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 \( pT \) in \( T \) when \( p \) is a nonzero prime ideal in \( R \). If \( F_p \) denotes the completion of \( F \) with respect to \( p \), the theorem explains how the tensor product \( K \otimes_F F_p \) splits uniquely as a direct sum of completions of valued fields. The theorem in effect reduces the question of the splitting of \( pT \) in \( T \) to the splitting of \( F_p \) in a complete field in which only one of the prime factors of \( pT \) 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 \(\xi\) 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

\[
x^2 - 5 \equiv (x - 1)^2 + 2x - 6 \equiv (x - 1)^2 \mod 2,
\]

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

\[
x^2 - 5 \equiv (x - 1)(x + 1) - 4 \equiv (x - 1)(x + 1) \mod 4,
\]

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.