Advanced Algebra

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

Cornerstones

Anthony W. Knapp

CONTENTS

CONTENTS OF *BASIC ALGEBRA*

PREFACE

Advanced Algebra and its companion volume *Basic Algebra* systematically develop concepts and tools in algebra that are vital to every mathematician, whether pure or applied, aspiring or established. The two books together aim to give the reader a global view of algebra, its use, and its role in mathematics as a whole. The idea is to explain what the young mathematician needs to know about algebra in order to communicate well with colleagues in all branches of mathematics.

The books are written as textbooks, and their primary audience is students who are learning the material for the first time and who are planning a career in which they will use advanced mathematics professionally. Much of the material in the two books, including nearly all of *Basic Algebra* and some of *Advanced Algebra*, corresponds to normal course work, with the proportions depending on the university. The books include further topics that may be skipped in required courses but that the professional mathematician will ultimately want to learn by self-study. The test of each topic for inclusion is whether it is something that a plenary lecturer at a broad international or national meeting is likely to take as known by the audience.

Key topics and features of *Advanced Algebra* are as follows:

- Topics build on the linear algebra, group theory, factorization of ideals, structure of fields, Galois theory, and elementary theory of modules developed in *Basic Algebra*.
- Individual chapters treat various topics in commutative and noncommutative algebra, together providing introductions to the theory of associative algebras, homological algebra, algebraic number theory, and algebraic geometry.
- The text emphasizes connections between algebra and other branches of mathematics, particularly topology and complex analysis. All the while, it carries along two themes from *Basic Algebra*: the analogy between integers and polynomials in one variable over a field, and the relationship between number theory and geometry.
- Several sections in two chapters introduce the subject of Gröbner bases, which is the modern gateway toward handling simultaneous polynomial equations in applications.
- The development proceeds from the particular to the general, often introducing examples well before a theory that incorporates them.

- More than 250 problems at the ends of chapters illuminate aspects of the text, develop related topics, and point to additional applications. A separate section "Hints for Solutions of Problems" at the end of the book gives detailed hints for most of the problems, complete solutions for many.

It is assumed that the reader is already familiar with linear algebra, group theory, rings and modules, unique factorization domains, Dedekind domains, fields and algebraic extension fields, and Galois theory at the level discussed in *Basic Algebra*. Not all of this material is needed for each chapter of *Advanced Algebra*, and chapter-by-chapter information about prerequisites appears in the Guide for the Reader beginning on page xvii.

Historically the subjects of algebraic number theory and algebraic geometry have influenced each other as they have developed, and the present book tries to bring out this interaction to some extent. It is easy to see that there must be a close connection. In fact, one number-theory problem already solved by Fermat and Euler was to find all pairs (x, y) of integers satisfying $x^2 + y^2 = n$, where n is a given positive integer. More generally one can consider higher-order equations of this kind, such as $y^2 = x^3 + 8x$. Even this simple change of degree has a great effect on the difficulty, so much so that one is inclined first to solve an easier problem: find the *rational* pairs satisfying the equation. Is the search for rational solutions a problem in number theory or a problem about a curve in the plane? The answer is that really it is both. We can carry this kind of question further. Instead of considering solutions of a single polynomial equation in two variables, we can consider solutions of a system of polynomial equations in several variables. Within the system no individual equation is an intrinsic feature of the problem because one of the equations can always be replaced by its sum with another of the equations; if we regard each equation as an expression set equal to 0, then the intrinsic problem is to study the locus of common zeros of the equations. This formulation of the problem sounds much more like algebraic geometry than number theory.

A doubter might draw a distinction between integer solutions and rational solutions, saying that finding integer solutions is number theory while finding rational solutions is algebraic geometry. Experience shows that this is an artificial distinction. Although algebraic geometry was initially developed as a subject that studies solutions for which the variables take values in a field, particularly in an algebraically closed field, the insistence on working only with fields imposed artificial limitations on how problems could be approached. In the late 1950s and early 1960s the foundations of the subject were transformed by allowing variables to take values in an arbitrary commutative ring with identity. The very end of this book aims to give some idea of what those new foundations are.

Along the way we shall observe parallels between number theory and algebraic geometry, even as we nominally study one subject at a time. The book begins with

a chapter on those aspects of number theory that mark the historical transition from classical number theory to modern algebraic number theory. Chapter I deals with three celebrated advances of Gauss and Dirichlet in classical number theory that one might wish to generalize by means of algebraic number theory. The detailed level of knowledge that one gains about those topics can be regarded as a goal for the desired level of understanding about more complicated problems. Chapter I thus establishes a framework for the whole book.

Associative algebras are the topic of Chapters II and III. The tools for studying such algebras provide methods for classifying noncommutative division rings. One such tool, known as the Brauer group, has a cohomological interpretation that ties the subject to algebraic number theory.

Because of other work done in the 1950s, homology and cohomology can be abstracted in such a way that the theory impacts several fields simultaneously, including topology and complex analysis. The resulting subject is called homological algebra and is the topic of Chapter IV. Having cohomology available at this point of the present book means that one is prepared to use it both in algebraic number theory and in situations in algebraic geometry that have grown out of complex analysis.

The last six chapters are about algebraic number theory, algebraic geometry, and the relationship between them. Chapters V–VI concern the three main foundational theorems in algebraic number theory. Chapter V goes at these results in a direct fashion but falls short of giving a complete proof in one case. Chapter VI goes at matters more indirectly. It explores the parallel between number theory and the theory of algebraic curves, makes use of tools from analysis concerning compactness and completeness, succeeds in giving full proofs of the three theorems of Chapter V, and introduces the modern approach via adeles and ideles to deeper questions in these subject areas.

Chapters VII–X are about algebraic geometry. Chapter VII fills in some prerequisites from the theories of fields and commutative rings that are needed to set up the foundations of algebraic geometry. Chapters VIII–X concern algebraic geometry itself. They come at the subject successively from three points of view—from the algebraic point of view of simultaneous systems of polynomial equations in several variables, from the number-theoretic point of view suggested by the classical theory of Riemann surfaces, and from the geometric point of view.

The topics most likely to be included in normal course work include the Wedderburn theory of semisimple algebras in Chapter II, homological algebra in Chapter IV, and some of the advanced material on fields in Chapter VII. A chart on page xvi tells the dependence of chapters on earlier chapters, and, as mentioned above, the section Guide for the Reader tells what knowledge of *Basic Algebra* is assumed for each chapter.

The problems at the ends of chapters are intended to play a more important

role than is normal for problems in a mathematics book. Almost all problems are solved in the section of hints at the end of the book. This being so, some blocks of problems form additional topics that could have been included in the text but were not; these blocks may be regarded as optional topics, or they may be treated as challenges for the reader. The optional topics of this kind usually either carry out further development of the theory or introduce significant applications to other branches of mathematics. For example a number of applications to topology are treated in this way.

Not all problems are of this kind, of course. Some of the problems are really pure or applied theorems, some are examples showing the degree to which hypotheses can be stretched, and a few are just exercises. The reader gets no indication which problems are of which type, nor of which ones are relatively easy. Each problem can be solved with tools developed up to that point in the book, plus any additional prerequisites that are noted.

The theorems, propositions, lemmas, and corollaries within each chapter are indexed by a single number stream. Figures have their own number stream, and one can find the page reference for each figure from the table on page xv. Labels on displayed lines occur only within proofs and examples, and they are local to the particular proof or example in progress. Each occurrence of the word "PROOF" or "PROOF" is matched by an occurrence at the right margin of the symbol □ to mark the end of that proof.

I am grateful to Ann Kostant and Steven Krantz for encouraging this project and for making many suggestions about pursuing it, and I am indebted to David Kramer, who did the copyediting. The typesetting was by A_MS-TEX, and the figures were drawn with Mathematica.

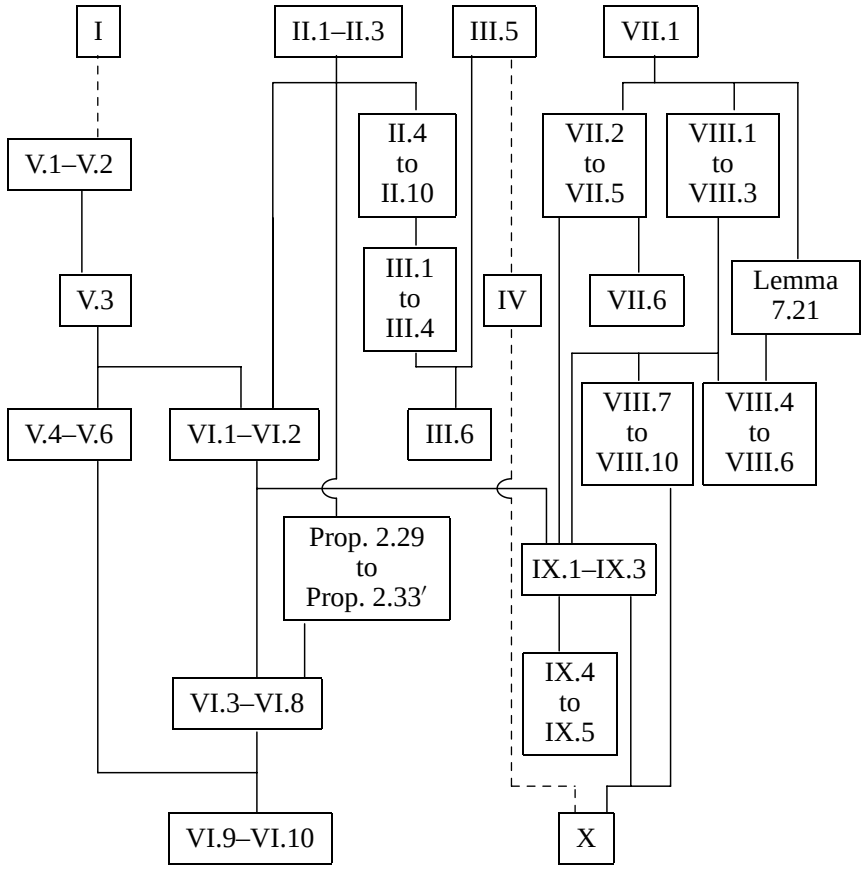
I invite corrections and other comments from readers. I plan to maintain a list of known corrections on my own Web page.

A. W. KNAPP
August 2007

LIST OF FIGURES

DEPENDENCE AMONG CHAPTERS

Below is a chart of the main lines of dependence of chapters on prior chapters. The dashed lines indicate helpful motivation but no logical dependence. Apart from that, particular examples may make use of information from earlier chapters that is not indicated by the chart.



GUIDE FOR THE READER

This section is intended to help the reader find out what parts of each chapter are most important and how the chapters are interrelated. Further information of this kind is contained in the abstracts that begin each of the chapters.

The book treats its subject material as pointing toward algebraic number theory and algebraic geometry, with emphasis on aspects of these subjects that impact fields of mathematics other than algebra. Two chapters treat the theory of associative algebras, not necessarily commutative, and one chapter treats homological algebra; both these topics play a role in algebraic number theory and algebraic geometry, and homological algebra plays an important role in topology and complex analysis. The constant theme is a relationship between number theory and geometry, and this theme recurs throughout the book on different levels.

The book assumes knowledge of most of the content of *Basic Algebra*, either from that book itself or from some comparable source. Some of the less standard results that are needed from *Basic Algebra* are summarized in the section Notation and Terminology beginning on page xxi. The assumed knowledge of algebra includes facility with using the Axiom of Choice, Zorn's Lemma, and elementary properties of cardinality. All chapters of the present book but the first assume knowledge of Chapters I–IV of *Basic Algebra* other than the Sylow Theorems, facts from Chapter V about determinants and characteristic polynomials and minimal polynomials, simple properties of multilinear forms from Chapter VI, the definitions and elementary properties of ideals and modules from Chapter VIII, the Chinese Remainder Theorem and the theory of unique factorization domains from Chapter VIII, and the theory of algebraic field extensions and separability and Galois groups from Chapter IX. Additional knowledge of parts of *Basic Algebra* that is needed for particular chapters is discussed below. In addition, some sections of the book, as indicated below, make use of some real or complex analysis. The real analysis in question generally consists in the use of infinite series, uniform convergence, differential calculus in several variables, and some point-set topology. The complex analysis generally consists in the fundamentals of the one-variable theory of analytic functions, including the Cauchy Integral Formula, expansions in convergent power series, and analytic continuation.

The remainder of this section is an overview of individual chapters and groups of chapters.

Chapter I concerns three results of Gauss and Dirichlet that marked a transition from the classical number theory of Fermat, Euler, and Lagrange to the algebraic number theory of Kummer, Dedekind, Kronecker, Hermite, and Eisenstein. These results are Gauss's Law of Quadratic Reciprocity, the theory of binary quadratic forms begun by Gauss and continued by Dirichlet, and Dirichlet's Theorem on primes in arithmetic progressions. Quadratic reciprocity was a necessary preliminary for the theory of binary quadratic forms. When viewed as giving information about a certain class of Diophantine equations, the theory of binary quadratic forms gives a gauge of what to hope for more generally. The theory anticipates the definition of abstract abelian groups, which occurred later historically, and it anticipates the definition of the class number of an algebraic number field, at least in the quadratic case. Dirichlet obtained formulas for the class numbers that arise from binary quadratic forms, and these formulas led to the method by which he proved his theorem on primes in arithmetic progressions. Much of the chapter uses only elementary results from *Basic Algebra*. However, Sections 6–7 use facts about quadratic number fields, including the multiplication of ideals in their rings of integers, and Section 10 uses the Fourier inversion formula for finite abelian groups, which is in Section VII.4 of *Basic Algebra*. Sections 8–10 make use of a certain amount of real and complex analysis concerning uniform convergence and properties of analytic functions.

Chapters II–III introduce the theory of associative algebras over fields. Chapter II includes the original theory of Wedderburn, including an amplification by E. Artin, while Chapter III introduces the Brauer group and connects the theory with the cohomology of groups. The basic material on simple and semisimple associative algebras is in Sections 1–3 of Chapter II, which assumes familiarity with commutative Noetherian rings as in Chapter VIII of *Basic Algebra*, plus the material in Chapter X on semisimple modules, chain conditions for modules, and the Jordan–Hölder Theorem. Sections 4–6 contain the statement and proof of Wedderburn's Main Theorem, telling the structure of general finite-dimensional associative algebras in characteristic 0. These sections include a relatively self-contained segment from Proposition 2.29 through Proposition 2.33′ on the role of separability in the structure of tensor products of algebras. This material is the part of Sections 4–6 that is used in the remainder of the chapter to analyze finite-dimensional associative division algebras over fields. Two easy consequences of this analysis are Wedderburn's Theorem that every finite division ring is commutative and Frobenius's Theorem that the only finite-dimensional associative division algebras over $\mathbb{R}$ are $\mathbb{R}$, $\mathbb{C}$, and the algebra $\mathbb{H}$ of quaternions, up to $\mathbb{R}$ isomorphism.

Chapter III introduces the Brauer group to parametrize the isomorphism classes of finite-dimensional associative division algebras whose center is a given field. Sections 2–3 exhibit an isomorphism of a relative Brauer group with what turns

out to be a cohomology group in degree 2. This development runs parallel to the theory of factor sets for groups as in Chapter VII of *Basic Algebra*, and some familiarity with that theory can be helpful as motivation. The case that the relative Brauer group is cyclic is of special importance, and the theory is used in the problems to construct examples of division rings that would not have been otherwise available. The chapter makes use of material from Chapter X of *Basic Algebra* on the tensor product of algebras and on complexes and exact sequences.

Chapter IV is about homological algebra, with emphasis on connecting homomorphisms, long exact sequences, and derived functors. All but the last section is done in the context of "good" categories of unital left R modules, R being a ring with identity, where it is possible to work with individual elements in each object. The reader is expected to be familiar with some example for motivation; this can be knowledge of cohomology of groups at the level of Section III.5, or it can be some experience from topology or from the cohomology of Lie algebras as treated in other books. Knowledge of complexes and exact sequences from Chapter X of *Basic Algebra* is prerequisite. Homological algebra properly belongs in this book because it is fundamental in topology and complex analysis; in algebra its role becomes significant just beyond the level of the current book. Important applications are not limited in practice to "good" categories; "sheaf" cohomology is an example with significant applications that does not fit this mold. Section 8 sketches the theory of homological algebra in the context of "abelian" categories. In this case one does not have individual elements at hand, but some substitute is still possible; sheaf cohomology can be treated in this context.

Chapters V and VI are an introduction to algebraic number theory. The theory of Dedekind domains from Chapters VIII and IX of *Basic Algebra* is taken as known, along with knowledge of the ingredients of the theory—Noetherian rings, integral closure, and localization. Both chapters deal with three theorems—the Dedekind Discriminant Theorem, the Dirichlet Unit Theorem, and the finiteness of the class number. Chapter V attacks these directly, using no additional tools, and it comes up a little short in the case of the Dedekind Discriminant Theorem. Chapter VI introduces tools to get around the weakness of the development in Chapter V. These tools are valuations, completions, and decompositions of tensor products of fields with complete fields. Chapter VI makes extensive use of metric spaces and completeness, and compactness plays an important role in Sections 9–10. As noted in remarks with Proposition 6.7, Section VI.2 takes for granted that Theorem 8.54 of *Basic Algebra* about extensions of Dedekind domains does not need separability as a hypothesis; the actual proof of the improved theorem without a hypothesis of separability is deferred to Section VII.3.

Chapter VII supplies additional background needed for algebraic geometry, partly from field theory and partly from the theory of commutative rings. Knowledge of Noetherian rings is needed throughout the chapter. Sections 4–5 assume

knowledge of localizations, and the indispensable Corollary 7.14 in Section 3 concerns Dedekind domains. The most important result is the Nullstellensatz in Section 1. Transcendence degree and Krull dimension in Sections 2 and 4 are tied to the notion of dimension in algebraic geometry. Zariski's Theorem in Section 5 is tied to the notion of singularities; part of its proof is deferred to Chapter X. The material on infinite Galois groups in Section 6 has applications to algebraic number theory and algebraic geometry but is not used in this book after Chapter VII.

Chapters VIII–X introduce algebraic geometry from three points of view. Chapter VIII approaches it as an attempt to understand solutions of simultaneous polynomial equations in several variables using module-theoretic tools. Chapter IX approaches the subject of curves as an outgrowth of the complex-analysis theory of compact Riemann surfaces and uses number-theoretic methods. Chapter X approaches its subject matter geometrically, using the field-theoretic and ring-theoretic tools developed in Chapter VII. All three chapters assume knowledge of Section VII.1 on the Nullstellensatz.

Chapter VIII is in three parts. Sections 1–4 are relatively elementary and concern the resultant and preliminary forms of Bezout's Theorem. Sections 5–6 concern intersection multiplicity for curves and make extensive use of localizations; the goal is a better form of Bezout's Theorem. Sections 7–10 are independent of Sections 5–6 and introduce the theory of Gröbner bases. This subject was developed comparatively recently and lies behind many of the symbolic manipulations of polynomials that are possible with computers.

Chapter IX concerns irreducible curves and is in two parts. Sections 1–3 define divisors and the genus of such a curve, while Sections 4–5 prove the Riemann–Roch Theorem and give applications of it. The tool for the development is discrete valuations as in Section VI.2, and the parallel between the theory in Chapter VI for algebraic number fields and the theory in Chapter IX for curves becomes more evident than ever. Some complex analysis is needed to understand the motivation in Sections 1 and 4.

Chapter X largely concerns algebraic sets defined as zero loci over an algebraically closed field. The irreducible such sets are called varieties. Sections 1–3 are concerned with algebraic sets and their dimension, Sections 4–6 treat maps between varieties, and Sections 7–8 deal with finer questions. Sections 9–12 are independent of Sections 6–8 and do two things simultaneously: they tie the theoretical work on dimension to the theory of Gröbner bases in Chapter VIII, making dimension computable, and they show how the dimension of a zero locus is affected by adding one equation to the defining system. The chapter concludes with an introductory section about schemes, in which the underlying algebraically closed field is replaced by a commutative ring with identity. The entire chapter assumes knowledge of elementary point-set topology.

NOTATION AND TERMINOLOGY

This section contains some items of notation and terminology from *Basic Algebra* that are not necessarily reviewed when they occur in the present book. A few results are mentioned as well. The items are grouped by topic.

Set theory

$\in$	membership symbol
$\#S$ or $\|S\|$	number of elements in S
$\varnothing$	empty set
$\{x \in E \mid P\}$	the set of x in E such that P holds
E^c	complement of the set E
$E \cup F,\ E \cap F,\ E - F$	union, intersection, difference of sets
$\bigcup_\alpha E_\alpha,\ \bigcap_\alpha E_\alpha$	union, intersection of the sets E_α
$E \subseteq F,\ E \supseteq F$	containment
$E \subsetneqq F,\ E \supsetneqq F$	proper containment
$(a_1, \ldots, a_n)$	ordered n-tuple
$\{a_1, \ldots, a_n\}$	unordered n-tuple
$f : E \to F,\ x \mapsto f(x)$	function, effect of function
$f \circ g$ or $fg,\ f\big\|_E$	composition of f following g, restriction to E
$f(\cdot, y)$	the function $x \mapsto f(x, y)$
$f(E),\ f^{-1}(E)$	direct and inverse image of a set
in one-one correspondence	matched by a one-one onto function
countable	finite or in one-one correspondence with integers
2^A	set of all subsets of A

Number systems

δ_{ij}	Kronecker delta: 1 if $i = j$, 0 if $i \neq j$
$\binom{n}{k}$	binomial coefficient
n positive, n negative	$n > 0$, $n < 0$
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	integers, rationals, reals, complex numbers
max, min	maximum/minimum of finite subset of reals
$[x]$	greatest integer $\leq x$ if x is real
Re z, Im z	real and imaginary parts of complex z
$\bar{z}$	complex conjugate of z
$\|z\|$	absolute value of z

Linear algebra and elementary number theory

$\mathbb{F}^n$	space of n-dimensional column vectors
e_j	j^{th} standard basis vector of $\mathbb{F}^n$
V'	dual vector space of vector space V
$\dim_{\mathbb{F}} V$ or $\dim V$	dimension of vector space V over field $\mathbb{F}$
0	zero vector, matrix, or linear mapping
1 or I	identity matrix or linear mapping
A^t	transpose of A
$\det A$	determinant of A
$[M_{ij}]$	matrix with $(i, j)^{\text{th}}$ entry M_{ij}
$\binom{L}{\Delta\ \Gamma}$	matrix of L relative to domain ordered basis Γ and range ordered basis Δ
$x \cdot y$	dot product
$\cong$	is isomorphic to, is equivalent to
$\mathbb{F}_p$	integers modulo a prime p, as a field
GCD	greatest common divisor
$\equiv$	is congruent to
φ	Euler's φ function

Groups, rings, modules, and categories

0	additive identity in an abelian group
1	multiplicative identity in a group or ring
$\cong$	is isomorphic to, is equivalent to
C_m	cyclic group of order m
unit	invertible element in ring R with identity
$R^\times$	group of units in ring R with identity
R^n	space of column vectors with entries in ring R
R^o	opposite ring to R with $a \circ b = ba$
$M_{mn}(R)$	m-by-n matrices with entries in R
$M_n(R)$	n-by-n matrices with entries in R
unital left R module	left R module M with $1m = m$ for all $m \in M$
$\text{Hom}_R(M, N)$	group of R homomorphisms from M into N
$\text{End}_R(M)$	ring of R homomorphisms from M into M
$\ker \varphi$, $\text{image}\, \varphi$	kernel and image of φ
$H^n(G, N)$	n^{th} cohomology of group G with coefficients in abelian group N
simple left R module	nonzero unital left R module with no proper nonzero R submodules
semisimple left R module	sum (= direct sum) of simple left R modules
$\text{Obj}(\mathcal{C})$	class of objects for category $\mathcal{C}$
$\text{Morph}_{\mathcal{C}}(A, B)$	set of morphisms from object A to object B

Groups, rings, modules, and categories, continued

1_A	identity morphism on A
$\mathcal{C}^S$	category of S-tuples of objects from Obj($\mathcal{C}$)
product of $\{X_s\}_{s\in S}$	$(X, \{p_s\}_{s\in S})$ such that if A in Obj($\mathcal{C}$) and $\{\varphi_s \in \mathrm{Morph}_{\mathcal{C}}(A, X_s)\}$ are given, then there exists a unique $\varphi \in \mathrm{Morph}_{\mathcal{C}}(A, X)$ with $p_s\varphi = \varphi_s$ for all s
coproduct of $\{X_s\}_{s\in S}$	$(X, \{i_s\}_{s\in S})$ such that if A in Obj($\mathcal{C}$) and $\{\varphi_s \in \mathrm{Morph}_{\mathcal{C}}(X_s, A)\}$ are given, then there exists a unique $\varphi \in \mathrm{Morph}_{\mathcal{C}}(X, A)$ with $\varphi i_s = \varphi_s$ for all s
$\mathcal{C}^{\mathrm{opp}}$	category opposite to $\mathcal{C}$

Commutative rings R with identity and factorization of elements

identity	denoted by 1, allowed to equal 0
ideal $I = (r_1, \ldots, r_n)$	ideal generated by $r_1, \ldots, r_n$
prime ideal I	*proper* ideal with $ab \in I$ implying $a \in I$ or $b \in I$
integral domain	R with no zero divisors and with $1 \neq 0$
R/I with I prime	always an integral domain
GL(n, R)	group of invertible n-by-n matrices, entries in R
Chinese Remainder Theorem	$I_1, \ldots, I_n$ given ideals with $I_i + I_j = R$ for $i \neq j$. Then the natural map $\varphi : R \to \prod_{j=1}^n R/I_j$ yields isomorphism $R\big/\bigcap_{j=1}^n I_j \cong R/I_1 \times \cdots \times R/I_n$ of rings. Also $\bigcap_{j=1}^n I_j = I_1 \cdots I_n$.
Nakayama's Lemma	If I is an ideal contained in all maximal ideals and M is a finitely generated unital R module with $IM = M$, then $M = 0$.
algebra A over R	unital R module with an R bilinear multiplication $A \times A \to A$. In this book nonassociative algebras appear only in Chapter II, and each associative algebra has an identity.
RG	group algebra over R for group G
$R[X_1, \ldots, X_n]$	polynomial algebra over R with n indeterminates
$R[x_1, \ldots, x_n]$	R algebra generated by $x_1, \ldots, x_n$
irreducible element $r \neq 0$	$r \notin R^\times$ such that $r = ab$ implies $a \in R^\times$ or $b \in R^\times$
prime element $r \neq 0$	$r \notin R^\times$ such that whenever r divides ab, then r divides a or r divides b
irreducible vs. prime	prime implies irreducible; in any unique factorization domain, irreducible implies prime
GCD	greatest common divisor in unique factorization domain

Fields

$\mathbb{F}_q$	a finite field with $q = p^n$ elements, p prime
K/F	an extension field K of a field F
$[K : F]$	degree of extension K/F, i.e., $\dim_F K$
$K(X_1, \ldots, X_n)$	field of fractions of $K[X_1, \ldots, X_n]$
$K(x_1, \ldots, x_n)$	field generated by K and $x_1, \ldots, x_n$
number field	finite-dimensional field extension of $\mathbb{Q}$
$\mathrm{Gal}(K/F)$	Galois group, automorphisms of K fixing F
$N_{K/F}(\cdot)$ and $\mathrm{Tr}_{K/F}(\cdot)$	norm and trace functions from K to F

Tools for algebraic number theory and algebraic geometry

Noetherian R	commutative ring with identity whose ideals satisfy the ascending chain condition; has the property that any R submodule of a finitely generated unital R module is finitely generated.
Hilbert Basis Theorem	R nonzero Noetherian implies $R[X]$ Noetherian

Integral closure

Situation: R = integral domain, F = field of fractions, K/F = extension field.

$x \in K$ integral over R	x is a root of a monic polynomial in $R[X]$
integral closure of R in K	set of $x \in K$ integral over R, is a ring
R integrally closed	R equals its integral closure in F

Localization

Situation: R = commutative ring with identity, S = multiplicative system in R.

$S^{-1}R$	localization, pairs (r, s) with $r \in R$ and $s \in S$, modulo $(r, s) \sim (r', s')$ if $t(rs' - sr') = 0$ for some $t \in S$
property of $S^{-1}R$	$I \mapsto S^{-1}I$ is one-one from set of ideals I in R of form $I = R \cap J$ onto set of ideals in $S^{-1}R$
local ring	commutative ring with identity having a unique maximal ideal
R_P for prime ideal P	localization with S = complement of P in R
Dedekind domain	Noetherian integrally closed integral domain in which every nonzero prime ideal is maximal, has unique factorization of nonzero ideals as product of prime ideals
Dedekind domain extension	R Dedekind, F field of fractions, K/F finite separable extension, T integral closure of R in K. Then T is Dedekind, and any nonzero prime ideal $\wp$ in R has $\wp R = \prod_{i=1}^{g} P_i^{e_i}$ for distinct prime ideals P_i with $P_i \cap R = \wp$. These have $\sum_{i=1}^{g} e_i f_i = [K : F]$, where $f_i = [T/P_i : R/\wp]$.