

Advanced Algebra

Final Version, September, 2007
For Publication by Birkhäuser Boston
Along with a Companion Volume *Basic Algebra*
In the Series

Cornerstones

Selected Pages from Chapter VI: pp. 313–330

Anthony W. Knapp

Copyright © 2007 by Anthony W. Knapp
All Rights Reserved

CHAPTER VI

Rinterpretation 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 adèle 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

$$x^2 - 5 = (x - 1)^2 + 2x - 6 \equiv (x - 1)^2 \pmod{2},$$

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

$$x^2 - 5 = (x - 1)(x + 1) - 4 \equiv (x - 1)(x + 1) \pmod{4},$$

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

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

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 $x^2 - 17 = (x - m)(x + m) \pmod{2^k}$ 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 $m_k^2 \equiv 17 \pmod{2^k}$, 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, $|m_k - m_l|_2 \leq 2^{-(k-1)}$ and $|m_k^2 - 17|_2 \leq 2^{-k}$. 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

¹This 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 $|q_n - q_m|_p < \epsilon_0/2$ 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 $\mathbb{Q} \rightarrow \mathcal{R} \rightarrow \mathcal{R}/\mathcal{I}$ 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

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

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

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

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

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

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 $|x_n|_p \geq \frac{1}{2}|x|_p$ for $n \geq N$. The computation

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

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 $bn - a \equiv 0 \pmod{p^k}$. 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 $0, 1, 2, \dots, p^n - 1$. In fact, every integer z has $z \equiv k \pmod{p^n}$ for some integer $k \in \{0, 1, 2, \dots, p^n - 1\}$. 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 $0, 1, 2, \dots, p^n - 1$. 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 $0, 1, 2, \dots, p^n - 1$. 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. \square

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 $x = p^m ab^{-1}$ 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 \mathbb{k}_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 choices² 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 $(\pi^{-n})P_v^n = \pi^{-n}R_v\pi^nR_v = R_v = P_v^{-n}P_v^n$, 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). \square

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 \mathbb{k}_v has p elements, with the integers $0, 1, \dots, p - 1$ 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 $1 + p^na b^{-1}$, where a and b are integers and b is prime to p . If we write this as $b^{-1}(b + p^na)$, 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.

²Some 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 $b = zb'$. \square

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 $S^{-1}P = P_{v_P}$. \square

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 $xR = P^n Q$, 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 $xR_v = xRR_v = P^n QR_v = P^n R_v = (PR_v)^n = P_v^{en}$, 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 $R_v P$, and (c) showed that $R_v P = P_v$. 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 $P^n + P P_v^n = (P R_v) P_v^{n-1} = P_v P_v^{n-1} = P_v^n$. Since $P \subseteq P_v$, the term $P P_v^n$ 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 $R \rightarrow R_v$, when followed by the passage to the quotient R_v/P_v , descends to the quotient as a field map $R/P \rightarrow R_v/P_v$. 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 $R/P \rightarrow R_v/P_v$ is onto, and (e) is proved. \square

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 . \square

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

³This 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 $\mathbb{k}(X)$, where X is an indeterminate and \mathbb{k}

- (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 \mathbb{k} are regarded as constants, and the interest is only in valuations that are 0 on \mathbb{k}^\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

$$x^n = a_{n-1}x^{n-1} + \dots + a_1x + a_0.$$

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

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

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 . \square

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 \mathbb{k} , 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 $v = v_P$. \square

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 theory⁴ from \mathbb{C} to a general field \mathbb{k} , says that there are no other discrete valuations of interest for this example.

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

⁴For 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 $\mathbb{k}[X]$. Then the only discrete valuations of F that are 0 on the multiplicative group \mathbb{k}^\times of nonzero constant polynomials are the various valuations $v_{(p)}$, where $p(X)$ is a monic prime polynomial in $\mathbb{k}[X]$, 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 \mathbb{k}^\times . First suppose that $v(X) \geq 0$. Being 0 on the coefficients, v is nonnegative on all polynomials. Thus $\mathbb{k}[X]$ is contained in the valuation ring of v , and Theorem 6.5 applies. By (a) in the theorem, the intersection of $\mathbb{k}[X]$ with the valuation ideal is a nonzero prime ideal of $\mathbb{k}[X]$, 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 $\mathbb{k}[X^{-1}]$ has $\mathbb{k}(X)$ 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 $\mathbb{k}[X^{-1}]$. 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 $\mathbb{k}[X]$ 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 $\mathbb{k}[X^{-1}]$ 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 $\mathbb{k}[X]$, 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 $c \in \mathbb{k}^\times$, 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. \square

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

$\mathbb{k}[X]$, let T be the integral closure of $\mathbb{k}[X]$ in K , and let v be a discrete valuation of K that is 0 on the multiplicative group \mathbb{k}^\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 $\mathbb{k}[X^{-1}]$ in K such that $P \cap \mathbb{k}[X^{-1}] = X^{-1}\mathbb{k}[X^{-1}]$ 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 $\mathbb{k}[X]$, 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). \square

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 $\mathcal{C} \rightarrow \mathcal{I}/\mathcal{P}$ 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.