Description of the chapters

The chapters of this book are designed to lead the reader in a logical progression from learning the local properties of rings and curves (such as local principal ideal domains and nonsingular points) to understanding the global properties of rings and curves (through the study of class groups and of the Riemann-Roch Theorem).

The first five chapters of the book are "affine" in nature. Basic notions in algebra are introduced and are illustrated with examples coming alternately from number theory and from algebraic geometry. The unifying theme of these first five chapters is the concept of integral closure of a ring. Algebraic number theory studies the integral closure $\mathcal{O}_L$ of the ring of integers $\mathbb{Z}$ in a finite extension $L/\mathbb{Q}$, where L is obtained by adjoining to the field $\mathbb{Q}$ a root α of an irreducible polynomial $f(y) \in \mathbb{Q}[y]$. In algebraic geometry, one associates to a nonsingular plane curve given by an equation $f(x, y) = 0$ ($f \in k[x, y]$, k any field) its ring of functions $B := k[x, y]/(f)$ and its function field L (the field of fractions of the domain B). The field L is obtained by adjoining to the field $k(x)$ a root of the polynomial $f \in k(x)[y]$. If, in addition, $f(x, y)$ is monic in y, then the ring B is nothing but the integral closure of the ring $k[x]$ in L. Both quadruples, $(\mathbb{Z}, \mathbb{Q}, \mathcal{O}_L, L)$ and $(k[x], k(x), B, L)$, are, from a commutative algebra perspective, instances of the same phenomenon. The reader gains insight into both the number theoretic context and the algebraic-geometric context by being able, very early on, to pass easily from one context to the other.

Since this book is not, after all, merely a course in commutative algebra, but is intended to introduce the reader to arithmetic geometry, we also, in the first five chapters, take a geometric perspective and discuss the fact that a ring extension $B/k[x]$ corresponds to a map of plane curves, namely, the projection to the x-axis. This geometric perspective gives the reader added insight by allowing the reader to draw "pictures" of ring extensions/maps of curves and of various concepts attached to extensions, such as ramification.

The local properties of rings and curves having been studied in detail in the first four chapters, Chapter **??** introduces one of the basic global invariants attached to a Dedekind domain, its ideal class group. In addition, Chapter **??** is used to motivate the subsequent study of projective curves (rather than affine curves only) as follows. If one identifies the function-field analogues of the archimedian absolute values of number fields, then one of the standard proofs of the finiteness of the class group for number fields can be used *mutatis mutandis* to prove the finiteness of the class number of the ring of functions on a nonsingular affine curve X over a finite field. In fact, these analogues, one soon discovers, are the absolute values attached to the "points at infinity" of the affine curve X. We thus introduce in Chapter **??** the notions of valuations and absolute values and prove the finiteness of the class group in both the number field case and the function field case as discussed above. This allows us, in Chapter ??, to introduce the notion of projective curve and to relate the algebra introduced in Chapter ?? (the concept of discrete valuation ring) to geometry by establishing, for nonsingular plane curves, the bijection between points on the curve and valuations of its field of functions.

After a study, in Chapter ??, of the geometry of plane projective curves over (mostly) algebraically closed fields, Chapter ?? introduces the reader to the study of curves over non-algebraically closed fields. The motivating problem in this chapter is the problem of counting the solutions of equations over finite fields. The general theory of nonsingular complete curve is developed here in order to apply it later on in Chapter ?? to the case of finite fields.

In Chapter ??, the reader will find the proofs of several important theorems regarding curves over finite fields and their zeta-functions. To motivate the definition of the zeta-function of a curve over a finite field, a short section on the historically older Riemann zeta-function and Dirichlet zeta-functions is included. In that section, the reader is introduced, without proofs, to the main analytic properties of the Dedekind zeta-functions, including the functional equation, the residue at $s = 1$, and the Riemann hypothesis. The analogues for the zeta-functions of curves of these three properties of the Dedekind zeta-functions are proved in full generality in subsequent sections.

Chapter ?? also serves to illustrate the power of a key theorem, the Riemann-Roch Theorem. Indeed, the proofs of the functional equation and of the analogue of the Riemann hypothesis for the zeta-function of a curve make use in an essential way of the Riemann-Roch Theorem. Because the Riemann-Roch Theorem is easily stated, we feel that it is better first to introduce the reader to this theorem "in action" when proving the functional equation of the zeta-function, and then to devote most of Chapter ?? to proving the Riemann-Roch Theorem.

Chapter ?? introduces the reader to a technical difficulty, inseparability, that does not appear in algebraic number theory, nor in algebraic geometry over a field of characteristic zero. Associated to a purely inseparable extension of the field of functions of a curve over a finite field is an endomorphism of the curve called the Frobenius endomorphism. Properties of this endomorphism are studied in this chapter and are used in the last section to prove the analogue of the Riemann hypothesis for curves over finite fields.

Chapter ?? introduces the reader to more advanced topics, such as reduction of curves and Galois representations. This chapter is intended as a general discussion of these topics, with an ample bibliography providing direction and suggested readings for the reader interested in pursuing further study in arithmetic geometry.

The Appendix lists basic facts assumed to be known to the reader, such as Gauss' Lemma and Galois theory.

Conventions

All rings are commutative and have an identity element, denoted by 1. If A is a ring, then A^* denotes the set of units of A.

Let A be a ring contained in a ring B. Let $\alpha \in B$. The smallest subring of B that contains A and α is denoted by $A[\alpha]$. This subring is the image in B of the map $A[x] \to B$, which sends $g(x)$ to $g(\alpha)$.

Let K be a field contained in a ring B. Let $\alpha \in B$. If the map $K[x] \to B$, which sends $g(x)$ to $g(\alpha)$, is not injective, then its image $K[\alpha]$ is a subfield of B denoted by $K(\alpha)$. It is the smallest subfield of B that contains K and α.

A proper ideal of a ring A is an ideal I such that $I \neq A$. A prime ideal is a proper ideal.

A principal ideal domain is a domain A such that every ideal can be generated by a single element and such that A contains a nonzero proper ideal. In particular, a field is not a principal ideal domain.

We say that two elements α, β in a ring A are *congruent modulo an ideal* I of A if $\alpha - \beta \in I$. We denote it by $\alpha \equiv \beta \mod I$.

A glossary of notation used in this book can be found on page ??.