}$ as in the abstract theory with M. The map $\beta_i : (F_\mathfrak{p}, |\cdot|_\mathfrak{p}) \to (L_i, |\cdot|_{\mathfrak{p},\beta_i})$ is a homomorphism of valued fields such that $\gamma\beta_i = \varphi_j$, and the map $\alpha_i : (K, |, \cdot|_{P_{j(i)}}) \to (L_i, |\cdot|_{\mathfrak{p},\beta_i})$ is a homomorphism of valued fields such that $\gamma\alpha_i = \psi_j$. The existence part of Theorem 6.33 shows that there exists an absolute value $|\cdot|_\gamma$ on K_{P_j} such that $\gamma : (L_i, |\cdot|_{\mathfrak{p},\beta_i}) \to (K_{P_j}, |\cdot|_\gamma)$ is a homomorphism of valued fields. Since $\varphi_j^*(|\cdot|_{P_j}) = |\cdot|_\mathfrak{p} = \beta_i^*(|\cdot|_{\mathfrak{p},\beta_i}) = \beta_i^*\gamma^*(|\cdot|_\gamma) = \varphi_j^*(|\cdot|_\gamma))$, the uniqueness

[18]The same argument applies here with $F_\mathfrak{p}$ as was used in Section 4 with $\mathbb{R}$: within a field if a nonzero element is algebraic over a base field, then the smallest ring containing the base field and the element contains also the inverse of the element.

part of Theorem 6.33 shows that $|\cdot|_\gamma = |\cdot|_{P_j}$ on K_{P_j}. Meanwhile, the equality $\psi_j = \gamma\alpha_i$ implies that $\psi_j^* = \alpha_i^*\gamma^*$. Then we have

$$\begin{aligned}
\big(|\cdot|_{P_j} \text{ on } K\big) &= \psi_j^*\big(|\cdot|_{P_j} \text{ on } K_{P_j}\big) \\
&= \alpha_i^*\gamma^*\big(|\cdot|_{P_j} \text{ on } K_{P_j}\big) \qquad \text{since } \psi_j^* = \alpha_i^*\gamma^* \\
&= \alpha_i^*\gamma^*\big(|\cdot|_{\gamma} \text{ on } K_{P_j}\big) \qquad \text{since } |\cdot|_\gamma = |\cdot|_{P_j} \\
&= \alpha_i^*\big(|\cdot|_{\mathfrak{p},\beta_i} \text{ on } L_i\big) \\
&= \big(|,\cdot|_{P_{j(i)}}) \text{ on } K\big).
\end{aligned}$$

Therefore $j = j(i)$, and the map $i \mapsto j(i)$ is onto.

To complete the proof, let us compute dimensions relative to $F_\mathfrak{p}$, starting from the decomposition into fields L_i. The ramification index e_j^* and the residue class degree f_j^* for the valuation ring and ideal of K_{P_j} equal the corresponding parameters e_j and f_j for T and P_j, by Lemma 6.36. Thus we have

$$\begin{aligned}
n &= \sum_{i=1}^{g'} \dim_{F_\mathfrak{p}} L_i = \sum_{i=1}^{g'} \dim_{F_\mathfrak{p}} K_{P_{j(i)}} = \sum_{j=1}^{g} \sum_{j(i)=j} \dim_{F_\mathfrak{p}} K_{P_{j(i)}} \\
&= \sum_{j=1}^{g} \sum_{j(i)=j} e_{j(i)}^* f_{j(i)}^* = \sum_{j=1}^{g} \sum_{j(i)=j} e_{j(i)} f_{j(i)} = \sum_{j=1}^{g} |\{i \mid j(i)=j\}|\, e_j f_j.
\end{aligned}$$

On the other hand, we know that $n = \sum_j e_j f_j$, and we have just proved that $|\{i \mid j(i) = j\}| \geq 1$ for each j. It follows that $|\{i \mid j(i) = j\}| = 1$ for each j, i.e., that the function $i \mapsto j(i)$ is one-one onto. In particular, $g' = g$. The theorem follows. □

Notationally what is happening in the proof of the theorem is that a function $i \mapsto j(i)$ is constructed such that $\alpha_i : K \to L_i$ factors as $\alpha_i = \iota\psi_{j(i)}$ for some canonical isomorphism $\iota : K_{P_{j(i)}} \to L_i$ of complete valued fields. Renumbering the factors and ignoring canonical isomorphisms, we find that $K \otimes_F F_\mathfrak{p}$ is the direct product of the factors K_{P_i} and that $\alpha_i = \psi_i$ carries K to $K \otimes 1$ and then to the i^{th} factor K_{P_i}. Any linear mapping of the form $A \otimes 1$ in effect is therefore block diagonal with each block corresponding to the effect on some K_{P_i}.

Let us apply these considerations to operations "left-multiplication-by," which we write as $l(\cdot)$. If ξ is a member of K, the characteristic polynomial of $l(\xi)$ over F is $\det(X1 - l(\xi))$, and the characteristic polynomial of $l(\xi) \otimes 1$ over $F_\mathfrak{p}$ is still $\det(X1 - l(\xi))$, but now with its coefficients from F regarded as members of $F_\mathfrak{p}$ via the inclusion $\psi_0 : F \to F_\mathfrak{p}$.

The linear function $X(1 \otimes 1) - l(\xi) \otimes 1$ is block diagonal, equal to $X1 - l(\psi_i(\xi))$ on the i^{th} block for $1 \leq i \leq g$. The characteristic polynomial

$\det(X1 - l(\xi))$, regarded as having coefficients in $F_\mathfrak{p}$, is therefore the product of the g characteristic polynomials $X1 - l(\psi_i(\xi))$, each with coefficients in $F_\mathfrak{p}$. In turn, this product formula yields a sum formula for the trace $\mathrm{Tr}_{K/F}(\xi)$ and a product formula for the norm $N_{K/F}(\xi)$. If ξ is a primitive element for the extension K/F, then we can say even more. Let us write all these consequences as a corollary.

Corollary 6.37. Let R be a Dedekind domain regarded as a subring of its field of fractions F, let K be a finite separable extension of F with $[K : F] = n$, and let T be the integral closure of R in K. Let $\mathfrak{p}$ be a nonzero prime ideal of R, and let the ideal $\mathfrak{p}T$ in T have a prime factorization of the form $\mathfrak{p}T = P_1^{e_1} \cdots P_g^{e_g}$, where $P_1, \ldots, P_g$ are distinct prime ideals in T and $e_1, \ldots, e_g$ are positive. For $1 \le i \le g$, let $f_i = [T/P_i : R/\mathfrak{p}]$. If ξ is *any* element of K, then

(a) the F linear map $l(\xi)$ on K given by left multiplication by ξ has the property that its field polynomial $\det(X - l(\xi))$ over F, when reinterpreted as having coefficients in $F_\mathfrak{p}$, factors over $F_\mathfrak{p}$ as the product

$$\det(X - l(\xi)) = \prod_{i=1}^{g} \det(X - l(\xi_i))$$

of the g field polynomials of the images $\xi_i = \psi_i(\xi)$ under the completion map $\psi_i : K \to K_{P_i}$,

(b) $N_{K/F}(\xi) = \prod_{i=1}^{g} N_{K_{P_i}/F_\mathfrak{p}}(\xi_i)$,

(c) $\mathrm{Tr}_{K/F}(\xi) = \sum_{i=1}^{g} \mathrm{Tr}_{K_{P_i}/F_\mathfrak{p}}(\xi_i)$.

Furthermore, if ξ and F together generate K, if $m(X)$ is the minimal polynomial of ξ over F, and if $m(X) = \prod_{j=1}^{g'} m_j(X)$ expresses $m(X)$ as the product of distinct monic irreducible polynomials in $F_\mathfrak{p}[X]$, then

(d) $g' = g$,

(e) there is a one-one onto function $i \mapsto k(i)$ on the set $\{1, \ldots, g\}$ such that K_{P_i} is isomorphic as a field to $F_\mathfrak{p}[X]/(m_{k(i)}(X))$,

(f) $\deg m_{k(i)}(X) = e_i f_i$.

PROOF. Conclusion (a) was proved in the paragraph before the statement of the corollary, and (b) and (c) follow immediately from (a).

Under the assumption that $K = F(\xi)$, the minimal polynomial $m(X)$ of ξ and the characteristic polynomial $\det(X1 - l(\xi))$ are equal; thus $m(X) = \det(X - l(\xi))$ is irreducible over F. Applying Proposition 2.29a, we see that $K \otimes_F F_\mathfrak{p} \cong F_\mathfrak{p}[X]/(m(X))$ as an $F_\mathfrak{p}$ algebra. The assumed separability of K/F means that $m(X)$ is a separable polynomial, and $m(X)$ therefore factors over the extension field $F_\mathfrak{p}$ of F as a product of distinct monic irreducible polynomials

in $F_{\mathfrak{p}}[X]$, say as $m(X) = m_1(X) \cdots m_{g'}(X)$. The Chinese Remainder Theorem implies that

$$K \otimes_F F_{\mathfrak{p}} \cong \prod_{i=1}^{g'} F_{\mathfrak{p}}[X]/(m_i(X)),$$

and each $F_{\mathfrak{p}}[X]/(m_i(X))$ is a field. The factors on the right must coincide with the factors in Theorem 6.31, and it follows that $g' = g$ and that each K_{P_i} is of the form $F_{\mathfrak{p}}[X]/(m_k(X))$ for some $k = k(i)$. This proves (d) and (e). For (f), $\deg m_{k(i)}(X)$ is the product of the ramification index and the residue class degree for $K_{P_i}/F_{\mathfrak{p}}$, and this product equals $e_i f_i$ as a consequence of Lemma 6.36 and its remark. □

A by-product of (d) is that we obtain a way of computing g for the extension: it is the number of irreducible factors into which $m(X)$ splits when it is factored over $F_{\mathfrak{p}}$ instead of F. Hensel's Lemma in the form of Theorem 6.30 can help with carrying out this factorization in favorable cases if ξ is chosen to be integral over R, i.e., to be in T. Namely we reduce the coefficients of $m(X)$ modulo $\mathfrak{p}$, obtaining a monic polynomial in $(R/\mathfrak{p})[X]$, and we factor this polynomial[19] as a product of powers of distinct primes in $(R/\mathfrak{p})[X]$. Since the powers of distinct primes are relatively prime and since everything is monic, Theorem 6.30 is applicable and allows us to lift the factorization to $F_{\mathfrak{p}}[X]$. The resulting monic factors in $F_{\mathfrak{p}}[X]$ may not be irreducible in unfavorable circumstances,[20] but we have at least made progress.

Theorem 6.31 has accomplished even more than is stated in Corollary 6.37. For each i, it has identified a field extension, namely $K_{P_i}/F_{\mathfrak{p}}$, in which the indices e_i and f_i are isolated from the other e_j's and f_j's. Under an additional hypothesis on the residue class field (it is enough to assume that the residue class field is finite), Proposition 6.38 below shows that it is possible to interpolate a unique intermediate field L with $F_{\mathfrak{p}} \subseteq L \subseteq K_{P_i}$ such that the residue class degree (the parameter f) of K_{P_i}/L is 1 and the ramification index (the parameter e) of $K/F_{\mathfrak{p}}$ is 1. Thus the proposition says that we can separate e_i and f_i from each other. One says that K_{P_i}/L is **totally ramified** and $L/F_{\mathfrak{p}}$ is **unramified**.

Proposition 6.38. Let F be a complete valued field under a nonarchimedean discrete valuation v, let R and $\mathfrak{p}$ be the valuation ring and valuation ideal for v, let K be a finite separable extension of F of degree n, let T be the integral closure of R in K, and let P be the unique maximal ideal in T as in Theorem 6.33. Suppose

[19] On a computer, for example, if $R/\mathfrak{p}$ is finite.

[20] In Example 5 in the previous section, the given polynomial in $\mathbb{Z}[X]$ is $m(X) = X^3+X^2-2X+8$, and the reduced polynomial in $\mathbb{F}_2[X]$ is $X^2(X+1)$. Theorem 6.30 exhibits a factorization of $m(X)$ over $\mathbb{Z}_2[X]$ as the product of a linear factor and a quadratic factor, and we saw in Example 5 of Section 5 that the quadratic factor is reducible over $\mathbb{Z}_2[X]$.

that $R/\mathfrak{p}$ is a finite field. Let e be the integer such that $\mathfrak{p}T = P^e$, and let f be the dimension of T/P over $R/\mathfrak{p}$. Then there exists a unique intermediate field L for which the integral closure U of R in L and the unique maximal ideal $\wp$ in U have the following properties:

(a) $\mathfrak{p}U = \wp$ and $\wp T = P^e$,
(b) $[U/\wp : R/\mathfrak{p}] = f$ and $[T/P : U/\wp] = 1$.

The proof is carried out in Problems 15–16 at the end of the chapter. We shall apply Proposition 6.38 in Section 8. The intermediate field L in the proposition is called the **inertia subfield** of K/F.

Once this separation of an extension of a complete valued field into a totally ramified extension and an unramified extension has been accomplished, one can go on to study each kind of extension separately, in order to find out what kind of ramification is possible. The results are stated as Lemmas 6.47 and 6.48, and proofs are carried out in Problems 17–19 at the end of the chapter.

7. Special Features of Galois Extensions

In this section we analyze what happens in the setting of Theorem 6.31 when the extension of fields is a Galois extension. For simplicity for the moment, let us work with the number-field setting, even though analogous results hold for function fields in one variable as well. Thus let K/F be a finite *Galois* extension of number fields, let T and R be the rings of algebraic integers in K and F respectively, and let $\mathfrak{p}$ be a nonzero prime ideal in R. Since the extension K/F is Galois, the Galois group $\mathrm{Gal}(K/F)$ permutes transitively the nonzero prime ideals containing $\mathfrak{p}T$, and the factorization of $\mathfrak{p}T$ into powers of distinct prime ideals of T takes the special form $\mathfrak{p}T = P_1^e \cdots P_g^e$ with all the exponents the same.[21] In addition, the dimension of each finite field T/P_i over $R/\mathfrak{p}$ is an integer f independent of i, and we have $efg = [K : F]$.

Let us review Theorem 9.64 and its surrounding discussion in *Basic Algebra*. If we write P for one of the ideals P_i, then the subgroup G_P of $G = \mathrm{Gal}(K/F)$ is called the **decomposition group** at P. Each $\sigma \in G_P$ descends to an automorphism $\overline{\sigma}$ of T/P that fixes $R/\mathfrak{p}$, thereby yielding a member of $\overline{G} = \mathrm{Gal}((T/P)/(R/\mathfrak{p}))$. The map $G \to \overline{G}$ is certainly a homomorphism, and Theorem 9.64 of *Basic Algebra* says that it is onto. It follows that this homomorphism is e-to-1. In *Basic Algebra* this homomorphism was of interest when $F = \mathbb{Q}$ and $e = 1$, since it ensures the presence of certain kinds of permutations in G and makes it possible to determine G completely in certain circumstances.

[21] Lemma 9.61 and Theorem 9.62 of *Basic Algebra*.

Theorem 6.31 allows us to isolate each prime ideal P in such an analysis, reinterpreting everything in the context of a particular $\mathfrak{p}$-adic field. Carrying through this process gives insights into the decomposition group and the nature of the homomorphism $G_P \to \overline{G}$. The point of this section is to explain some of these insights.

We work within the setting of Theorem 6.31 except that we assume that the residue class fields are finite fields, as they are in the number-theory context. Thus let R be a Dedekind domain regarded as a subring of its field of fractions F, let K be a finite *Galois* extension of F with $[K : F] = n$, and let T be the integral closure of R in K. We suppose that $\mathfrak{p}$ is a nonzero prime ideal of R and that $R/\mathfrak{p}$ is a finite field. Let $\mathfrak{p}T = P_1^e \cdots P_g^e$ be the prime factorization of the ideal $\mathfrak{p}T$ in T; here $P_1, \ldots, P_g$ are assumed to be distinct prime ideals in T. Let f be the common value of the dimension of T/P_i over R/P.

In the decomposition $K \otimes_F F_{\mathfrak{p}} \cong \prod_{i=1}^g K_{P_i}$ of Theorem 6.31, the projection η_i to the i^{th} factor on the right side is a member of $K \otimes_F F_{\mathfrak{p}}$; specifically it is the member of the direct product whose i^{th} coordinate is the multiplicative identity of K_{P_i} and whose other coordinates are 0. The element η_i is an **idempotent** in the sense that $\eta_i^2 = \eta_i$, and the η_i's are **orthogonal** in the sense that $\eta_i \eta_j = 0$ for $i \neq j$. The only idempotents of $K \otimes_F F_{\mathfrak{p}}$ are the sums of distinct elements η_i, and the η_i's are distinguished from the other idempotents in being **primitive**: η_i is not the sum of two nonzero orthogonal idempotents.

Recall the relationship derived in the proof of Theorem 6.31 between P_i and the element η_i: the mapping $\beta_i : F_{\mathfrak{p}} \to K_{P_i}$ given by $\beta_i(x) = (1 \otimes x)\eta_i$ for $x \in F_{\mathfrak{p}}$ is a homomorphism of valued fields, and so is the mapping $\alpha_i : K \to K_{P_i}$ given by $\alpha_i(k) = (k \otimes 1)\eta_i$ for $k \in K$. These facts uniquely determine P_i from among the ideals $P_1, \ldots, P_g$.

We extend the action by each member σ of $G = \mathrm{Gal}(K/F)$ to $K \otimes_F F_{\mathfrak{p}}$ as the transformation $\sigma \otimes 1$. Then G acts on $K \otimes_F F_{\mathfrak{p}}$, manifestly keeping each element of $F_{\mathfrak{p}}$ fixed. Since the members of G respect multiplication and addition, they map idempotents to idempotents in $K \otimes_F F_{\mathfrak{p}}$, sending primitive idempotents to primitive idempotents. Thus G permutes the elements η_i. The elements x with $\eta_i x = x$ are exactly the members of K_{P_i}, and hence G permutes the fields K_{P_i}.

Lemma 6.39. In the above setting with K/F Galois, let P_i be one of the ideals $P_1, \ldots, P_g$. Then a member σ of the Galois group $G = \mathrm{Gal}(K/F)$ extends to a field automorphism of K_{P_i} fixing $F_{\mathfrak{p}}$ if and only if it is an isometry of $(K, |\cdot|_{P_i})$, i.e., if and only if σ satisfies $|\sigma x|_{P_i} = |x|_{P_i}$ for all $x \in K$.

PROOF. If σ is an isometry from K into itself in the metric determined by $|\cdot|_{P_i}$, then σ is uniformly continuous as a function from K into the complete space K_{P_i} and therefore extends to a continuous function from the completion K_{P_i} into K_{P_i}.

It follows from the continuity of the extension and the fact that σ respects the operations on K that σ respects the operations on K_{P_i}. These remarks apply also to the extension of σ^{-1}, and the extension of σ^{-1} is a two-sided inverse to the extension of σ. Since σ is the identity on F, the continuity forces the extension of σ to be the identity on $F_{\mathfrak{p}}$.

Conversely suppose that σ extends to an automorphism of K_{P_i} fixing $F_{\mathfrak{p}}$. Let us use the name σ also for the extension. On K_{P_i}, the functions $x \mapsto |x|_{P_i}$ and $x \mapsto |\sigma(x)|_{P_i}$ are absolute values that extend $|\cdot|_{\mathfrak{p}}$ on $F_{\mathfrak{p}}$. Theorem 6.33 shows that they must be equal, and therefore σ is an isometry. □

Proposition 6.40. In the above setting with K/F Galois, let P be one of the ideals $P_1, \dots, P_g$, let $G = \mathrm{Gal}(K/F)$ be the Galois group, and let G_P be the decomposition group at P. Then K_P is a Galois extension of $F_{\mathfrak{p}}$, the members of G_P extend to be isometries of K_P that fix $F_{\mathfrak{p}}$, and the resulting map $\varphi : G_P \to \mathrm{Gal}(K_P/F_{\mathfrak{p}})$ exhibits G_P as isomorphic to $\mathrm{Gal}(K_P/F_{\mathfrak{p}})$.

PROOF. Since K_P is generated by $F_{\mathfrak{p}}$ and K, it is obtained by adjoining to $F_{\mathfrak{p}}$ the same roots of the same polynomials over F that are used to generate K. Therefore $K_P/F_{\mathfrak{p}}$ is a Galois extension.

Lemma 6.39 gives us the map of G_P into $\mathrm{Gal}(K_P/F_{\mathfrak{p}})$. The map φ is a homomorphism because the extension of each member of G_P is unique. It is one-one because the inclusion $K \subseteq K_P$ is one-one.

To see that it is onto, let σ be in $\mathrm{Gal}(K_P/F_{\mathfrak{p}})$, and choose an element $\xi \in K$ such that $K = F(\xi)$. If $m(X)$ is the minimal polynomial of ξ over F, then $\sigma(\xi)$ is an element of K_P with $m(\sigma(\xi)) = 0$. Consequently $\sigma(\xi)$ is a root of $m(X)$. Since K/F is Galois and $m(X)$ has one root in K, all its roots are in K. Thus $\sigma(\xi)$ is in K. The most general member of K is of the form $q(\xi)$, where $q(X)$ is a polynomial of degree less than $\deg m(X)$, and $q(\sigma(\xi))$ has to be in K also. Thus σ is an automorphism of K fixing F. As such, σ must send T into itself and must send P into some ideal P_i of T containing $\mathfrak{p}T$. Meanwhile, Lemma 6.39 shows that σ is an isometry of K relative to $|\cdot|_P$. Thus σ must send P into itself. In other words, the restriction of σ to K is in the decomposition group G_P. □

We know from Theorem 9.64 of *Basic Algebra* that every member σ of the decomposition group G_P yields a member $\overline{\sigma}$ of $\mathrm{Gal}((T/P)/(R/\mathfrak{p}))$ and that the resulting map $\sigma \mapsto \overline{\sigma}$ is a homomorphism onto. Proposition 6.40 allows us to reinterpret this homomorphism as carrying the Galois group of K_P onto the Galois group of T/P. The order of $\mathrm{Gal}(K_P/F_{\mathfrak{p}})$ is ef, and the order of $\mathrm{Gal}((T/P)/(R/\mathfrak{p}))$ is f. Thus the kernel of this homomorphism, which is called the **inertia group** of $K_P/F_{\mathfrak{p}}$, has order e. By Galois theory the fixed field L of the inertia group has $[K_P : L] = e$, $L/F_{\mathfrak{p}}$ is a Galois extension,

and $\mathrm{Gal}(L/F_{\mathfrak{p}})$ has order f. This construction has been arranged to make $\mathrm{Gal}(L/F_{\mathfrak{p}}) \cong \mathrm{Gal}((T/P)/(R/F_{\mathfrak{p}}))$. As the Galois group of a finite extension of finite fields, the Galois group on the right is cyclic of order f. Therefore $\mathrm{Gal}(L/F_{\mathfrak{p}})$ is cyclic of order f.

Referring back to the statement of Proposition 6.38, we might guess that the fixed field L of the inertia group is the unique intermediate field such that K/L is totally ramified and L/F is unramified. This guess is completely correct, but we omit the proof.

8. Different and Discriminant

Theorem 6.31 is the key to a "local/global" approach to handling certain kinds of problems in algebraic number theory and in its analog in algebraic geometry. To illustrate the approach and its power, we shall give in this section and in the problems at the end of the chapter a full proof for the Dedekind Discriminant Theorem (Theorem 5.5), which was left only partially proved in Chapter V. That theorem as stated in Chapter V says that the prime numbers p for which ramification occurs in passing from $\mathbb{Q}$ to a number field K are exactly the primes dividing the field discriminant. The result we obtain now[22] will in fact generalize Theorem 5.5 significantly. In giving the details, we leave the proofs of Proposition 6.38 and Lemmas 6.47 and 6.48 to Problems 15–19 at the end of the chapter.

In the approach used in Chapter V, we were unable to handle primes that are "common index divisors" in the sense of Section V.2. Section V.4 exhibited an example of a common index divisor. The difficulty with the approach in Chapter V is that localization by itself does not ostensibly separate the primes from one another sufficiently for us fully to handle them one at a time. The completion step is a tool powerful enough to complete the separation.

For part of this section, we shall work in the setting of Theorem 6.31, in which we compare two Dedekind domains whose fields of fractions are related by a separable field extension. The situation of eventual interest is that the two Dedekind domains are the rings of algebraic integers within two number fields, but we shall encounter also $\mathfrak{p}$-adic versions of this situation. Thus let R be a Dedekind domain regarded as a subring of its field of fractions F, let K be a finite separable extension of F with $[K : F] = n$, and let T be the integral closure of R in K. In this setting we shall introduce an ideal $\mathcal{D}(K/F)$ of T known as the "relative different" of the two fields, and we shall establish conditions under which the relative different captures fairly precisely what ramification occurs in passing from R to T. This is the generalized version of the Dedekind Discriminant Theorem and appears as Theorem 6.45 below.

[22] Dedekind's Theorem on Differents, given as Theorem 6.45.

In the special case that $F = \mathbb{Q}$, we shall see that the field discriminant D_K satisfies $|D_K| = N(\mathcal{D}(K/\mathbb{Q}))$. In words, the field discriminant is the absolute norm of the relative different $\mathcal{D}(K/\mathbb{Q})$ except possibly for a sign. Using the properties of $N(\cdot)$ listed in Proposition 5.4, we can read off the version of the Dedekind Discriminant Theorem stated in Theorem 5.5 from the results we establish about the relative different.

We work with fractional ideals in F and in K. If M is any nonzero fractional ideal of K, we define its (relative) **dual** as

$$\widehat{M} = \{x \in K \mid \mathrm{Tr}_{K/F}(xy) \text{ is in } R \text{ for all } y \in M\}.$$

Lemma 6.41. In the above setting, if M is a nonzero fractional ideal of K, then so is its dual $\widehat{M}$.

PROOF. Since T has K as its field of fractions, there exists an F vector space basis $\{t_1, \dots, t_n\}$ of K consisting of members of T. If m_0 is a nonzero member of M and $m_j = t_j m_0$, then $\{m_1, \dots, m_n\}$ is an F vector space basis of K lying in M. Form the R submodule $M_1 = \sum_{j=1}^n Rm_j$ of M, and let $\{x_1, \dots, x_n\}$ be the F vector space basis of K such that $\mathrm{Tr}_{K/F}(x_j m_j) = \delta_{ij}$. Let

$$\widehat{M}_1 = \{x \in K \mid \mathrm{Tr}_{K/F}(xm) \text{ is in } R \text{ for all } m \in M_1\}.$$

If we expand a general element x of K as $x = \sum_{j=1}^n c_i x_i$, then a necessary condition for x to be in $\widehat{M}_1$ is that $c_j = \mathrm{Tr}_{K/F}(xm_j)$ be in R for all j. On the other hand, this condition is also sufficient because an element x with all $c_j \in R$ has $\mathrm{Tr}_{K/F}(xm) = \sum_{j=1}^n c_j r_j$ if $m = \sum_{j=1}^n r_j m_j$. Thus $\widehat{M}_1$ is a finitely generated R module with $x_1, \dots, x_n$ as generators. Let S be the T submodule of K given by $S = \sum_{j=1}^n Tx_j$. This is a finitely generated T submodule of K that contains $\widehat{M}_1$. The inclusion $M \supseteq M_1$ evidently implies that $\widehat{M} \subseteq \widehat{M}_1$, and hence $\widehat{M} \subseteq S$. In this way, $\widehat{M}$ is exhibited as a T submodule of the finitely generated T submodule S of K, and $\widehat{M}$ must itself be finitely generated because T is a Noetherian ring. □

Proposition 6.42. In the above setting, the dual $\widehat{T}$ of T is of the form $\widehat{T} = \mathcal{D}(K/F)^{-1}$ for an ideal $\mathcal{D}(K/F)$ of T. This ideal $\mathcal{D}(K/F)$ has the property that

$$\widehat{M} = M^{-1}\mathcal{D}(K/F)^{-1}$$

for every nonzero fractional ideal M of K.

REMARK. The ideal $\mathcal{D}(K/F)$ in T is called the **relative different** of K with respect to F.

PROOF. From the definition, $\widehat{T}$ consists of all x in K for which $\mathrm{Tr}_{K/F}(xt)$ is in R; any member x of T has this property, and thus $T \subseteq \widehat{T}$. Lemma 6.41 shows that $\widehat{T}$ is a fractional ideal of K. Since $\widehat{T}$ contains T, it is the inverse of an ideal of T. This ideal we define as $\mathcal{D}(K/F)$.

Let M be an arbitrary nonzero fractional ideal of K. Since $M^{-1}M = T$, we have $\mathrm{Tr}_{K/F}(M^{-1}\mathcal{D}(K/F)^{-1} \cdot M) = \mathrm{Tr}_{K/F}(\mathcal{D}(K/F)^{-1}) = \mathrm{Tr}_{K/F}(\widehat{T}T) \subseteq R$, and it follows that $M^{-1}\mathcal{D}(K/F)^{-1} \subseteq \widehat{M}$. For the reverse inclusion, let x be in $\widehat{M}$. Then $\mathrm{Tr}_{K/F}(xM \cdot t) \subseteq \mathrm{Tr}_{K/F}(xM) \subseteq R$ for all $t \in T$, and hence $xM \subseteq \widehat{T} = \mathcal{D}(K/F)^{-1}$. This being true for all $x \in \widehat{M}$, we obtain $\widehat{M}M \subseteq \mathcal{D}(K/F)^{-1}$. Therefore $\widehat{M} \subseteq M^{-1}\mathcal{D}(K/F)^{-1}$. □

Proposition 6.43. In the above setting, if L is a field with $F \subseteq L \subseteq K$, then

$$\mathcal{D}(K/F) = \mathcal{D}(K/L)\mathcal{D}(L/F)$$

as an equality of fractional ideals in K.

REMARKS. Let U be the integral closure of R in L. In the displayed line of the proposition, $\mathcal{D}(L/F)$ is an ideal in U, and the right side amounts to the product in T given by $\mathcal{D}(K/L) \cdot \mathcal{D}(L/F)T$.

PROOF. We use the fact that traces can be computed in stages. An element x of K is in $\mathcal{D}(K/F)^{-1}$ if and only if $\mathrm{Tr}_{K/F}(xT) \subseteq R$, if and only if $\mathrm{Tr}_{L/F}\big(\mathrm{Tr}_{K/L}(xT)\big) \subseteq R$, if and only if $\mathrm{Tr}_{K/L}(xT) \subseteq \widehat{U} = \mathcal{D}(L/F)^{-1}$, if and only if $\mathrm{Tr}_{K/L}(xT\mathcal{D}(L/F)) \subseteq U$, if and only if $xT\mathcal{D}(L/F) \subseteq \mathcal{D}(K/L)^{-1}$. Thus $\mathcal{D}(K/F)^{-1}\mathcal{D}(L/F) = \mathcal{D}(K/L)^{-1}$, and the result follows. □

The main result of this section, from which the Dedekind Discriminant Theorem will be derived as Corollary 6.49, is Theorem 6.45 below, Dedekind's Theorem on Differents. The proof requires some preparation. Two results will be used to reduce Theorem 6.45 to a statement about complete fields, for which only a single prime ideal is involved, both for R and for T. The first of these is Theorem 6.31, or more particularly its consequence for traces given in Corollary 6.37c. The other is the following strengthening of the Weak Approximation Theorem in the presence of additional hypotheses. The reduction step to a statement about complete fields then appears as Corollary 6.46.

Theorem 6.44 (Strong Approximation Theorem). Let F be a number field, let R be its ring of algebraic integers, let $P_1, \dots, P_r$ be distinct nonzero prime ideals in R, and let v_{P_j} for each j be the valuation of F and of its completion that corresponds to P_j. If $l_1, \dots, l_r$ are integers and if x_j for $1 \le j \le r$ is a member of the completed field F_{P_j}, then there exists y in F such that

$$v_{P_j}(y - x_j) \ge l_j \qquad \text{for } 1 \le j \le r$$

and such that $v_Q(y) \ge 0$ for all other nonzero prime ideals Q of R.

REMARKS.

(1) It will be helpful to have a name for the property in the conclusion of Theorem 6.44. Thus let T be a Dedekind domain regarded as a subring of its field of fractions K. We say that T has the **strong approximation property** if whenever distinct nonzero prime ideals $P_1, \dots, P_r$ of T are given, along with integers $l_1, \dots, l_r$ and members x_j of the completed field K_{P_j} for $1 \le j \le r$, then there exists y in K such that $v_{P_j}(y - x_j) \ge l_j$ for $1 \le j \le r$ and such that $v_Q(y) \ge 0$ for all other nonzero prime ideals Q of T. The content of Theorem 6.44 is that the ring of algebraic integers in any number field has the strong approximation property.

(2) More generally any principal ideal domain has the strong approximation property. In fact, if R is a principal ideal domain with field of fractions F, if K is a finite extension of F, and if T is the integral closure of R in K, then K is a Dedekind domain (according to the remarks with Proposition 6.7), and K has the strong approximation property. The proof is an easy adaptation of the proof below, with the principal ideal domain substituting for the ring $\mathbb{Z}$ of integers. As a consequence if $\Bbbk$ is a field and if T is the integral closure of $\Bbbk[X]$ in a finite extension of $\Bbbk(X)$, then T has the strong approximation property.

(3) Any Dedekind domain with only finitely many prime ideals has the strong approximation property as an immediate consequence of the Weak Approximation Theorem (Theorem 6.23). One does not need to make use of the fact that such a domain is always a principal ideal domain.

(4) For a number field the conclusion of the theorem as stated imposes a limitation on all the nonarchimedean absolute values. The conclusion cannot be strengthened to impose a limitation on *all* equivalence classes of absolute values, since the Artin product formula (Theorem 6.51 below) imposes a constraint on the set of all of them.

PROOF.[23] We may assume that each l_j satisfies $l_j \ge 0$. Recall that for each prime number p, there are only finitely many prime ideals P in R with $P \cap \mathbb{Z} = p\mathbb{Z}$. Possibly by moving some of the conditions $v_Q(y) \ge 0$ into the displayed hypothesis concerning the P_j's, we may assume that there is some finite set $\{p_1, \dots, p_q\}$ of primes such that $\{P_1, \dots, P_r\}$ consists exactly of all prime ideals P such that $P \cap \mathbb{Z} = p_i\mathbb{Z}$ for some i with $1 \le i \le q$.

Application of the Weak Approximation Theorem (Theorem 6.23) to the absolute values corresponding to $P_1, \dots, P_r$ produces an element $z \in F$ with

[23] This proof is from Hasse's *Number Theory*, pp. 379–380. The argument for $R = \mathbb{Z}$ and all $l_j = 0$ is the key. After an application of the Weak Approximation Theorem, what has to be shown is that if $P_j = p_j\mathbb{Z}$ for $1 \le j \le r$ and if a rational ab^{-1} is given, then there exists a rational mn^{-1} with l prime to $p_1, \dots, p_r$ such that the denominator of $ab^{-1} - mn^{-1}$ is divisible only by the primes $p_1, \dots, p_r$. Another proof of Theorem 6.44, which appears in other books, uses the theory of adeles and ideles to be developed in the next two sections, and again the argument for $\mathbb{Z}$ is the key.

$$v_{P_j}(z - x_j) \geq l_j \qquad \text{for } 1 \leq j \leq r.$$

Form the fractional ideal zR in F, and let its unique factorization be $zR = P_1^{a_1} \cdots P_r^{a_r} Q_1 Q_2^{-1}$, where the a_j are in $\mathbb{Z}$ and where Q_1 and Q_2 are ideals of R whose prime factorizations involve no P_j. Let us see that Q_2 divides a nonzero principal ideal (N) of R whose generator N is in $\mathbb{Z}$ and that N can be chosen to be relatively prime to $p_1, \ldots, p_q$. In fact, it is enough to treat each prime factor of Q_2 separately and multiply the results. For a prime factor P, we know that $P \cap \mathbb{Z} = p\mathbb{Z}$ for some prime p in $\mathbb{Z}$, and we know that pR is the product of P and another ideal of R. This prime p is nonassociate to each of $p_1, \ldots, p_q$ because the only prime ideals whose intersection with $\mathbb{Z}$ is some $p_i\mathbb{Z}$ are $P_1, \ldots, P_r$ and because no such prime ideal divides Q_2. Therefore the prime factorization of (N) contains no factor $P_1, \ldots, P_r$.

Let b be a positive integer to be specified, and choose an integer l such that $lN \equiv 1 \bmod p_i^b$ for $1 \leq i \leq q$. If $p_i R$ factors as $\prod_k P_{i_k}^{m_{i_k}}$ with each P_{i_k} in $\{P_1, \ldots, P_r\}$, then l has the property that $lN - 1$ lies in $\left(\prod_k P_{i_k}^{m_{i_k}}\right)^b$, hence in each $P_{i_k}^b$. Consequently $lN - 1$ lies in P_j^b for $1 \leq j \leq r$.

We show that if b is sufficiently large, then the element $y = lNz$ is the element we seek. First consider nonzero prime ideals Q not in $\{P_1, \ldots, P_r\}$. Our factorizations of zR and (N) show that $yR = lQ_3 Q_1 P_1^{a_1} \cdots P_r^{a_r}$. The power of Q on the right side is ≥ 0 because Q_1 and Q_3 are ideals of R, and thus

$$v_Q(y) \geq 0. \tag{$*$}$$

Now write $y - x_j = (lN - 1)z + (z - x_j)$, and apply the valuation v_{P_j}. Then we have

$$v_{P_j}(y - x_j) \geq \min\left(v_{P_j}((lN - 1)z), v_{P_j}(z - x_j)\right),$$

and it follows from $v_{P_j}(z - x_j)) \geq l_j$ that

$$v_{P_j}(y - x_j) \geq l_j \tag{$**$}$$

if we can arrange that

$$v_{P_j}((lN - 1)z) \geq l_j. \tag{$\dagger$}$$

Since $lN - 1$ lies in P_j^b and since $v_{P_j}(z) = a_j$, a sufficient condition for ($\dagger$) is that $b + a_j \geq l_j$. As j varies, we impose only finitely many conditions on b to get ($\dagger$) to hold for all j, and then the result is that ($**$) holds for all j. In combination with ($*$), this inequality shows that y has the required properties. □

The preparation is all in place to prove Dedekind's Theorem on Differents, from which we shall easily derive the Dedekind Discriminant Theorem. The statement is as follows.

Theorem 6.45 (Dedekind's Theorem on Differents). Let R be a Dedekind domain regarded as a subring of its field of fractions F, let K be a finite separable extension of F with $[K : F] = n$, and let T be the integral closure of R in K. Suppose that T has the strong approximation property. Let $p > 0$ be the characteristic of the residue class field of $R/\mathfrak{p}$, let $\mathfrak{p}$ be a nonzero prime ideal in R, let $\mathfrak{p}T = P_1^{e_1} \cdots P_g^{e_g}$ be the factorization of $\mathfrak{p}T$ as the product of positive powers of distinct prime ideals in T, and let the relative different of K/F split as $\mathcal{D}(K/F) = P_1^{e_1'} \cdots P_g^{e_g'} Q$ for an ideal Q relatively prime to all P_j. Then for each j with $1 \le j \le g$, e_j' is given by

$$e_j' = \begin{cases} e_j - 1 & \text{if } p \text{ does not divide } e_j, \\ \bar{e}_j & \text{with } \bar{e}_j \ge e_j \text{ if } p \text{ divides } e_j. \end{cases}$$

Consequently $\mathcal{D}(K/F)$ has all $e_j' = 0$ if and only if $e_j = 1$ for all j.

The idea is to reduce Theorem 6.45 to the case of complete fields. In the notation in the statement of the theorem, the prime ideals $P_1, \dots, P_g$ are exactly the prime ideals of T that divide $\mathfrak{p}T$, and it is customary to write $P_j \mid \mathfrak{p}$ for these prime ideals of T and only these. If M is a nonzero fractional ideal of K and if $M = P_1^{k_1} \cdots P_g^{k_g} Q$ with Q a fractional ideal whose factorization involves no P_j, we define the $\mathfrak{p}^{\text{th}}$ component of M to be

$$M_{\mathfrak{p}} = P_1^{k_1} \cdots P_g^{k_g}.$$

The understanding in the special case that all k_j are 0 is that $M_{\mathfrak{p}}$ is taken to be T. In all cases, M is then the product over all $\mathfrak{p}$ of its $\mathfrak{p}^{\text{th}}$ component, since the complete factorization of M has nonzero exponents for only finitely many nonzero prime ideals of T. For the two examples that appear in the statement of Theorem 6.45,

$$(\mathfrak{p}T)_{\mathfrak{p}} = \prod_{P_j \mid \mathfrak{p}} P_j^{e_j} \qquad \text{and} \qquad \mathcal{D}(K/F)_{\mathfrak{p}} = \prod_{P_j \mid \mathfrak{p}} P_j^{e_j'}.$$

The reduction of Theorem 6.45 to the case of complete fields results from the following proposition, which combines Theorem 6.31 and the strong approximation property (Theorem 6.44 in the case of number fields).

Proposition 6.46. Let R be a Dedekind domain regarded as a subring of its field of fractions F, let K be a finite separable extension of F with $[K : F] = n$, and let T be the integral closure of R in K. Suppose that T has the strong approximation property. If $\mathfrak{p}$ is any nonzero prime ideal in R, then the different $\mathcal{D}(K/F)$ has the property that

$$\mathcal{D}(K/F) = \prod_{\mathfrak{p}} \prod_{P \mid \mathfrak{p}} \mathcal{D}(K_P/F_{\mathfrak{p}}),$$

the outer product being taken over all nonzero prime ideals $\mathfrak{p}$ of R and the inner product being taken over all prime ideals P of T containing $\mathfrak{p}T$. Here the fields K_P and $F_\mathfrak{p}$ are the completions of K and F corresponding to P and $\mathfrak{p}$, respectively.

PROOF. We actually will show equality of the inverses of the two sides of the displayed formula. By the first conclusion of Proposition 6.42, we are to show that a member x of K has

$$\mathrm{Tr}_{K/F}(xT) \subseteq R \qquad \text{if and only if} \qquad \mathrm{Tr}_{K_P/F_\mathfrak{p}}((xT)_i) \subseteq R_\mathfrak{p} \qquad (*)$$

for all $\mathfrak{p}$ and all P with $P \mid \mathfrak{p}$. Here $(\,\cdot\,)_i$ refers to the embedding $K \to K_{P_i}$ in Theorem 6.31 given by $\xi \mapsto \xi_i = \eta_i(1 \otimes \xi)$, where η_i is the i^{th} projection. To prove $(*)$, we use the formula of Corollary 6.37c, namely

$$\mathrm{Tr}_{K/F}(\xi) = \sum_{i=1}^{g} \mathrm{Tr}_{K_{P_i}/F_\mathfrak{p}}(\xi_i) \qquad \text{for all } \xi \in K. \qquad (**)$$

This formula is valid for every $\mathfrak{p}$.

First suppose that $\mathrm{Tr}_{K_P/F_\mathfrak{p}}((xT)_i) \subseteq R_\mathfrak{p}$ for all $\mathfrak{p}$ and all P with $P \mid \mathfrak{p}$. Fix $\mathfrak{p}$, and put $\xi = xt$ with $t \in T$. Summing the traces over P with $P \mid \mathfrak{p}$ and applying $(**)$, we see that the valuation with respect to $\mathfrak{p}$ of the member $\mathrm{Tr}_{K/F}(\xi)$ of F is ≥ 0. That is, the factor $\mathfrak{p}^k$ that appears in the factorization of the principal fractional ideal $\mathrm{Tr}_{K/F}(\xi)R$ of F has $k \geq 0$. This being true for all $\mathfrak{p}$ means that $\mathrm{Tr}_{K/F}(\xi)R$ is an ordinary ideal. Hence $\mathrm{Tr}_{K/F}(\xi)$ is in R.

In the reverse direction, suppose that $\mathrm{Tr}_{K/F}(xT) \subseteq R$. For each nonzero prime ideal P in T, let v_P be the corresponding valuation. Fix $\mathfrak{p}$. Let $\{P_1, \ldots, P_g\}$ be the set of P's with $P \mid \mathfrak{p}$. Now fix i. By the assumed strong approximation property of K, there exists an element y in K with

$$\begin{aligned} v_{P_i}(y - x) &\geq \max(v_{P_i}(x), 0), \\ v_{P_j}(y) &\geq \max(v_{P_j}(x), 0) \qquad \text{for } j \neq i, \\ v_Q(y) &\geq 0 \qquad\qquad\quad \text{for all prime ideals } Q \notin \{P_1, \ldots, P_g\}. \end{aligned}$$

Let us see that $v_{P_j}(yx^{-1}) \geq 0$ for all j. For $j \neq i$, this is immediate because $v_{P_j}(y) \geq v_{P_j}(x)$. For $j = i$, we compute that

$$\begin{aligned} v_{P_i}(yx^{-1} - 1) &= v_{P_i}(y - x) - v_{P_i}(x) \geq \max(v_{P_i}(x), 0) - v_{P_i}(x) \\ &= \max(0, -v_{P_i}(x)) \geq 0, \end{aligned}$$

and then we see that $v_{P_i}(yx^{-1}) \geq \min(v_{P_i}(yx^{-1} - 1), v_{P_i}(1)) \geq 0$.

With y now fixed, we make use of the strong approximation property of K a second time, obtaining an element z in K with

$$\begin{aligned} v_{P_j}(z - yx^{-1}) &\geq \max(v_{P_j}(x^{-1}), 0) \quad \text{for } 1 \leq j \leq g, \\ v_Q(z) &\geq 0 \qquad\qquad\qquad\quad \text{for all prime ideals } Q \notin \{P_1, \dots, P_g\}. \end{aligned}$$

Since $v_{P_j}(yx^{-1}) \geq 0$ and $v_{P_j}(z - yx^{-1}) \geq 0$ for all j, we find that $v_{P_j}(z) \geq 0$ for all j. From $v_Q(z) \geq 0$ for all other Q, we conclude that z is in T. Since $\mathrm{Tr}_{K/F}(xT) \subseteq R$, $\mathrm{Tr}_{K/F}(xz)$ lies in R. The trace formula $(**)$ therefore shows that

$$\sum_{j=1}^{g} \mathrm{Tr}_{K_{P_j}/F_{\mathfrak{p}}}(x_j z_j) \qquad \text{lies in } R_{\mathfrak{p}}. \tag{$\dagger$}$$

Meanwhile, we have

$$\mathrm{Tr}_{K_{P_j}/F_{\mathfrak{p}}}(x_j z_j) = \mathrm{Tr}_{K_{P_j}/F_{\mathfrak{p}}}(x_j(z_j - y_j x_j^{-1})) + \mathrm{Tr}_{K_{P_j}/F_{\mathfrak{p}}}(y_j) \tag{$\dagger\dagger$}$$

for $1 \leq j \leq g$. For all j, the first term on the right side of $(\dagger\dagger)$ lies in $R_{\mathfrak{p}}$ because the definition of z makes $v_{P_j}(x(z - yx^{-1})) \geq 0$. For $j \neq i$, the second term on the right side lies in $R_{\mathfrak{p}}$ because of the definition of y. Thus $(\dagger\dagger)$ shows that $\mathrm{Tr}_{K_{P_j}/F_{\mathfrak{p}}}(x_j z_j)$ lies in $R_{\mathfrak{p}}$ for $j \neq i$. Comparing this conclusion with $(\dagger)$, we see that $\mathrm{Tr}_{K_{P_i}/F_{\mathfrak{p}}}(x_i z_i)$ lies in $R_{\mathfrak{p}}$. Resubstituting into $(\dagger\dagger)$, we find that

$$\mathrm{Tr}_{K_{P_i}/F_{\mathfrak{p}}}(y_i) \qquad \text{lies in } R_{\mathfrak{p}}. \tag{$\ddagger$}$$

Finally the definition of y shows that $v_{P_i}(y - x) \geq 0$. Hence $\mathrm{Tr}_{K_{P_i}/F_{\mathfrak{p}}}(y_i - x_i)$ is in $R_{\mathfrak{p}}$. Combining this fact with $(\ddagger)$, we conclude that $\mathrm{Tr}_{K_{P_i}/F_{\mathfrak{p}}}(x_i)$ is in $R_{\mathfrak{p}}$. Since i is arbitrary, $\mathrm{Tr}_{K_{P_j}/F_{\mathfrak{p}}}(x_j)$ is in $R_{\mathfrak{p}}$ for $1 \leq j \leq g$. □

With the proof of Theorem 6.45 reduced to the case of complete valued fields by Proposition 6.46, we need to make use of Lemmas 6.47 and 6.48 below, whose proofs are carried out in Problems 17–19 at the end of the chapter.

Lemma 6.47. Let F be a complete valued field with respect to a discrete nonarchimedean valuation, let R be its valuation ring, let $\mathfrak{p}$ be its valuation ideal, let K be a finite separable extension of F with $[K : F] = n$, let T be the integral closure of R in K, and let P be the unique nonzero prime ideal in T. Suppose that K/F is totally ramified with $\mathfrak{p}T = P^e$ for an integer $e \geq 1$, and suppose that the isomorphic residue class fields $R/\mathfrak{p}$ and T/P are finite fields of characteristic p. Then the different $\mathcal{D}(K/F)$ is given by $\mathcal{D}(K/F) = P^{e'}$, where

$$e' = \begin{cases} e - 1 & \text{if } p \text{ does not divide } e, \\ \bar{e} & \text{with } \bar{e} \geq e \text{ if } p \text{ divides } e. \end{cases}$$

Lemma 6.48. Let F be a complete valued field with respect to a discrete nonarchimedean valuation, let R be its valuation ring, let $\mathfrak{p}$ be its valuation ideal, let K be a finite separable extension of F with $[K : F] = n$, let T be the integral closure of R in K, and let P be the unique nonzero prime ideal in T. Suppose that K/F is unramified, i.e., has $\mathfrak{p}T = P$, and suppose that the residue class fields $R/\mathfrak{p}$ and T/P are finite fields of characteristic p. Then the different $\mathcal{D}(K/F)$ equals T.

PROOF OF THEOREM 6.45. Proposition 6.46 shows that

$$\mathcal{D}(K/F)_{\mathfrak{p}} = \prod_{P|\mathfrak{p}} \mathcal{D}(K_P/F_{\mathfrak{p}}). \tag{$*$}$$

Thus consider an extension $K_P/F_{\mathfrak{p}}$ of complete valued fields. Let L be the inertia subfield of $K_P/F_{\mathfrak{p}}$ as given by Proposition 6.38. The intermediate field L has the properties that K_P/L is totally ramified and that $L/F_{\mathfrak{p}}$ is unramified.

Let U be the integral closure of R in L, and let $\wp$ be the unique nonzero prime ideal in U. The properties of L make $\wp T = P^e$ for a suitable integer $e = e(P \mid \wp)$, $T/P \cong U/\wp$, and $\mathfrak{p}U = \wp$. Lemmas 6.47 and 6.48 tell us that $\mathcal{D}(L/F_{\mathfrak{p}}) = U$ and that $\mathcal{D}(K_P/L) = P^{e'}$, where

$$e' = \begin{cases} e - 1 & \text{if } p \text{ does not divide } e, \\ \bar{e} & \text{with } \bar{e} \geq e \text{ if } p \text{ divides } e. \end{cases} \tag{$**$}$$

Problem 33 at the end of Chapter IX of *Basic Algebra* shows that ramification indices multiply for successive extensions. Thus $e(P \mid \mathfrak{p}) = e(P \mid \wp)e(\wp \mid \mathfrak{p}) = e \cdot 1 = e$. Proposition 6.43 shows that differents multiply in corresponding fashion. Therefore $\mathcal{D}(K_P/F_{\mathfrak{p}}) = \mathcal{D}(K_P/L)\mathcal{D}(L/F_{\mathfrak{p}}) = P^{e'}U = P^{e'}$. Substituting into $(*)$, we obtain

$$\mathcal{D}(K/F)_{\mathfrak{p}} = \bigoplus_{P|\mathfrak{p}} \mathcal{D}(K_P/F_{\mathfrak{p}}) = \bigoplus_{P|\mathfrak{p}} P^{e'(P|\mathfrak{p})},$$

where $e'(P \mid \mathfrak{p})$ is the integer e' of $(**)$ when $e = e(P \mid \mathfrak{p})$. This proves Theorem 6.45 for the $\mathfrak{p}^{\text{th}}$ component of $D(K/F)$. Since $\mathfrak{p}$ is arbitrary and only finitely many components can be unequal to T, the theorem follows. □

Corollary 6.49 (= THEOREM 5.5, Dedekind Discriminant Theorem). Let K be a number field, let T be its ring of algebraic integers, let p be a prime number, and let $(p)T = P_1^{e_1} \cdots P_g^{e_g}$ be the factorization of $(p)T$ as the product of powers of distinct prime ideals in T. Then e_j is greater than 1 for some j if and only if p divides the field discriminant D_K.

PROOF. Let us observe first that the discriminant D_K is given up to sign by the index $|\widehat{T}/T|$. In fact, T is a torsion-free finitely generated abelian group and hence is free abelian of rank $n = [K : \mathbb{Q}]$, say with an ordered $\mathbb{Z}$ basis $\Gamma = (x_1, \dots, x_n)$. Since the $\mathbb{Q}$ bilinear form $(x, y) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(xy)$ is nondegenerate on K, there exists an ordered basis $\Delta = (y_1, \dots, y_n)$ of K with $\mathrm{Tr}_{K/\mathbb{Q}}(x_i y_j) = \delta_{ij}$. Let us write $x_j = \sum_i a_{ij} y_i$ with all a_{ij} in $\mathbb{Q}$. According to Proposition 5.1, D_K equals the discriminant $D(\Gamma)$ of Γ, defined in Section V.2 by $D(\Gamma) = \det[\mathrm{Tr}_{K/\mathbb{Q}}(x_i x_j)]_{ij}$. Substituting $x_j = \sum_i a_{ij} y_i$, we obtain

$$D_K = \det\Big[\sum_k a_{kj}\,\mathrm{Tr}_{K/\mathbb{Q}}(x_i y_k)\Big]_{ij} = \det\Big[\sum_k a_{kj}\delta_{ik}\Big]_{ij} = \det[a_{ij}]_{ij}.$$

Thus $|D_K| = |\widehat{T}/T| = \big|\mathcal{D}(K/\mathbb{Q})^{-1}\big/T\big|$, as asserted.

In a moment we shall show that

$$\big|\mathcal{D}(K/\mathbb{Q})^{-1}\big/T\big| = |T/\mathcal{D}(K/\mathbb{Q})|, \tag{$*$}$$

from which we conclude that $|D_K| = N(\mathcal{D}(K/\mathbb{Q}))$. Assuming $(*)$, we continue. Unique factorization of ideals allows us to write $\mathcal{D}(K/\mathbb{Q}) = P_1^{e'_1} \cdots P_g^{e'_g} Q$, where Q is an ideal relatively prime to (p). Combining the equality $D_K = N(\mathcal{D}(K/\mathbb{Q}))$ with Proposition 5.4 shows that

$$D_K = N(\mathcal{D}(K/\mathbb{Q})) = N(Q) \prod_{j=1}^{g} N(P_j^{e'_j}) = N(Q) \prod_{j=1}^{g} p^{e'_j f_j},$$

where $N(Q)$ is an integer not divisible by p and where $f_j = \dim_{\mathbb{F}_p}(T/P_j)$ for $1 \le j \le g$. Consequently D_K is prime to p if and only if $e'_j = 0$ for all j. If we take into account that T has the strong approximation property as a consequence of Theorem 6.44, then application of Theorem 6.45 completes the proof of the present corollary except for the verification of $(*)$.

Thus we are left with proving that $\big|\mathcal{D}(K/\mathbb{Q})^{-1}\big/T\big| = |T/\mathcal{D}(K/\mathbb{Q})|$. More generally we shall show that

$$|I^{-1}/T| = |T/I| \tag{$**$}$$

for every nonzero ideal I in T. In turn, we shall deduce $(**)$ after showing that

$$|M/PM| = N(P) \tag{$\dagger$}$$

whenever M is a nonzero fractional ideal in K and P is a nonzero prime ideal in T. We do so by showing that M/PM is a vector space over the field T/P of dimension 1. It is evident that T carries M to itself and PM to itself, and that

P carries M to PM. Thus the action of T on M/PM descends to an action of T/P on M/PM. The vector space M/PM is not 0 because $M \neq PM$ by unique factorization of fractional ideals. To see that M/PM has dimension at most 1, fix an element x of M that does not lie in PM. Then $xT + PM$ is a fractional ideal of K that is contained in $M + PM = M$ and contains PM and a member of M that is not in PM. Hence it equals M. Accordingly, if $y \in M$ is given, we can choose $t \in T$ such that $xt - y$ is in PM. Then $(t + P)(x + PM) = y + PM$, and T/P carries $x + PM$ onto M/PM. So M/PM is 1-dimensional over T/P, and (†) follows.

Returning to (∗∗), let $I = Q_1 \cdots Q_k$ express I as the product of nonzero prime ideals. Iterated application of (∗∗) and the First Isomorphism Theorem gives

$$\begin{aligned} |I^{-1}/T| &= |I^{-1}/Q_1 \cdots Q_k I^{-1}| = |I^{-1}/Q_1 \cdots Q_{k-1} I^{-1}| N(Q_k) \\ &= |I^{-1}/Q_1 \cdots Q_{k-2} I^{-1}| N(Q_k) N(Q_{k-1}) \\ &= \cdots = |I^{-1}/I^{-1}| \prod_{j=1}^{k} N(Q_j) = N(I). \end{aligned}$$

This proves (∗∗) and therefore also (∗). □

One more point needs explanation. The discussion in Section IX.17 of *Basic Algebra* concerned a monic irreducible polynomial $F(X)$ in $\mathbb{Z}[X]$ and its reduction $\overline{F}(X)$ modulo p, and the interest was in the Galois group G of the splitting field $\mathbb{K}'$ of $F(X)$ over $\mathbb{Q}$. Theorem 9.64 of that book dealt with the natural homomorphism from a decomposition subgroup G_P of G onto the Galois group $\overline{G}$ of the splitting field over $\mathbb{F}_p$ of $\overline{F}(X)$, and it was asserted without proof that this homomorphism is one-one if p does not divide the discriminant of $F(X)$. The order of the kernel of the homomorphism was identified as the common ramification index of the prime ideals P' containing $(p)R'$, R' being the ring of algebraic integers in $\mathbb{K}'$. Let $\mathbb{K} = \mathbb{Q}[X]/(F(X))$. Except in the quadratic case, the field $\mathbb{K}$ typically has much lower dimension over $\mathbb{Q}$ than $\mathbb{K}'$ does. The Dedekind Discriminant Theorem relates $D_{\mathbb{K}}$ to ramification relative to $\mathbb{K}$, as well as $D_{\mathbb{K}'}$ to ramification relative to $\mathbb{K}'$. We know that primes not dividing the discriminant of $F(X)$ do not divide $D_{\mathbb{K}}$, but we need a proof that primes not dividing the discriminant of $F(X)$ do not divide $D_{\mathbb{K}'}$.

To approach this question, one needs the notion of "relative discriminant" analogous to that of "relative different" for an extension $\mathbb{K}/\mathbb{F}$ of number fields. The relative different is defined so as to be an ideal for $\mathbb{K}$, and the relative discriminant is an ideal for $\mathbb{F}$. (The field discriminant is the generator of the relative discriminant for $\mathbb{K}/\mathbb{Q}$ with the appropriate sign attached.) One proves that the behavior of the relative discriminant under successive extension is reasonable, just as it is for degree of extension, ramification indices, residue class degrees, and relative

differents. These results show that if $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L}$, then the field discriminant for $\mathbb{K}$ divides the field discriminant for $\mathbb{L}$. The next step is to extend the notion of field discriminant so that it applies to commutative semisimple algebras and to show that the discriminant of a tensor product over $\mathbb{Q}$ of finitely many number fields is a certain function of the field discriminants and dimensions of the factors. Finally we return to $F(X)$ and its splitting field $\mathbb{K}'$. Let ξ be a root of $F(X)$ in $\mathbb{K}'$, and let $\sigma_1(\xi), \dots, \sigma_n(\xi)$ be the distinct conjugates of ξ. Then $\mathbb{K}'$ is generated by the subfields $\mathbb{Q}(\xi_1), \dots, \mathbb{Q}(\xi_n)$, and the ($\mathbb{Q}$ multilinear) multiplication map extends to an algebra homomorphism of $\mathbb{Q}(\xi_1) \otimes_{\mathbb{Q}} \cdots \otimes_{\mathbb{Q}} \mathbb{Q}(\xi_n)$ onto $\mathbb{K}'$. As the tensor product of commutative semisimple algebras in characteristic 0, this is commutative semisimple (Corollary 2.37) and is therefore a direct sum of fields (Theorem 2.2). Thus we can regard $\mathbb{K}'$ as a subfield of the tensor product of fields isomorphic to $\mathbb{Q}[X]/(F(X))$, and the discriminant of $\mathbb{K}'$ divides the discriminant of the tensor product. Putting everything together, we see that the only possible primes dividing $D_{\mathbb{K}'}$ are the primes that divide $D_{\mathbb{K}}$. Therefore the primes that fail to divide the discriminant of $F(X)$ do not ramify in $\mathbb{K}'$.

9. Global and Local Fields

A **global field** K is either a number field, i.e., a finite extension of $\mathbb{Q}$, or a function field in one variable over a finite field, i.e., a finite extension of some $\mathbb{F}_q(X)$, where $\mathbb{F}_q$ is a finite field.[24] An example of the latter is

$$K = \mathbb{F}_p(x)[y]/(y^2 - (x^3 - x)) \cong \mathbb{F}_p(x)\big[\sqrt{x^3 - x}\,\big].$$

In this section we shall develop some machinery for working with global fields. Our interest at present is in number fields, but function fields in one variable are the object of study in Chapter IX. Consequently the results will be stated for all global fields as long as all global fields can readily be treated together, and thereafter we shall specialize to number fields.

The virtue of global fields for current purposes is that their completions with respect to nontrivial absolute values are always locally compact with a nontrivial topology. In the case of number fields, we know this for archimedean absolute values by Proposition 6.27, and it follows for nonarchimedean absolute values by Corollary 6.21 and Theorem 6.26. In the function-field case as above, the completions have to be nonarchimedean by Proposition 6.14, and their absolute values have to be discrete by Corollary 6.22; then the residue class fields are always

[24] It will be shown in Chapter VII that a function field in one variable over a finite field is always a finite *separable* extension of $\mathbb{F}_q(Y)$ for a suitable indeterminate Y.

finite, and Theorem 6.26 shows that the completions are all locally compact with a nontrivial topology.

To study a global field K in the style of this chapter, one studies simultaneously the completions[25] of K with respect to one absolute value from each equivalence class.[26] Two completions are said to be **equivalent completions** if the absolute values on the domains of the completion maps are equivalent in the sense of Section 3. An equivalence class of completions of nontrivial absolute values is called a **place** of K. A place is called **archimedean** or **nonarchimedean** according as the corresponding absolute values are archimedean or nonarchimedean; in the archimedean case it is called **real** or **complex** according as the locally compact completed field is $\mathbb{R}$ or $\mathbb{C}$.

Because of the special hypotheses for the situation with global fields, we shall see that to each place corresponds a distinguished choice of an absolute value on K from the equivalence class, called the **normalized** absolute value in the class.[27] These normalized completions are glued together[28] in a fashion to be described in the next section to form the ring of "adeles" of K and the group of "ideles" of K. Historically ideles preceded adeles, and ideles were introduced in order to reinterpret class field theory and improve upon it; convincing motivation is therefore not readily at hand without knowledge that extends beyond this book. However, we can get some advance insight into how adeles and ideles might be useful from the first part of the classical proof of the Dirichlet Unit Theorem (Theorem 5.13) as given in Section V.5.

That proof in effect handles archimedean places in a way similar to the way that adeles handle all places. In more detail let K be a number field of degree n over $\mathbb{Q}$, and let R be its ring of algebraic integers. In Chapter V we usually regarded K as a subfield of $\mathbb{C}$, but we shall not do so here. As was observed in Section V.2, there exist exactly n field mappings of K into $\mathbb{C}$, and we denote them by $\sigma_1, \dots, \sigma_n$. If x is in K, then the images $\sigma_1(x), \dots, \sigma_n(x)$ are called the **conjugates** of x. Among $\sigma_1, \dots, \sigma_n$ are r_1 real-valued mappings and r_2 complex conjugate pairs, with $r_1 + 2r_2 = n$. Let us number the mappings so that $\sigma_1, \dots, \sigma_{r_1}$ are real-valued and so that $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}$ pick out one from each complex conjugate pair. Proposition 6.27 shows that the functions $x \mapsto |\sigma_1(x)|$,

[25] It is important not to lose sight of the fact that a "completion" is a certain kind of homomorphism of valued fields and does not consist merely of the range space.

[26] The completion of the trivial absolute value is excluded.

[27] The range of each completion is a locally compact field whose topology is not the discrete topology. Such a field is often called a **local field** in books. Examples are $\mathbb{R}$, $\mathbb{C}$, $\mathfrak{p}$-adic fields, and fields $\mathbb{F}_q((X))$ of formal Laurent series. One can show that there are no other locally compact fields whose topology is not discrete. The definition of "local field" in some books is arranged to exclude $\mathbb{R}$ and $\mathbb{C}$.

[28] It is tempting to think in terms of the gluing as involving just the locally compact fields, but the completion mappings play a role and that description is thus an oversimplification.

$\dots$, $x \mapsto |\sigma_{r_1+r_2}(x)|$ are a complete set of representatives for the archimedean places of K; the first r_1 are real, and the last r_2 are complex.

Just before Lemma 5.17 we introduced the mapping $\Phi : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ given by

$$\Phi(x) = \big(\sigma_1(x), \dots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \dots, \sigma_{r_1+r_2}(x)\big) \qquad \text{for } x \in K.$$

Lemma 5.17 observed that the image $\Phi(R)$ of R is a lattice in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$. The starting point for proving the Dirichlet Unit Theorem in Section V.5 was to apply the Minkowski Lattice-Point Theorem to this lattice $\Phi(R)$. Proposition 6.27 allows us to interpret the mapping Φ as the natural embedding of K into the product of its completions at all archimedean places.

The ring of adeles of K will be a corresponding space for dealing with completions with respect to all nontrivial absolute values, archimedean and nonarchimedean.

While we have the archimedean places of the number field K at hand, let us address the question of their normalized representatives. Since the field maps from K into $\mathbb{C}$ given by $\sigma_{r_1+1,\dots,r_1+r_2}$ are equal to the complex conjugates of $\sigma_{r_1+r_2+1}, \dots, \sigma_n$, every member x of K has

$$N_{F/\mathbb{Q}}(x) = \prod_{j=1}^{n} \sigma_j(x) = \Big(\prod_{j=1}^{r_1} \sigma_j(x)\Big)\Big(\prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|^2\Big).$$

This formula can be viewed as an archimedean analog of the formula in Corollary 6.37b. The number field $\mathbb{Q}$ has one archimedean place, and ordinary absolute value is taken as its normalized representative. We denote this representative by $|\cdot|_\infty$. With $|\cdot|$ denoting ordinary absolute value on $\mathbb{R}$ and $\mathbb{C}$, we obtain

$$|N_{K/\mathbb{Q}}(x)|_\infty = \Big(\prod_{j=1}^{r_1} |\sigma_j(x)|\Big)\Big(\prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|^2\Big).$$

It is customary to use letters like v and w as indices for places. The real places are the completions $x \mapsto \sigma_j(x)$, $1 \le j \le r_1$, of K into $\mathbb{R}$, and the **normalized absolute value** on K for a real place is the pullback from ordinary absolute value on $\mathbb{R}$. Thus if $|\cdot|_{\mathbb{R}}$ denotes ordinary absolute value on $\mathbb{R}$ and if v is a real place corresponding to σ_j, then we define $|x|_v = |\sigma_j(x)|_{\mathbb{R}}$ for $x \in K$. The normalization to use for the complex places is motivated by the formula above. If $r_1 + 1 \le j \le r_1 + r_2$, then σ_j in effect contributes twice to the above formula, once from j and once from $j + r_2$, and the notion of normalized absolute value is to take this double contribution into account. Thus we write $|\cdot|_{\mathbb{C}}$ for the *square* of the ordinary absolute value on $\mathbb{C}$; this quantity is not really an absolute value, since the triangle inequality fails for it, but it has too many desirable features to

be ignored. We define the **normalized absolute value** on K for a complex place to be the pullback from this function $|\cdot|_{\mathbb{C}}$ on $\mathbb{C}$ even though the result fails to satisfy the triangle inequality. Thus if v is a complex place corresponding to σ_j with $r_1 + 1 \le j \le r_1 + r_2$, then we define $|x|_v = |\sigma_j(x)|_{\mathbb{C}} = |\sigma_j(x)|^2$ for $x \in K$. With these definitions of normalized absolute values for archimedean places, the formula above for $|N_{F/\mathbb{Q}}(x)|_\infty$ can be rewritten as

$$|N_{K/\mathbb{Q}}(x)|_\infty = \Big(\prod_{j=1}^{r_1} |\sigma_j(x)|_{\mathbb{R}}\Big)\Big(\prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|_{\mathbb{C}}\Big) = \Big(\prod_{v \text{ real}} |x|_v\Big)\Big(\prod_{v \text{ complex}} |x|_v\Big).$$

We summarize matters in the following proposition.

Proposition 6.50. If K is a number field, then

$$|N_{F/\mathbb{Q}}(x)|_\infty = \prod_{v \text{ archimedean}} |x|_v \qquad \text{for } x \in K,$$

where $|\cdot|_v$ is the pullback of $|\cdot|_{\mathbb{R}}$, the ordinary absolute value, for real places and where $|\cdot|_v$ is the pullback of $|\cdot|_{\mathbb{C}}$, the ordinary absolute value *squared*, for complex places.

At this point we could give a definition of normalized absolute value corresponding to nonarchimedean places. But we shall digress in order to motivate the definition using concepts from measure theory that may be known to some readers and not to others. These concepts play a role within the text only in the next paragraph and in Example 4 of normalized discrete absolute values below, and the reader will not miss any results or proofs by skipping this material.

The digression begins. Any locally compact group has a nonzero measure on it that is invariant under left translation,[29] and this measure is unique up to multiplication by a scalar. Let a locally compact field L be given, and let μ be an invariant measure of this kind with respect to the additive group of L. Each nonzero element c of L has the property that $\mu(cE)$ is a multiple of $\mu(E)$ that is independent of E. If we write $|c|_L$ for this multiple and put $|0|_L = 0$, then it turns out that some power $|\cdot|_L^\alpha$ with $0 < \alpha \le 1$ is necessarily an absolute value and that this power α can be taken to be 1 in all cases except when $L = \mathbb{C}$. In the case of $\mathbb{C}$, it is easy to check that $|c|_{\mathbb{C}} = |c|^2$, and the triangle inequality therefore

[29] Although the details will not be important for us, let us be more precise: The measure is on the σ-algebra of "Baire sets" on the group—the smallest σ-algebra containing those compact sets that are intersections of countably many open sets. The measure is not the 0 measure, it is finite on all the generating compact sets, and it takes the same value on a set as it does on any left translate of the set. It is called a left **Haar measure**. For more information, see the author's *Advanced Real Analysis*, Chapter VI.

fails for $\alpha = 1$. But in all other cases, $|\cdot|_L$ is a canonical choice for an absolute value on L. Now suppose that $\psi : K \to L$ is a field map of a global field K onto a dense subfield of a locally compact field. We impose this special absolute value $|\cdot|_L$ on L. Then a necessary and sufficient condition on an absolute value $|\cdot|_K$ for $\psi : (K, |\cdot|_K) \to (L, |\cdot|_L)$ to be a completion is that $|\cdot|_K = \psi^*(|\cdot|_L)$. In other words, the pullback of the special normalization of the absolute value on the locally compact field is the natural normalization to use for the absolute value on the global field.

With the digression now over, we want to associate to each nonarchimedean place of a global field a special normalization of an absolute value. (We handled the question of normalization at archimedean places earlier in the section.) We can be a bit more general. Suppose that F is an arbitrary field with a discrete valuation v and with corresponding nontrivial absolute value given by $|x|_v = r^{-v(x)}$ for some $r > 0$. Let R be the valuation ring and $\mathfrak{p}$ the valuation ideal; $\mathfrak{p}$ is a principal ideal of the form (π) for some $\pi \in R$. Suppose that the residue class field $R/\mathfrak{p}$ is finite. Then we say that $|\cdot|_v$ is **normalized** if $|\pi|_v = |R/\mathfrak{p}|^{-1}$. This definition is independent of the choice of π.

EXAMPLES OF NORMALIZED DISCRETE ABSOLUTE VALUES.

(1) The field $\mathbb{Q}$ and the p-adic absolute value given by $|ab^{-1}p^k|_p = p^{-k}$ when a and b are integers prime to p. The valuation ring R consists of all ab^{-1} with $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, and b prime to p. The valuation ideal consists of all such ab^{-1} with a divisible by p, and the quotient $R/\mathfrak{p}$ is isomorphic to $\mathbb{F}_p$. The element π may be taken to be p, and $|p|_p$ equals p^{-1}, which equals $|R/\mathfrak{p}|^{-1}$. Thus the p-adic absolute value on $\mathbb{Q}$ is normalized.

(2) Let K be a number field of degree n over $\mathbb{Q}$, and let T be its ring of algebraic integers. Let $\mathfrak{p}$ be a nonzero prime ideal in T, and let v be the corresponding valuation of K. Let $q = |T/\mathfrak{p}|$, and define $|x|_\mathfrak{p} = q^{-v(x)}$. Then $|\cdot|_\mathfrak{p}$ is normalized because Theorem 6.5e shows that the residue class field obtained from the valuation is isomorphic to $T/\mathfrak{p}$.

(3) Let $K = \mathbb{F}_q(X)$, fix a prime polynomial $c(X)$ in $\mathbb{F}_q[X]$, and consider the absolute value on K defined by $|a(X)b(X)^{-1}c(X)^k| = q^{-k \deg c(X)}$ whenever $a(X)$ and $b(X)$ are polynomials relatively prime to $c(X)$. This example runs completely parallel to the two previous examples, and π may be taken to be $c(X)$. The residue class field has as representatives all polynomials $h(X)$ with $\deg h(X) < \deg c(X)$ and thus has order $q^{\deg c(X)}$. This order matches $|c(X)|^{-1}$, and hence $|\cdot|$ is normalized.

(4) If F is a locally compact field whose topology comes from some nontrivial discrete absolute value with finite residue class field, then the canonical absolute value $|\cdot|_F$ described in the digression above and obtained from an invariant

measure μ on the additive group of F is normalized. To see this, let R and $\mathfrak{p}$ be the valuation ring and valuation ideal, and write $\mathfrak{p} = (\pi)$. Put $m = |R/\mathfrak{p}|$, and let $x_1, \dots, x_m$ be representatives of the m cosets of $R/\mathfrak{p}$ in R. Then $\mu(x_j + \mathfrak{p}) = \mu(\mathfrak{p})$ for $1 \le j \le m$ by translation invariance of μ, and hence $\mu(R) = \sum_{j=1}^{m} \mu(x_j + \mathfrak{p}) = m\mu(\mathfrak{p})$. Substituting and using the definition of $|\cdot|_F$ gives $\mu(\mathfrak{p}) = \mu(\pi R) = |\pi|_F \mu(R) = |\pi|_F m\mu(\mathfrak{p})$. The number $\mu(\mathfrak{p})$ is positive, since $\mathfrak{p}$ is a nonempty open subset of F, and we can cancel to get $|\pi|_F m = 1$. Thus $|\pi|_F = |R/\mathfrak{p}|^{-1}$, and $|\cdot|_F$ is normalized.

Theorem 6.51 (Artin product formula). If F is a number field and if normalized absolute values are used, then

$$\prod_v |x|_v = 1 \qquad \text{for all nonzero } x \in F,$$

the product being taken over all places v. In this product, only finitely many of the factors can be different from 1.

REMARKS. A version of this theorem is valid for function fields in one variable. As Corollary 6.22 permits, one can state this analogous theorem in terms of discrete valuations that are trivial on the base field, and absolute values need play no role. The precise statement and proof appear in Chapter IX. Corollary 6.9 in the present chapter is a special case.

PROOF. First we prove the result for $\mathbb{Q}$. Let a rational $y = \pm p_1^{k_1} \cdots p_r^{k_r}$ be given; here $p_1, \dots, p_r$ are distinct primes. The product $\prod_v |y|_v$ is taken over all places, hence over all primes and the one archimedean place ∞. For this $y \in \mathbb{Q}$, we have $|y|_{p_j} = p_j^{-k_j}$ for $1 \le j \le r$ and $|y|_{p'} = 1$ for all other primes p'. So $\prod_{p \text{ prime}} |y|_p = p_1^{-k_1} \cdots p_r^{-k_r}$. Since $|y|_\infty = p_1^{k_1} \cdots p_r^{k_r}$, we obtain $\prod_{\text{all } v} |y|_v = 1$.

Let R be the ring of algebraic integers in F. Given x in F, factor the fractional ideal xR. The nonarchimedean places correspond to the nonzero prime ideals in R, and $|x|_v$ is 1 except for the v's corresponding to those prime ideals in the factorization. There are only finitely many of these. Since also there are only finitely many archimedean places, we see that $|x|_v = 1$ for all but finitely many v.

Let us consider the nonarchimedean places separately from the archimedean ones. The nonarchimedean places correspond to nonzero prime ideals $\wp$, and we group these according to the prime number p such that $\wp \cap \mathbb{Z} = p\mathbb{Z}$, writing $\wp \mid p\mathbb{Z}$ for this correspondence. For fixed p and for each $\wp$ with $\wp \mid p\mathbb{Z}$, let $x_\wp$ be the image of x under the local embedding in $F_\wp$. Corollary 6.37b gives $N_{F/\mathbb{Q}}(x) = \prod_{\wp \mid p\mathbb{Z}} N_{F_\wp/\mathbb{Q}_p}(x_\wp)$. Theorem 6.33 shows that $|x_\wp|_{F_\wp}$ is a power of $|N_{F_\wp/\mathbb{Q}_p}(x_\wp)|_{\mathbb{Q}_p}$. To determine the power, we observe from Example 2 that

the canonical absolute values on $\mathbb{Q}_p$ and $F_\wp$ are normalized, and we specialize $|x_\wp|_{F_\wp}$ and $|N_{F_\wp/\mathbb{Q}_p}(x_\wp)|_{\mathbb{Q}_p}$ to $x_\wp$ in $\mathbb{Q}_p$. Making the comparison, we find that $|N_{F_\wp/\mathbb{Q}_p}(x_\wp)|_{\mathbb{Q}_p} = |x_\wp|_{F_\wp}$. We know that each local embedding respects absolute values; since Theorems 6.5e and 6.26e together show that the residue class fields of $F_\wp$ and $\mathbb{Q}_p$ have orders $|R/\wp|$ and $|\mathbb{Z}/p\mathbb{Z}|$, it follows that $|x_\wp|_{F_\wp} = |x|_\wp$. Therefore

$$\begin{aligned} |N_{F/\mathbb{Q}}(x)|_p = |N_{F/\mathbb{Q}}(x)|_{\mathbb{Q}_p} &= \prod_{\wp|p\mathbb{Z}} |N_{F_\wp/\mathbb{Q}_p}(x_\wp)|_{\mathbb{Q}_p} \\ &= \prod_{\wp|p\mathbb{Z}} |x_\wp|_{F_\wp} = \prod_{\wp|p\mathbb{Z}} |x|_\wp. \end{aligned} \tag{$*$}$$

For the finitely many archimedean places, Proposition 6.50 gives us the formula

$$|N_{F/\mathbb{Q}}(x)|_\infty = \prod_{v \text{ archimedean}} |x|_v, \tag{$**$}$$

where $|\cdot|_\infty$ is the ordinary absolute value on $\mathbb{Q}$. Multiplying $(*)$ and $(**)$ and using the known identity $\prod_v |y|_v = 1$ for the element $y = N_{F/\mathbb{Q}}(x)$ of $\mathbb{Q}$, we obtain the theorem. □

10. Adeles and Ideles

In this section we do the gluing that creates the adeles and the ideles out of the places of a global field. We begin with a topological construction, and then we superimpose the algebraic structure. The general constructions and the two main theorems will be valid for all global fields, but we shall discuss proofs of the theorems only for number fields.

Suppose that $\{X_i \mid i \in I\}$ is a nonempty family of locally compact Hausdorff spaces. Assume that for all but finitely many $i \in I$ we are given a compact open subset Z_i of X_i. The **restricted direct product** of the X_i's relative to the Z_i's is the subset

$$\prod_{i\in I}{}' X_i \subseteq \prod_{i\in I} X_i$$

defined by

$$(x_i)_{i\in I} \in \prod_{i\in I}{}' X_i \qquad \text{if and only if} \qquad x_i \in Z_i \text{ for all but finitely many } i.$$

The restricted direct product is topologized as follows. Suppose that $S \subseteq I$ is a finite subset and that Z_i is defined for $i \notin S$. Put

$$X(S) = \prod_{i\in S} X_i \times \prod_{i\notin S} Z_i.$$

In their respective product topologies the first factor is locally compact, and the second factor is compact. Certainly $X(S)$ is a subset of the restricted direct product, and evidently the restricted direct product is the union of the subsets $X(S)$ over all finite subsets S for which Z_i is defined when $i \notin S$. We topologize $\prod'_{i\in I} X_i$ by insisting that each $X(S)$ be an open subset.[30] The resulting topology is locally compact Hausdorff. In fact, any two members of $\prod'_{i\in I} X_i$ lie in a common $X(S)$, and the open sets that separate them in $X(S)$ separate them in $\prod'_{i\in I} X_i$. Also, any $(x_i)_{i\in I}$ is in some $X(S)$, which is locally compact, and a compact neighborhood within $X(S)$ will be a compact neighborhood in $\prod'_{i\in I} X_i$.

Now we superimpose the algebraic structure. Let K be a global field. To each place v of K, we have associated a normalized absolute value $|\cdot|_v$ on K and a completion $\iota_v : (K, |\cdot|_v) \to (K_v, |\cdot|_{K_v})$. Each of the complete valued fields K_v is locally compact. Except at the finitely many archimedean places, which occur only in the number-field case, $|\cdot|_{K_v}$ arises from a discrete valuation. We take R_v to be the corresponding valuation ring, i.e., $R_v = \{x \in K_v \mid |x|_v \le 1\}$. This is a compact open additive subgroup of K_v. Thus we can form a restricted direct product in which the index set I is the set of places of K, the v^{th} locally compact Hausdorff space is K_v, and the v^{th} compact open subset is R_v. This restricted direct product carries the structure of a commutative ring with identity, with its addition and multiplication defined in coordinate-by-coordinate fashion, and the operations are continuous. Thus we obtain a topological ring, known as the ring of **adeles** of K and denoted by $\mathbb{A}_K$ or simply by $\mathbb{A}$ when no ambiguity is possible.

If for each $x \in K_{v_0}$, we send x into the tuple $(a_v)_v$ that has $a_{v_0} = x$ and $a_v = 0$ for $v \ne v_0$, then the result is a one-one continuous ring homomorphism of K_v into $\mathbb{A}$. This homomorphism of course does not send the multiplicative identity of K_v to the multiplicative identity of $\mathbb{A}$.

The completion mappings $\iota_v : K \to K_v$ embed K into each K_v, and we can form a corresponding diagonal map $\iota : K \to \prod_v K_v$ into the full product of K_v's by defining $\iota(x) = (\iota_v(x))_v$. Actually, we shall check for $x \ne 0$ that only finitely many places have $|\iota_v(x)|_v = |x|_v$ unequal to 1, and therefore the image of the diagonal map is in the adeles. Thus we have a diagonal ring homomorphism

$$\iota : K \to \mathbb{A} \qquad \text{given by} \qquad \iota(x) = (\iota_v(x))_v \text{ for } x \in K.$$

The fact that in the number-field case, $|x|_v$ is unequal to 1 for only finitely many places appears as part of Theorem 6.51. For the function-field case, the field K is a finite separable extension of some field $\mathbb{F}_q(X)$, and all but finitely many places come from nonzero prime ideals in the integral closure R of $\mathbb{F}_q[X]$ in K. At the

[30] In other words, a set in $\prod'_{i\in I} X_i$ is open if and only if its intersection with each $X(S)$ is open in $X(S)$.

unexceptional such places the value of $|x|_v$ comes by treating xR as a fractional ideal and factoring it; only finitely many ideals are involved in the factorization, and only those among all the unexceptional places can have $|x|_v \neq 1$. The main structural theorem about the adeles is as follows.

Theorem 6.52. If K is a global field, then the image of K in the adeles $\mathbb{A}$ under the diagonal mapping $\iota : K \to \mathbb{A}$ is discrete, and the quotient $\mathbb{A}/\iota(K)$ of additive groups is compact.

For a number field the compactness in Theorem 6.52 encodes Lemma 5.17 and the Strong Approximation Theorem. The proof of the theorem is not hard, and we return to it in a moment. In the current discussion Theorem 6.52 is not something to appreciate for its own consequences but instead is a prototype for a corresponding theorem about "ideles" that encodes for number fields the finiteness of the class number and the Dirichlet Unit Theorem.

The construction of the "ideles" of K proceeds similarly to the construction of the adeles. Again we use a restricted direct product, with the set of places as index set. The locally compact Hausdorff space associated to the place v is the multiplicative group $K_v^\times$. For v nonarchimedean, we again let R_v be the valuation ring in K_v, and take the compact open subset of $K_v^\times$ to be the group $R_v^\times$ of units in R_v, i.e., $R_v^\times = \left\{x \in K_v \;\middle|\; |x|_v = 1\right\}$. The group of ideles is the restricted direct product of the groups $K_v^\times$ relative to the compact subgroups $R_v^\times$. The result is a locally compact abelian group, known as the group of **ideles** of K and denoted by $\mathbb{I}_K$ or simply by $\mathbb{I}$.

Warning: As a set, $\mathbb{I}$ coincides with the group of units $\mathbb{A}^\times$. However, the topologies do not match. The topology for $\mathbb{I}$ is finer than the relative topology on $\mathbb{A}^\times$. See Problems 7–8 at the end of the chapter.

If for each $x \in K_{v_0}$, we send x into the tuple $(a_v)_v$ that has $a_{v_0} = x$ and $a_v = 1$ for $v \neq v_0$, then the result is a one-one continuous group homomorphism of $K_v^\times$ into $\mathbb{I}$. As with the ideles we also have a diagonal mapping $\iota : K^\times \to \mathbb{I}$ given by $\iota(x) = (\iota_v(x))_v$; the image is contained in I, since for a nonzero $x \in K$, $|x|_v$ can be unequal to 1 for only finitely many v.

The Artin product formula (Theorem 6.51) and the corresponding result for function fields in one variable over a finite field put a constraint on the image. We define the **absolute value** $|(a_v)_v|$ of an idele $(a_v)_v$ to be the product of the absolute values of the components: $|(a_v)_v| = \prod_v |a_v|_v$. This is well defined because only finitely many factors are allowed to be different from 1. If $\mathbb{I}^1$ denotes the group of ideles of absolute value 1, then $\mathbb{I}^1$ is a closed subgroup of $\mathbb{I}$. The Artin product formula and its function-field analog imply that the image of the diagonal mapping is contained in $\mathbb{I}^1$. The main structural theorem about the ideles is as follows.

Theorem 6.53. If K is a global field, then the image of $K^\times$ in the subgroup $\mathbb{I}^1$ of the ideles $\mathbb{I}$ under the diagonal mapping $\iota : K^\times \to \mathbb{I}$ is discrete, and the quotient group $\mathbb{I}^1/\iota(K^\times)$ is compact.

From now on, we suppose that the global field K is a number field. Let S_∞ be the set of archimedean places. We begin by supplying direct proofs of the discreteness in Theorems 6.52 and 6.53 and of the compactness of the quotient in Theorem 6.52. After some additional discussion we return to prove the compactness of the quotient in Theorem 6.53.

PROOF OF DISCRETENESS OF $\iota(K)$ IN THEOREM 6.52. It is enough to produce a neighborhood U of 0 in $\mathbb{A}$ such that $U \cap \iota(K) = \{0\}$. The set U of all $(x_v)_v \in \mathbb{A}$ such that $|x_v|_v < 1$ for all archimedean places and $|x_v|_v \le 1$ for all nonarchimedean places is an open product set in $\mathbb{A}(S_\infty)$ and hence is an open neighborhood of 0 in $\mathbb{A}$. Since Theorem 6.51 shows that $\prod_v |\iota_v(y)|_v = 1$ for all $y \ne 0$ in K and since $\prod_v |x_v|_v < 1$ for all $(x_v)_v$ in U, $U \cap \iota(K) = \{0\}$. □

PROOF OF DISCRETENESS OF $\iota(K^\times)$ IN THEOREM 6.53. The set U of all $(x_v)_v \in \mathbb{I}$ such that $|x_v - 1|_v < 1$ for all archimedean places and $|x_v - 1|_v \le 1$ for all nonarchimedean places is an open product set in $\mathbb{I}(S_\infty)$ and hence is an open neighborhood of 1 in $\mathbb{I}$. If $(x_v)_v = \iota(y)$ with $y \in K^\times$ and $y \ne 1$, then $x_v - 1 = \iota_v(y-1)$ with $y - 1 \ne 0$, and Theorem 6.51 shows that $\prod_v |\iota_v(y) - 1|_v = \prod_v |\iota_v(y-1)|_v = 1$. The members $(x_v)_v$ of U all have $\prod_v |x_v - 1|_v < 1$, and thus $U \cap \iota(K^\times) = \{1\}$. □

PROOF OF COMPACTNESS OF $\mathbb{A}/\iota(K)$ IN THEOREM 6.52. We begin by observing that

$$\mathbb{A} = \iota(K) + \mathbb{A}(S_\infty), \tag{$*$}$$

i.e., that the set of sums of a member of $\iota(K)$ and a member of $\mathbb{A}(S_\infty)$ exhausts $\mathbb{A}$. In fact, given $(x_v)_v$ in $\mathbb{A}$, we let $v_1, \dots, v_r$ be the finitely many nonarchimedean places for which $|x_{v_j}|_{v_j} > 1$. The Strong Approximation Theorem (Theorem 6.44) applied to the elements $x_{v_1}, \dots, x_{v_r}$ produces a member y of K such that $|\iota_{v_j}(y) - x_{v_j}|_{v_j} < 1$ for $1 \le j \le r$ and such that $|\iota_v(y)|_v \le 1$ for all other nonarchimedean places v. Consequently $|\iota_v(y) - x_v|_v \le 1$ for all nonarchimedean v. This inequality means exactly that $(x_v)_v - \iota(y)$ is in $\mathbb{A}(S_\infty)$. Hence

$$x = \iota(y) + ((x_v)_v - \iota(y))$$

is the required decomposition, and $(*)$ is proved.

In addition, we have

$$\iota(R) = \iota(K) \cap \mathbb{A}(S_\infty). \tag{$**$}$$

In fact, the inclusion $\subseteq$ is clear. For the inclusion $\supseteq$, let y be a member of K such that $\iota(y)$ is in $\mathbb{A}(S_\infty)$. Then $|\iota_v(y)|_v \le 1$ for all nonarchimedean v, and it follows that y is in R.

To prove the compactness, we use the identity $(M+N)/M \cong N/(M\cap N)$ given by the Second Isomorphism Theorem in the category of locally compact abelian groups, taking $M = \iota(K)$ and $N = \mathbb{A}(S_\infty)$. Then $(*)$ shows that $M + N = \mathbb{A}$, and $(**)$ shows that $M \cap N = \iota(R)$. Hence

$$\mathbb{A}/\iota(K) \cong \mathbb{A}(S_\infty)/\iota(R). \tag{$\dagger$}$$

Let us write $\mathbb{A}(S_\infty) = \Omega \times \Delta$, where $\Omega = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = \prod_{v \text{ archimedean}} K_v$ and $\Delta = \prod_{v \text{ nonarchimedean}} R_v$. The mapping $\Phi : K \to \Omega$ defined near the beginning of Section 9 has the property that

$$\iota(R) + (\{0\} \times \Delta) = \Phi(R) \times \Delta.$$

From this equality we obtain

$$\mathbb{A}(S_\infty)/(\iota(R) + (\{0\} \times \Delta) \cong (\Omega \times \Delta)/(\Phi(R) \times \Delta) \cong \Omega/\Phi(R),$$

and Lemma 5.17 shows that this is compact. Since $(\{0\} \times \Delta) \cap \iota(R) = \{0\}$, application of the First Isomorphism Theorem and then the Second Isomorphism Theorem gives

$$\begin{aligned}\big(\mathbb{A}(S_\infty)/\iota(R)\big)\big/\big(\mathbb{A}(S_\infty)/(\iota(R) + (\{0\} \times \Delta)\big) &\cong \big(\iota(R) + (\{0\} \times \Delta)\big)\big/\iota(R) \\ &\cong (\{0\} \times \Delta)/\big((\{0\} \times \Delta) \cap \iota(R)\big) \\ &= \{0\} \times \Delta,\end{aligned}$$

and this is compact also. So the closed subgroup $\mathbb{A}(S_\infty)/(\iota(R) + (\{0\} \times \Delta)$ of $\mathbb{A}(S_\infty)/\iota(R)$ and the quotient by this subgroup are both exhibited as compact, and it follows that $\mathbb{A}(S_\infty)/\iota(R)$ is compact. Application of $(\dagger)$ shows that $\mathbb{A}/\iota(K)$ is compact. □

A first approach to proving the compactness of $\mathbb{I}^1/\iota(K^\times)$ in Theorem 6.53 is to pursue an analogy with the above proof for $\mathbb{A}/\iota(K)$ by showing that multiplicative analogs of $(*)$ and $(**)$ from that proof are valid here:

$$\begin{aligned}\mathbb{I} &\stackrel{?}{=} \iota(K^\times)\,\mathbb{I}(S_\infty), \\ \iota(R^\times) &= \iota(K^\times) \cap \mathbb{I}(S_\infty).\end{aligned}$$

The second of these formulas is fine and is easily proved: The inclusion $\iota(R^\times) \subseteq \iota(K^\times)\cap\mathbb{I}(S_\infty)$ is clear. For the inclusion $\iota(R^\times) \supseteq \iota(K^\times)\cap\mathbb{I}(S_\infty)$, let y be a member of $K^\times$ such that $\iota(y)$ is in $\mathbb{I}(S_\infty)$. Then $|\iota_v(y)|_v = 1$ for all nonarchimedean v, and it follows that y and y^{-1} are in R, hence that y is in $R^\times$.

The difficulty is that an equality $\mathbb{I} \stackrel{?}{=} \iota(K^\times)\,\mathbb{I}(S_\infty)$ holds if and only if the ring R of algebraic integers in K is a principal ideal domain. Let us elaborate on this point, since we will be led by it to the relationship between ideles and the ideal class group that makes ideles useful.

Let us enumerate the nonzero prime ideals of R as $P_1, P_2, \dots$ in some fashion. As was mentioned in Section 2, each nonzero fractional ideal I in K has a finite unique factorization of the form $I = P_{i_1}^{k_{i_1}} \cdots P_{i_m}^{k_{i_m}}$, where $k_{i_1}, \dots, k_{i_m}$ are integers. The mapping that carries I to the tuple $(a_j)_{j\ge1}$ with $a_j = k_{i_l}$ when $j = i_l$ and $a_j = 0$ when j is not in $\{k_{i_1}, \dots, k_{i_m}\}$ is a group isomorphism Ψ from the group $\mathcal{I}$ of fractional ideals onto a free abelian group $\bigoplus_{j=1}^\infty \mathbb{Z}$ of countably infinite rank. Some of these fractional ideals are of the form xR for some $x \in K^\times$, and they are the principal fractional ideals. They form a subgroup $\mathcal{P}$ of $\mathcal{I}$ that is isomorphic to $K^\times$, and the quotient $\mathcal{I}/\mathcal{P}$ is isomorphic to the ideal class group of K, as was shown at the end of Section 2. Theorem 5.19 says that the group $\mathcal{I}/\mathcal{P}$ is a finite group; its order is the **class number** of K.

Meanwhile, suppose that $(x_v)_v$ is a member of the group $\mathbb{I}$ of ideles. To each nonarchimedean place v, Corollary 6.8 associates a unique nonzero prime ideal, which we write as $P_{i(v)}$ for a function $i(\cdot)$. If $q_v = |R/P_{i(v)}|$, then the relationship between the valuation $\mathrm{ord}_v(\cdot)$ and the normalized absolute value associated to $P_{i(v)}$ is $|x_v|_v = q_v^{-\mathrm{ord}_v(x_v)}$. Since $(x_v)_v$ is an idele, there are only finitely many nonarchimedean v's for which $\mathrm{ord}_v(x_v)$ is not 0. We can therefore map $(x_v)_v$ into the tuple of integers $(\mathrm{ord}_v(x_v))_v$ and compose with Ψ^{-1} to obtain a homomorphism of the group $\mathbb{I}$ into the group $\mathcal{I}$ of fractional ideals. In more detail, the mapping from $\mathbb{I}$ to $\bigoplus_{j=1}^\infty \mathbb{Z}$ is given by $(x_v)_v \mapsto (a_j)_{j\ge1}$ with $a_{i(v)} = \mathrm{ord}_v(x_v)$, and then Ψ^{-1} interprets this sequence of integers as the exponents of the appropriate prime ideals. Since any association of members of $K_v^\times$ at finitely many nonarchimedean places can be extended to an idele by making the idele be 1 at the remaining places, this homomorphism of $\mathbb{I}$ into $\mathcal{I}$ is onto $\mathcal{I}$.

Now suppose that the given idele $(x_v)_v$ is of form $\iota(x)$ for some x in $K^\times$. Then the procedure for mapping this idele to a product of powers of the nonzero prime ideals of R is the same as the procedure for decomposing the fractional ideal xR as a product of powers of nonzero prime ideals of R. Consequently our homomorphism descends to a homomorphism

$$\mathbb{I}\big/\iota(K^\times) \longrightarrow \mathcal{I}/\mathcal{P}$$

of the **idele class group** $\mathbb{I}\big/\iota(K^\times)$ onto the (finite) ideal class group $\mathcal{I}/\mathcal{P}$. This is the fundamental fact about the ideles; the displayed homomorphism in effect says that the idele class group refines the information in the ideal class group. The subject of class field theory shows that this refined information is useful.

Under the homomorphism of $\mathbb{I}$ onto $\mathcal{I}$, the kernel consists exactly of $\mathbb{I}(S_\infty)$, the ideles whose components at each nonarchimedean place v are in $R_v^\times$. Thus

$\mathbb{I}/\mathbb{I}(S_\infty) \to \mathcal{I}$ is an isomorphism. Taking into account the effect on $\iota(K^\times)$, we obtain an isomorphism

$$\mathbb{I}\big/\big(\iota(K^\times)\,\mathbb{I}(S_\infty)\big) \cong \mathcal{I}/\mathcal{P}.$$

Returning to our hoped-for equality $\mathbb{I} \stackrel{?}{=} \iota(K^\times)\,\mathbb{I}(S_\infty)$ and comparing with the displayed isomorphism, we see that $\mathbb{I}$ equals $\iota(K^\times)\,\mathbb{I}(S_\infty)$ if and only if $\mathcal{I} = \mathcal{P}$. Equality $\mathcal{I} = \mathcal{P}$ holds if and only if every fractional ideal of K is principal, if and only if every ordinary ideal of R is principal.

Thus we see why a direct analog of the proof of Theorem 6.52 does not work for Theorem 6.53. But at the same time we obtain information about how to give a correct proof. We saw that factoring $\mathbb{I}/\iota(K^\times)$ by $\mathbb{I}(S_\infty)$ leads to the finite group $\mathcal{I}/\mathcal{P}$. We shall see that if we factor $\mathbb{I}/\iota(K^\times)$ by a suitably larger group $\mathbb{I}(S)$ with S still finite, then the quotient is the trivial group. An indication of this fact was in Problems 19–23 at the end of Chapter V, which showed that if we localize R at a large enough finite set of nonzero prime ideals, then the result is a principal ideal domain. In adelic/idelic terms the corresponding procedure is to enlarge S_∞ to a suitable finite set S containing S_∞ and to replace $\mathbb{I}(S_\infty)$ by $\mathbb{I}(S)$; this enlargement has the effect of replacing $R_v^\times$ by $K_v^\times$ at finitely many places v in considering what happens to ideals, and this is exactly what the localization in those problems accomplishes. Thus for a suitable finite set S containing S_∞, we will have an isomorphism

$$\mathbb{I}\big/\big(\iota(K^\times)\,\mathbb{I}(S)\big) \cong \{1\};$$

in other words,

$$\mathbb{I} = \iota(K^\times)\,\mathbb{I}(S)$$

for a suitable finite set S containing S_∞.

One final remark is needed, and then we are ready to carry out the proof of the compactness of $\mathbb{I}^1/\iota(K^\times)$. The remark is that we always have at least one archimedean place, and adjusting an idele suitably at one archimedean place can change it from being in $\mathbb{I}$ to being in the subgroup $\mathbb{I}^1$ of ideles for which $\prod_v |x_v|_v = 1$. The members of $\iota(K^\times)$ are already in this subgroup, but the members of $\mathbb{I}(S)$ need not be. Thus we replace $\mathbb{I}(S)$ by $\mathbb{I}(S) \cap \mathbb{I}^1 = \mathbb{I}^1(S)$, and the above equality becomes

$$\mathbb{I}^1 = \iota(K^\times)\,\mathbb{I}^1(S)$$

for a suitable finite set S.

PROOF OF COMPACTNESS OF $\mathbb{I}^1/\iota(K^\times)$ IN THEOREM 6.53. Let S be as above. Since $\mathbb{I}^1 = \iota(K^\times)\,\mathbb{I}^1(S)$, the Second Isomorphism Theorem gives

$$\mathbb{I}^1/\iota(K^\times) \cong \mathbb{I}^1(S)/(\iota(K^\times)\,\mathbb{I}^1(S)). \tag{$*$}$$

We shall prove that the right side is compact.

Let T be the complement of S_∞ in S, and define

$$\Omega_1^\times = \prod_{v\in S_\infty} K_v^\times, \quad \Omega_2^\times = \prod_{v\in T} K_v^\times, \quad \Delta_2^\times = \prod_{v\in T} R_v^\times, \quad \Delta_3^\times = \prod_{v\notin S} R_v^\times.$$

If E is any subset of $\mathbb{I}(S)$, E^1 will denote the set of members of E of total absolute value 1. Thus for example, $(\Omega_1^\times)^1$ is the set of tuples $(x_v)_{v\in S_\infty}$ with $\prod_{v\in S_\infty} |x_v|_v = 1$.

Let $\Phi : K^\times \to \Omega_1^\times$ be the mapping given in Section 9. Each member u of the group of units $R^\times$ has the property that $|u|_v = 1$ for every nonarchimedean place v. Then it follows from the Artin product formula (Theorem 6.51) that Φ carries $R^\times$ into $(\Omega_1^\times)^1$. One of the two key ingredients in the proof of Theorem 6.51 is the observation that

$$(\Omega_1^\times)^1/\Phi(R^\times) \qquad \text{is compact.} \tag{$**$}$$

In fact, $\Omega_1^\times$ is a product of r_1 copies of $\mathbb{R}^\times$ and r_2 copies of $\mathbb{C}^\times$. The function $\mathrm{Log} : \Omega_1^\times \to \mathbb{R}^{r_1+r_2}$ given by

$$\begin{aligned}\mathrm{Log}(x_1, \dots, x_r, x_{r_1+1}, \dots, x_{r_1+r_2+1}) \\ = (\log|x_1|_\mathbb{R}, \dots, \log|x_{r_1}|_\mathbb{R}, \log|x_{r_1+1}|_\mathbb{C}, \dots, \log|x_{r_1+r_2}|_\mathbb{C})\end{aligned}$$

is a continuous homomorphism of $\Omega_1^\times$ onto $\mathbb{R}^{r_1+r_2}$, and its kernel is compact, being the product of r_1 two-element groups and r_2 circles. The image of $(\Omega_1^\times)^1$ is a hyperplane, and the proof of the Dirichlet Unit Theorem (Theorem 5.13) shows that $\mathrm{Log}(\Omega_1^\times)^1/\mathrm{Log}\Phi(R^\times)$ is compact. Then $(**)$ follows.

The other key ingredient is the finiteness of the class number of K, which was proved as Theorem 5.19. Let h be this class number. For each v in $T = (S_\infty)^c$, let P_v be the corresponding nonzero prime ideal in R. The ideal P_v^h in R is principal, and we let π_v be a generator. This element has the properties that $K_v^\times/\iota_v(\pi_v)^\mathbb{Z} R_v$ is compact and that $|\iota_{v'}(\pi_v)|_{v'} = |\pi_v|_{v'} = 1$ for all nonarchimedean v' with $v' \neq v$. Let

$$\Sigma_2 = \prod_{v\in T} \iota_v(\pi_v)^\mathbb{Z} R_v;$$

this is a subgroup between Δ_2 and Ω_2 such that Ω_2/Σ_2 is compact. Let Π be the subgroup of $K^\times$ given by $\Pi = \prod_{v\in T} \pi_v^\mathbb{Z}$.

The group $\iota(\Pi)$ is certainly a subgroup of $\iota(K^\times)$, and the fact that $|\pi_v|_{v'} = 1$ for $v' \notin S$ implies that $\iota(\Pi)$ is contained in $\mathbb{I}^1(S)$. Each member of $\iota(R^\times)$ has all nonarchimedean absolute values equal to 1, and consequently we have an inclusion $\iota(R^\times)\iota(\Pi) \subseteq \iota(K^\times)\mathbb{I}^1(S)$. In view of $(*)$, $\mathbb{I}^1(S)/(\iota(K^\times)\,\mathbb{I}^1(S))$ is a homomorphic image of

$$\mathbb{I}^1(S)\Big/\big(\iota(R^\times)\iota(\Pi)(\{1\} \times \Delta_2^\times \times \Delta_3^\times)\big), \tag{$\dagger$}$$

and it is therefore enough to prove that (†) is compact.

The members of $\iota(R^\times)$ have all nonarchimedean absolute values equal to 1 and consequently

$$\iota(R^\times)(\{1\} \times \Delta_2^\times \times \Delta_3^\times) = \Phi(R^\times) \times \Delta_2^\times \times \Delta_3^\times.$$

Therefore the quotient of (†) by

$$\mathbb{I}^1(S) \Big/ \big(\iota(\Pi)((\Omega_1^\times)^1 \times \Delta_2^\times \times \Delta_3^\times)\big) \tag{††}$$

is isomorphic to

$$\mathbb{I}^1(S) \Big/ \big(\iota(\Pi)(\Phi(R^\times) \times \Delta_2^\times \times \Delta_3^\times)\big) \Big/ \mathbb{I}^1(S) \Big/ \big(\iota(\Pi)((\Omega_1^\times)^1 \times \Delta_2^\times \times \Delta_3^\times)\big),$$

which in turn is isomorphic to

$$\big(\iota(\Pi)((\Omega_1^\times)^1 \times \Delta_2^\times \times \Delta_3^\times)\big) \Big/ \big(\iota(\Pi)(\Phi(R^\times) \times \Delta_2^\times \times \Delta_3^\times)\big),$$

which is a homomorphic image of

$$((\Omega_1^\times)^1 \times \Delta_2^\times \times \Delta_3^\times) \Big/ (\Phi(R^\times) \times \Delta_2^\times \times \Delta_3^\times) \cong (\Omega_1^\times)^1 / \Phi(R^\times).$$

The right side is compact by (∗∗), and therefore it is enough to prove that (††) is compact.

Let us check that

$$\iota(\Pi)((\Omega_1^\times)^1 \times \Delta_2^\times \times \Delta_3^\times) = (\Omega_1^\times \times \Sigma_2 \times \Delta_3)^1. \tag{‡}$$

The inclusion $\subseteq$ is immediate. Thus suppose that $((\omega_v)_{v\in S_\infty}, (\sigma_v)_{v\in T}, (\delta_v)_{v\notin S})$ lies in the right side of (‡). Since $(\sigma_v)_{v\in T}$ lies in Σ_2, there exists an element π_0 in Π such that $r_v = \iota_v(\pi_0)^{-1}\sigma_v$ lies in R_v for all $v \in T$. Define $(\omega'_v)_{v\in S_\infty}$ in $\Omega_1^\times$ by $\omega'_v = \iota_v(\pi_0)^{-1}\omega_v$. For a suitable $(\delta'_v)_{v\notin S}$, we then have $\iota(\pi_0)((\omega'_v)_{v\in S_\infty}, (r_v)_{v\in T}, (\delta'_v)_{v\notin S}) = ((\omega_v)_{v\in S_\infty}, (\sigma_v)_{v\in T}, (\delta_v)_{v\notin S})$, and (‡) is proved.

Combining (‡) and (††), we see that it is enough to prove that

$$\mathbb{I}^1(S) \Big/ (\Omega_1^\times \times \Sigma_2 \times \Delta_3)^1 \tag{‡‡}$$

is compact. The inclusion of $\mathbb{I}^1(S)$ into $\mathbb{I}(S)$ induces a homomorphism

$$\mathbb{I}^1(S) \Big/ (\Omega_1^\times \times \Sigma_2 \times \Delta_3)^1 \to \mathbb{I}(S) \Big/ (\Omega_1^\times \times \Sigma_2 \times \Delta_3) \tag{§}$$

that is evidently one-one. But it is also onto because if v_0 is an archimedean place and if $(x_v)_v$ is given in $\mathbb{I}(S)$, then we can adjust (x_{v_0}) in such a way that the replacement $(x_v)_v$ has absolute value 1. The adjustment is by a member of $\Omega_1^\times \times \{1\} \times \{1\}$, and thus (§) is onto. The right side of (§) is

$$(\Omega_1^\times \times \Omega_2 \times \Delta_3)/(\Omega_1^\times \times \Sigma_2 \times \Delta_3) \cong \Omega_2/\Sigma_2,$$

and we have arranged that this is compact. Consequently (‡‡) is compact, and the proof is complete. □

11. Problems

1. If F is a complete field with a nonarchimedean absolute value and if $\sum_{n=1}^{\infty} a_n$ is an infinite series whose terms a_n are in F, prove that the series converges in F if and only if $\lim_n a_n = 0$.

2. Let the 2-adic absolute value be imposed on $\mathbb{Q}$. Theorem 6.5 shows that $\mathbb{Z}$ is dense in the subring of $\mathbb{Q}$ consisting of all rationals with odd denominator.
   (a) Find a sequence of integers converging in this metric to $\frac{1}{3}$.
   (b) Generalize the result of (a) by finding an explicit sequence of integers converging in this metric to any given rational ab^{-1}, where a and b are nonzero integers with b odd.

3. For the Dedekind domain $R = \mathbb{Z}$ and its field of fractions $K = \mathbb{Q}$, the ring of units $R^\times$ is just $\{\pm 1\}$, and the set of archimedean places is just $S_\infty = \{\infty\}$. The formula $\iota(R^\times) = \iota(K^\times) \cap \mathbb{I}(S_\infty)$ of Section 10 therefore becomes $\{\iota(\pm 1)\} = \iota(\mathbb{Q}^\times) \cap \big(\mathbb{R}^\times \times \prod_p \mathbb{Z}_p^\times\big)$.
   (a) Verify this formula directly.
   (b) Since $\mathbb{Z}$ is a principal ideal domain, the theory of Section 10 and the above remarks show that $\mathbb{I} = \iota(\mathbb{Q}^\times)\big(\mathbb{R}^\times \times \prod_p \mathbb{Z}_p^\times\big)$. Prove this formula by an explicit construction whose only allowable choice, in view of (a), is a certain sign.

4. Let R be the Dedekind domain $\mathbb{Z}[\sqrt{-5}\,]$.
   (a) Verify for each choice of sign that the ideals $(1 \pm \sqrt{-5}\,, 3)$ and $(1 \pm \sqrt{-5}\,, 2)$ are prime and that $(1 + \sqrt{-5}\,, 2) = (1 - \sqrt{-5}\,, 2)$.
   (b) Find the prime factorizations of the principal ideals $(1 + \sqrt{-5}\,)$ and (3).
   (c) Let P be the prime ideal $P = (1 + \sqrt{-5}\,, 3)$, and let v_P be the valuation of R determined by P. Prove that $v_P\big((1 + \sqrt{-5}\,)/3\big) = 0$.
   (d) Lemma 6.3 shows that $(1 + \sqrt{-5}\,)/3$ can be written as the quotient of two members a and b of R with $v_P(a) = v_P(b) = 0$. Find such a choice of a and b.

5. Let v be a discrete valuation of a field F, let R_v be the valuation ring, and let P_v be the valuation ideal. It was observed after Proposition 6.2 that $1 + P_v^n$ is a group under multiplication for any $n \geq 1$. Prove for $n \geq 1$ that the multiplicative group $(1 + P_v^n)/(1 + P_v^{n+1})$ is isomorphic to the additive group P_v^n / P_v^{n+1} under the mapping induced by $1 + x \mapsto x + P_v^{n+1}$.

6. Derive the finiteness of the class number of a number field K from the compactness of $\mathbb{I}_K^1 / \iota(K^\times)$ given as Theorem 6.53.

Problems 7–8 compare the topology on the ideles $\mathbb{I} = \mathbb{I}_K$ of a number field K with the topology of the adeles $\mathbb{A} = \mathbb{A}_K$. The notation is as in Section 10.

7. For each finite set S of places containing the archimedean places, exhibit the mappings $\mathbb{I}(S) \to K_v$ for $v \in S$ and $\mathbb{I}(S) \to R_v$ for $v \notin S$ as continuous, and deduce that the inclusion $\mathbb{I} \to \mathbb{A}$ is continuous.

8. Let p_n be the n^{th} positive prime in $\mathbb{Z}$, and let $x_n = (x_{n,v})_v$ be the adele in $\mathbb{A}_{\mathbb{Q}}$ with $x_{n,v} = p_n$ if $v = p_n$ and $x_{n,v} = 1$ if $v \neq p_n$. The result is a sequence $\{x_n\}$ of ideles in $\mathbb{I}_{\mathbb{Q}}$. Show that this sequence converges to the idele $(1)_v$ in the topology of the adeles but does not converge in the topology of the ideles.

Problems 9–10 below assume knowledge from measure theory of elementary properties of measures and of the existence–uniqueness theorem for translation-invariant measures (Haar measures) on locally compact abelian groups. The continuity in Problem 10a requires making estimates of integrals.

9. Let G be a locally compact abelian topological group with a Haar measure written as dx, and let Φ be an automorphism of G as a topological group, i.e., an automorphism of the group structure that is also a homeomorphism of G. Prove that there is a positive constant $a(\Phi)$ such that $d(\Phi(x)) = a(\Phi)\,dx$.

10. Let F be a locally compact topological field, and let $F^\times$ be the group of nonzero elements, the group operation being multiplication.
    (a) Let c be in $F^\times$, and define $|c|_F$ to be the constant $a(\Phi)$ from the previous problem when the measure is an additive Haar measure and Φ is multiplication by c. Define $|0|_F = 0$. Prove that $c \mapsto |c|_F$ is a continuous function from F into $[0, +\infty)$ such that $|c_1c_2|_F = |c_1|_F|c_2|_F$.
    (b) If dx is a Haar measure for F as an additive locally compact group, prove that $dx/|x|_F$ is a Haar measure for $F^\times$ as a multiplicative locally compact group.
    (c) Let $F = \mathbb{R}$ be the locally compact field of real numbers. Compute the function $x \mapsto |x|_F$. Do the same thing for the locally compact field $F = \mathbb{C}$ of complex numbers.
    (d) Let $F = \mathbb{Q}_p$ be the locally compact field of p-adic numbers, where p is a prime. Compute the function $x \mapsto |x|_F$.
    (e) For the field $F = \mathbb{Q}_p$ of p-adic numbers, suppose that the ring $\mathbb{Z}_p$ of p-adic integers has additive Haar measure 1. What is the additive Haar measure of the maximal ideal I of $\mathbb{Z}_p$?

Problems 11–14 analyze the structure of complete valued fields whose residue class fields are finite, showing that the only kinds are $\mathfrak{p}$-adic fields and fields of formal Laurent series over a finite field. Let F be a complete valued field with a discrete nonarchimedean valuation, let v be the valuation, let R be the valuation ring, and let $\mathfrak{p}$ be the maximal ideal of R. Suppose that the residue class field $R/\mathfrak{p}$ is finite of order $q = p^m$ for a prime number p. Theorem 6.26 shows that the topology on F is locally compact. The normalized absolute value on F corresponding to v is $|\cdot|_F = q^{-v(\cdot)}$. For some purposes it is convenient to separate the **equal-characteristic case** for F and $R/\mathfrak{p}$ from the **unequal-characteristic case**.

11. Show in the unequal-characteristic case that F has characteristic 0.

12. (a) In both cases, use Hensel's Lemma to show that F has a full set of $(q-1)^{\text{st}}$ roots of unity and that coset representatives in F for $R/\mathfrak{p}$ can be taken to be these elements and 0. Denote this subset of q elements of F by E. The subset E is of course closed under multiplication.
    (b) Show in the equal-characteristic case that E is closed under addition and subtraction and is therefore a subfield of F isomorphic to $\mathbb{F}_q$.

13. In the equal-characteristic case, write $\mathbb{F}_q$ for the subfield of F constructed in Problem 12b, and let t be a generator of the principal ideal $\mathfrak{p}$, so that $v(t) = 1$.
    (a) Show that each nonzero element of R has a convergent infinite-series expansion of the form $\sum_{k=0}^{\infty} a_k t^k$ with all a_k in $\mathbb{F}_q$ and that the value of v on such an element is the smallest $k \geq 0$ such that $a_k \neq 0$.
    (b) Show conversely that every series $\sum_{k=0}^{\infty} a_k t^k$ with all a_k in $\mathbb{F}_q$ lies in R, and conclude that $R \cong \mathbb{F}_q[[t]]$.
    (c) Deduce that F is isomorphic to the field $\mathbb{F}_q((t))$ of formal Laurent series over $\mathbb{F}_q$, the understanding being that each such series involves only finitely many negative powers of t.

14. Let F be an arbitrary complete valued field in the unequal-characteristic case. Since Problem 11 shows F to be of characteristic 0, F contains a subgroup $\mathbb{Q}'$ isomorphic as a field to $\mathbb{Q}$.
    (a) Show that the integer $q = p^m$ in $\mathbb{Q}'$ lies in $\mathfrak{p}$.
    (b) Deduce that the number $v_0 = v(p)$ is positive.
    (c) For each nonzero member $ab^{-1}p^k$ of $\mathbb{Q}'$ for which a and b are integers relatively prime to p, show that $v(ab^{-1}p^k) = kv_0$.
    (d) Deduce that $(\mathbb{Q}', |\cdot|_F^{1/(mv_0)})$ is isomorphic as a valued field to $(\mathbb{Q}, |\cdot|_p)$.
    (e) Let $\overline{\mathbb{Q}'}$ be the closure of $\mathbb{Q}'$ in F, and explain why $(\overline{\mathbb{Q}'}, |\cdot|_F^{1/m})$ is isomorphic as a valued field to $(\mathbb{Q}_p, |\cdot|_p)$.
    (f) Let t be a generator of $\mathfrak{p}$. With E as in Problem 12a, show that each member of F has a unique series expansion $\sum_{k=-N}^{\infty} a_k t^k$ with each a_k in E and with N depending on the element, and show furthermore that every such series expansion converges to an element of F.
    (g) Let $c_1, \ldots, c_l$ with $l = q^{v_0}$ be an enumeration of the elements $\sum_{k=0}^{v_0-1} a_k t^k$ with all a_k in E. Show that to each element x in R corresponds some c_j such that $p^{-1}(x - c_j)$ lies in R. Deduce that every element of R is the sum of a convergent series of the form $\sum_{k=0}^{\infty} c_{j_k} p^k$.
    (h) Explain how it follows from the previous part that F is a finite-dimensional vector space over $\overline{\mathbb{Q}'}$, hence that F is a finite extension of the field $\mathbb{Q}_p$.

Problems 15–19 continue the analysis in Problems 11–14 by examining finite separable extensions of complete valued fields whose residue class fields are finite. The

goal is to prove Proposition 6.38 and Lemmas 6.47 and 6.48. Let F be a complete valued field with a discrete nonarchimedean valuation, let R be the valuation ring, and let $\mathfrak{p}$ be the maximal ideal of R. Suppose that the residue class field $R/\mathfrak{p}$ is finite of order $q = p^m$ for a prime number p. Let K be a finite separable extension of F, put $n = [K : F]$, and let T be the integral closure of R in K. Theorem 6.33 shows that K is a valued field, that it has a unique nonzero prime ideal P, that the valuation ring of K is T, and that the valuation ideal is P. Write f for the dimension of T/P over $R/\mathfrak{p}$, so that T/P has order q^f. Also, write e for the power such that $\mathfrak{p}T = P^e$. It is known from Chapter IX of *Basic Algebra* that $n = ef$. In the equal-characteristic case, there is an especially transparent argument for proving Proposition 6.38, and Problem 15 gives that. Problem 16 gives a less transparent argument that handles both cases at once. The remaining problems address Lemmas 6.47 and 6.48.

15. In the equal-characteristic case, let E be the subset of q elements of F described in Problem 12, and let $\widetilde{E}$ be the corresponding subset of q^f elements of K. Problem 13 shows that E is a field isomorphic to $\mathbb{F}_q$ and that $\widetilde{E}$ is an extension field isomorphic to $\mathbb{F}_{q^f}$. Let t be a generator in R of $\mathfrak{p}$, and let $\widetilde{t}$ be a generator in T of P. Problem 13 shows that $F = \mathbb{F}_q((t))$ and that $K = \mathbb{F}_{q^f}((\widetilde{t}))$.
    (a) Show that the set L of formal Laurent series in t with coefficients from $\mathbb{F}_{q^f}$ is an intermediate field between F and K, so that $L = \mathbb{F}_{q^f}((t))$.
    (b) Why does it follow that the integral closure of R in L is $U = \mathbb{F}_{q^f}[[t]]$ and that the maximal ideal of U is $\wp = tU$?
    (c) Deduce that the residue class field of L is $\mathbb{F}_{q^f}$ of order q^f and that $\wp T = P^e$, so that the residue class degree of L/F is f and the ramification index of K/L is e.
    (d) How can one conclude that L/F is unramified and that K/L is totally ramified?

16. In this problem no distinction is made between the equal-characteristic case and the unequal-characteristic case. Let $\Bbbk_F$ and $\Bbbk_K$ be the residue class fields of F and K, and write $\Bbbk_K = \Bbbk_F(\overline{\alpha})$, where $\overline{\alpha}$ is a root of a monic irreducible polynomial $\overline{g}(X)$ in $\Bbbk_F[X]$. Let $g(X)$ be a monic polynomial in $R[X]$ that reduces modulo $\mathfrak{p}$ to $\overline{g}(X)$.
    (a) Prove that there exists $\alpha \in T$ with $\alpha + P = \overline{\alpha}$ and with $g(\alpha) = 0$.
    (b) With α as in (a), let L be the intermediate field between F and K given by $L = F(\alpha)$, let U be the integral closure of R in L, let $\wp$ be the maximal ideal of U, and let $\Bbbk_L = U/\wp$. Show that α lies in U and that the member $\overline{\alpha}$ of $\Bbbk_K$ is in the image of the natural field map $\Bbbk_L \to \Bbbk_K$.
    (c) Conclude from (b) that $\Bbbk_L = \Bbbk_K$.
    (d) By comparing $[L : K]$, the degrees of $g(X)$ and $\overline{g}(X)$, and the indices e and f for K/F and L/F, prove that L has the properties required by Proposition 6.38.

17. This problem applies to both the equal-characteristic case and the unequal-characteristic case. Let ξ be a member of T such that $K = F(\xi)$, and let $g(X) = X^n + c_1X^{n-1} + \cdots + c_n$ be its minimal polynomial over F.
    (a) Let $N = \sum_{k=0}^{n-1} R\xi^k$. This is a free R submodule of T of rank n with $\{1, \xi, \ldots, \xi^{n-1}\}$ as an R basis. Define
    $$\widehat{N} = \{y \in K \mid \mathrm{Tr}_{K/F}(xy) \text{ is in } R \text{ for all } x \in M\}.$$
    Put $x_i = \xi^{i-1}$ for $1 \le i \le n$. Why is there a unique y_j in K with $\mathrm{Tr}_{K/F}(x_i y_j) = \delta_{ij}$? Show that $\widehat{N}$ is a free R module with $\{y_1, \ldots, y_n\}$ as R basis.
    (b) If A is a matrix in $M_n(R)$ with $\det A = \pm 1$ and if $z_k = \sum_j A_{jk} y_j$, why is $\sum_{k=1}^n Rz_k = \sum_{k=1}^n Ry_k$?
    (c) Let K' be a splitting field of $g(X)$ over F, and let $\xi_1, \ldots, \xi_n$ be the roots of $g(X)$ in K', with $\xi_1 = \xi$. It is known from *Basic Algebra* that $\xi_1, \ldots, \xi_n$ are distinct. Prove that
    $$\sum_{i=1}^n \frac{g(X)}{g'(\xi_i)(X - \xi_i)} = 1$$
    by observing that the difference of the two sides is a polynomial in X of degree at most $n - 1$ and all of $\xi_1, \ldots, \xi_n$ are roots.
    (d) Let σ_j be the field map that fixes F and carries $F(\xi)$ into K' in such a way that $\sigma_j(\xi) = \xi_j$. These mappings have the property that $\mathrm{Tr}_{K/F}(\xi) = \sum_{j=1}^n \sigma_j(\xi)$ for all $\xi \in K$. If $h(X)$ is in the ring $K[[X]]$ of formal power series over K, let $h^{\sigma_j}(X)$ be the polynomial obtained by applying σ_j to each coefficient, and extend $\mathrm{Tr}_{K/F} : K \to F$ to a mapping of $K[[X]]$ to $F[[X]]$ by letting $\mathrm{Tr}_{K/F}\, h(X) = \sum_{j=1}^n h^{\sigma_j}(X)$. By making the substitution $X \mapsto 1/X$ in (c) and using the extended trace function just defined, show that
    $$\frac{X^n}{1 + c_1X + \cdots + c_nX^n} = \mathrm{Tr}_{K/F}\left(\frac{X}{g'(\xi)(1 - \xi X)}\right).$$
    (e) Write the identity in (d) out with power series, equate the coefficients of $X, X^2, \ldots, X^n$ on the two sides, and deduce that $\mathrm{Tr}_{K/F}\left(\xi^{k-1}g'(\xi)^{-1}\right)$ equals 0 for $1 \le k < n$ and equals 1 for $k = n$.
    (f) Form the n-by-n matrix A with $A_{ij} = \mathrm{Tr}_{K/F}\left((\xi^{i-1}g'(\xi)^{-1})(\xi^{j-1})\right)$. The result of (e) shows that this matrix has all entries equal to 0 that lie above the off-diagonal $i + j = n + 1$ and all entries equal to 1 that lie on the off-diagonal. By writing $\xi^{i+j-2} = \xi^n \xi^{i+j-(n+1)-1}$ and by substituting for ξ^n, show that the remaining entries A_{ij} lie in R.
    (g) Combine the conclusions of (a), (b), and (f) to prove that $\widehat{N} = g'(\xi)^{-1}N$.

18. This problem continues with the notation of Problem 17 and assumes in addition that K/F is unramified, i.e., that $f = n$ and $e = 1$. The objective is to prove the assertion of Lemma 6.48 that $\mathcal{D}(K/F) = T$.

(a) Prove that the intermediate field L constructed in Problem 16 is K itself, that the polynomial $g(X)$ is the minimal polynomial of α over F, and that $K = F(\alpha)$.

(b) Let $N = \sum_{k=0}^{n-1} R\alpha^k$. Apply Problem 17 to obtain $\widehat{N} = g'(\alpha)^{-1}N$. Using the inclusion $N \subseteq T$, deduce that $\widehat{N} \supseteq \widehat{T}$, and conclude that $\mathcal{D}(K/F)^{-1} \subseteq g'(\alpha)^{-1}T$.

(c) Prove that $g'(\alpha)$ is a unit in T, and deduce that $\mathcal{D}(K/F) = T$.

19. This problem continues with the notation of Problem 17 and assumes in addition that K/F is totally ramified, i.e., that $e = n$ and $f = 1$. The objective is to prove the assertion of Lemma 6.47 that $\mathcal{D}(K/F) = P^{e'}$ with e' equal to $e - 1$ if p does not divide e and with $e' \geq e$ if p divides e. Let E be the set of representatives in R of the members of $R/\mathfrak{p}$ as constructed in Problem 12. Since $f = 1$, the set E is also a set of representatives in T of the members of T/P. Let v_K and v_F be the respective discrete valuations of K and F, so that $v_F = nv_K\big|_F$ by Proposition 6.34. Let π and λ be respective generators of P and $\mathfrak{p}$.

(a) Prove that if M is a field with a discrete valuation w and if $x_1, \ldots, x_m$ are elements of M with $x_1 + \cdots + x_m = 0$ and $m \geq 2$, then the number of j's for which $w(x_j) = \min_{1 \leq i \leq m} w(x_i)$ is at least 2.

(b) Let $g(X) = c_0X^n + c_1X^{n-1} + \cdots + c_n$ with $c_0 = 1$ be the field polynomial of π over F. Why are all the coefficients c_j in R, and why is $v_K(c_j)$ divisible by n for each j?

(c) Taking into account that π is a root of its field polynomial and applying (a), show that there exist integers i and j with $0 \leq i < j \leq n$ such that $j - i = v_K(c_j) - v_K(c_i)$ and that all other integers k with $0 \leq k \leq n$ have $v_K(c_k\pi^{n-k}) \geq n$.

(d) Using the divisibility conclusion of (b), show that $g(X)$ is an **Eisenstein polynomial** relative to $\mathfrak{p}$ in the sense that $c_0 = 1$, that all of $c_1, \ldots, c_n$ lie in $\mathfrak{p}$, and that c_n does not lie in $\mathfrak{p}^2$.

(e) Conclude from (d) that $g(X)$ is irreducible over F, that $g(X)$ is the minimal polynomial of π over F, and that $K = F(\pi)$.

(f) For each $k \geq 0$, apply the division algorithm to write $k = ni + j$ with $0 \leq j < n = e$, and define $y_k = \lambda^i\pi^j$. Show that every member of T has a unique convergent series expansion as $\sum_{k=0}^{\infty} a_k y_k$ and that all such series expansions have sum in T.

(g) By rewriting the expansion in (f) suitably, show that $\{1, \pi, \ldots, \pi^{n-1}\}$ is an R basis for the free R module T.

(h) By applying Problem 17 with $N = \sum_{k=0}^{n-1} R\pi^k$, prove that $\widehat{T} = g'(\pi)^{-1}T$, and deduce that $\mathcal{D}(K/F) = (g'(\pi))$.

(i) Computing $g'(\pi)$ and applying the valuation v to it, show that $v(g'(\pi)) = e - 1$ if $v(e) = 0$ and that $v(g'(\pi)) \geq e$ if $v(e) > 0$. Explain how this conclusion proves Lemma 6.47.