ALGEBRAIC NUMBERS

By SERGE LANG

ADDISON-WESLEY SERIES IN MATHEMATICS

ALGEBRAIC NUMBERS

SERGE LANG
Columbia University, New York, New York

ADDISON-WESLEY PUBLISHING COMPANY, INC.
READING, MASS. · PALO ALTO · LONDON

Library of Congress Catalog Card No. 64–10374

ALGEBRAIC NUMBERS

This book is in the

ADDISON-WESLEY SERIES IN MATHEMATICS

LYNN H. LOOMIS
Consulting Editor

Foreword

The purpose of this book is to give an exposition of the classical and basic algebraic and analytic number theory. For lack of reference, I was forced to include a minimum of the algebraic theory in *Diophantine Geometry*. What is done there is very skeletal, and it seemed worth while to give a more substantial treatment, which could serve, among other things, as an introduction to the Artin-Tate notes on class field theory [3].

On the other hand, aside from the classical theory of integral closure, discrete valuation rings, different and discriminant, I have supplemented the unit and class number theorem by the standard Minkowski estimate for the discriminant, and the Artin-Whaples estimate of field elements in parallelotopes by a more precise asymptotic estimate. Both of these tend towards the quantitative point of view (as distinguished from the qualitative point of view of *Diophantine Geometry*, quoted as DG).

The four chapters on analytic number theory reproduce with no essential changes four works in or out of the literature, concerned with the zeta function and L-functions of a number field:

Tate's thesis, still unpublished, in Chapter VII.

The treatment of the density theorems for primes in generalized arithmetic progressions given in a seminar by Artin some 12 years ago.

Brauer's paper [5] proving the Siegel conjecture on the asymptotic estimate $\log (hR) \sim \log d^{1/2}$.

Weil's formulation of the explicit formulas for primes [10].

In a certain sense, the plan of the book is still that used more or less by Hilbert in his Bericht [6], although of course both the algebraic and the analytic aspects of number theory have been updated (and the class field theory is omitted). The Bericht contains a large number of computations and examples which still make it very pleasurable to read. Expositions of the theory of number fields are principally conditioned by it, and by Artin's *Algebraic numbers and algebraic functions* (and Artin's unpublished seminars). The point of view is global, and we deal with local fields only incidentally. For a more complete treatment of these, cf. Serre's book [8]. There is much to be said for a direct global approach to number fields, and I have even inserted the main lemma used by Artin in his original proof of the reciprocity law. I hope that the reader will thereby acquire some insight distinct from that exhibited by alternative approaches.

Serge Lang

New York, 1963

Prerequisites

Chapters I through V are self-contained, assuming only elementary algebra, say at the level of Galois theory. I have also taken for granted some elementary theorems concerning absolute values, which are stated in full, but whose simple proofs can be found in DG, Chapter I, and belong properly to a basic course in algebra. Chapter VI uses the language of point set topology (and little more).

The chapters on analytic number theory assume some analysis. Chapter VII assumes Fourier analysis on locally compact groups. Chapters VIII through X assume only standard analytical facts (we even prove some of them) except for one allusion to the Plancherel formula in Chapter X.

In the course of the Brauer-Siegel theorem, we use the formalism of L-series and characters. The theorems which are assumed without proof are always explicitly stated and should cause no trouble to a reader who has reached that stage of the book.

The word *ring* will always mean commutative ring without zero divisor and with unit element (unless otherwise specified).

If K is a field, then K^* denotes its multiplicative group, and $\overline{K}$ its algebraic closure. If f is a polynominal, then f' is either its formal derivative, or the reduction of f modulo a homomorphism. The context will always make clear what is meant.

We use the o and O notation. If f, g are two functions of a real variable, and g is always $\geqq 0$, we write $f = O(g)$ if there exists a constant $C > 0$ such that $|f(x)| \leqq Cg(x)$ for all sufficiently large x. We write $f = o(g)$ if $\lim_{x\to\infty} f(x)/g(x) = 0$. We write $f \sim g$ if $\lim_{x\to\infty} f(x)/g(x) = 1$.

Contents

CHAPTER V

Parallelotopes

CHAPTER VI

Ideles and Adeles

CHAPTER VII

Functional Equation

CHAPTER VIII

Density of Primes and Tauberian Theorem

CHAPTER IX

The Brauer-Siegel Theorem

CHAPTER X

Explicit Formulas

CHAPTER I

Algebraic Integers

This chapter describes the basic aspects of the ring of algebraic integers in a number field (always assumed to be of finite degree over the rational numbers $\mathbf{Q}$). This includes the general prime ideal structure.

Some proofs are given in a more general context, but only when they could not be made shorter by specializing the hypothesis to the concrete situation we have in mind. It is not our intention to write a treatise on commutative algebra.

§1. *Localization*

Let A be a ring. By a *multiplicative subset* of A we mean a subset containing 1 and such that, whenever two elements x, y lie in the subset, then so does the product xy. We shall also assume throughout that 0 does not lie in the subset.

Let K be the quotient field of A, and let S be a multiplicative subset of A. By $S^{-1}A$ we shall denote the set of quotients x/s with x in A and s in S. It is a ring, and A has a canonical inclusion in $S^{-1}A$.

If M is an A-module contained in some field L (containing K), then $S^{-1}M$ denotes the set of elements v/s with $v \in M$ and $s \in S$. Then $S^{-1}M$ is an $S^{-1}A$-module in the obvious way. We shall sometimes consider the case when M is a ring containing A as subring.

Let $\mathfrak{p}$ be a prime ideal of A (by definition, $\mathfrak{p} \neq A$). Then the complement of $\mathfrak{p}$ in A, denoted by $A - \mathfrak{p}$, is a multiplicative subset $S = S_{\mathfrak{p}}$ of A, and we shall denote $S^{-1}A$ by $A_{\mathfrak{p}}$.

A *local ring* is a ring which has a unique maximal ideal. If $\mathfrak{o}$ is such a ring, and $\mathfrak{m}$ its maximal ideal, then any element x of $\mathfrak{o}$ not lying in $\mathfrak{m}$ must be a unit, because otherwise, the principal ideal $x\mathfrak{o}$ would be contained in a maximal ideal unequal to $\mathfrak{m}$. Thus $\mathfrak{m}$ is the set of non-units of $\mathfrak{o}$.

The ring $A_{\mathfrak{p}}$ defined above is a local ring. As can be verified at once, its maximal ideal $\mathfrak{m}_{\mathfrak{p}}$ consists of the quotients x/s, with x in $\mathfrak{p}$ and s in $\mathfrak{o}$ but not in $\mathfrak{p}$.

We observe that $\mathfrak{m}_{\mathfrak{p}} \cap A = \mathfrak{p}$. The inclusion $\supset$ is clear. Conversely, if an element $y = x/s$ lies in $\mathfrak{m}_{\mathfrak{p}} \cap A$ with $x \in \mathfrak{p}$ and $s \in S$, then $x = sy \in \mathfrak{p}$ and $s \notin \mathfrak{p}$. Hence $y \in \mathfrak{p}$.

Let A be a ring and S a multiplicative subset. Let $\mathfrak{a}'$ be an ideal of $S^{-1}A$. Then

$$\mathfrak{a}' = S^{-1}(\mathfrak{a}' \cap A).$$

The inclusion $\supset$ is clear. Conversely, let $x \in \mathfrak{a}'$. Write $x = a/s$ with some $a \in A$ and $s \in S$. Then $sx \in \mathfrak{a}' \cap A$, whence $x \in S^{-1}(\mathfrak{a}' \cap A)$.

Under multiplication by S^{-1}, the multiplicative system of ideals of A is mapped homomorphically onto the multiplicative system of ideals of $S^{-1}A$. This is another way of stating what we have just proved. If $\mathfrak{a}$ is an ideal of A and $S^{-1}\mathfrak{a}$ is the unit ideal, then it is clear that $\mathfrak{a} \cap S$ is not empty, or as we shall also say, $\mathfrak{a}$ *meets* S.

§2. *Integral closure*

Let A be a ring and x an element of some field L containing A. We shall say that x is *integral* over A if either one of the following conditions is satisfied.

INT 1. *There exists a finitely generated non-zero A-module $M \subset L$ such that $xM \subset M$.*

INT 2. *The element x satisfies an equation*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

with coefficients $a_i \in A$, and an integer $n \geqq 1$. (Such an equation will be called an *integral equation*.)

The two conditions are actually equivalent. Indeed, assume INT 2. The module M generated by $1, x, \ldots, x^{n-1}$ is mapped into itself by the element x. Conversely, assume there exists $M = \langle v_1, \ldots, v_n \rangle$ such that $xM \subset M$, and $M \neq 0$. Then

$$\begin{aligned} xv_1 &= a_{11}v_1 + \cdots + a_{1n}v_n \\ &\vdots \\ xv_n &= a_{n1}v_1 + \cdots + a_{nn}v_n \end{aligned}$$

with coefficients a_{ij} in A. Transposing $xv_1, \ldots, xv_n$ to the right-hand side of these equations, we conclude that the determinant

$$\begin{vmatrix} x - a_{11} & & & a_{ij} \\ & x - a_{22} & & \\ & & \ddots & \\ a_{ij} & & & x - a_{nn} \end{vmatrix}$$

is equal to 0. In this way we get an integral equation for x over A.

PROPOSITION 1. *Let A be a ring, K its quotient field, and x algebraic over K. Then there exists an element $c \neq 0$ of A such that cx is integral over A.*

Proof. There exists an equation

$$a_n x^n + \cdots + a_0 = 0$$

with $a_i \in A$ and $a_n \neq 0$. Multiply it by a_n^{n-1}. Then

$$(a_n x)^n + \cdots + a_0 a_n^{n-1} = 0$$

is an integral equation for $a_n x$ over A.

Let B be a ring containing A. We shall say that B is *integral* over A if every element of B is integral over A.

PROPOSITION 2. *If B is integral over A and finitely generated as an A-algebra, then B is a finitely generated A-module.*

Proof. We may prove this by induction on the number of ring generators, and thus we may assume that $B = A[x]$ for some element x integral over A. But we have already seen that our assertion is true in that case.

PROPOSITION 3. *Let $A \subset B \subset C$ be three rings. If B is integral over A and C is integral over B, then C is integral over A.*

Proof. Let $x \in C$. Then x satisfies an integral equation

$$x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$$

with $b_i \in B$. Let $B_1 = A[b_0, \ldots, b_{n-1}]$. Then B_1 is a finitely generated A-module by Proposition 2, and $B_1[x]$ is a finitely generated B_1-module, whence a finitely generated A-module. Since multiplication by x maps $B_1[x]$ into itself, it follows that x is integral over A.

PROPOSITION 4. *Let $A \subset B$ be two rings, and B integral over A. Let σ be a homomorphism of B. Then $\sigma(B)$ is integral over $\sigma(A)$.*

Proof. Apply σ to an integral equation satisfied by any element x of B. It will be an integral equation for $\sigma(x)$ over $\sigma(A)$.

The above proposition is used frequently when σ is an isomorphism and is particularly useful in Galois theory.

PROPOSITION 5. *Let A be a ring contained in a field L. Let B be the set of elements of L which are integral over A. Then B is a ring, called the integral closure of A in L.*

Proof. Let x, y lie in B, and let M, N be two finitely generated A-modules such that $xM \subset M$ and $yN \subset N$. Then MN is finitely generated, and is mapped into itself by multiplication with $x \pm y$ and xy.

COROLLARY. *Let A be a ring, K its quotient field, and L a finite separable extension of K. Let x be an element of L which is integral over A. Then*

the norm and trace of x from L to K are integral over A, and so are the coefficients of the irreducible polynomial satisfied by x over K.

Proof. For each isomorphism σ of L over K, σx is integral over A. Since the norm is the product of σx over all such σ, and the trace is the sum of σx over all such σ, it follows that they are integral over A. Similarly, the coefficients of the irreducible polynomial are obtained from the elementary symmetric functions of the σx, and are therefore integral over A.

A ring A is said to be *integrally closed in a field L* if every element of L which is integral over A in fact lies in A. It is said to be *integrally closed* if it is integrally closed in its quotient field.

PROPOSITION 6. *Let A be a Noetherian ring, integrally closed. Let L be a finite separable extension of its quotient field K. Then the integral closure of A in L is finitely generated over A.*

Proof. It will suffice to show that the integral closure of A is contained in a finitely generated A-module, because A is assumed to be Noetherian.

Let $w_1, \ldots, w_n$ be a linear basis of L over K. After multiplying each w_i by a suitable element of A, we may assume without loss of generality that the w_i are integral over A (Proposition 1). The trace Tr from L to K is a K-linear map of L into K, and is non-degenerate (i.e. there exists an element $x \in L$ such that $\mathrm{Tr}(x) \neq 0$). If α is a non-zero element of L, then the function $\mathrm{Tr}(\alpha x)$ on L is an element of the dual space of L (as K-vector space), and induces a homomorphism of L into its dual space. Since the kernel is trivial, it follows that L is isomorphic to its dual under the bilinear form

$$(x, y) \rightsquigarrow \mathrm{Tr}(xy).$$

Let $w_1', \ldots, w_n'$ be the dual basis of $w_1, \ldots, w_n$, so that

$$\mathrm{Tr}(w_i' w_j) = \delta_{ij}.$$

Let $c \neq 0$ be an element of A such that cw_i' is integral over A. Let z be in L, integral over A. Then zcw_i' is integral over A, and so is $\mathrm{Tr}(czw_i')$ for each i. If we write

$$z = b_1 w_1 + \cdots + b_n w_n$$

with coefficients $b_i \in K$, then

$$\mathrm{Tr}(czw_i') = cb_i,$$

and $cb_i \in A$ because A is integrally closed. Hence z is contained in

$$Ac^{-1}w_1 + \cdots + Ac^{-1}w_n.$$

Since z was selected arbitrarily in the integral closure of A in L, it follows that this integral closure is contained in a finitely generated A-module, and our proof is finished.

PROPOSITION 7. *If A is a unique factorization domain, then A is integrally closed.*

Proof. Suppose that there exists a quotient a/b with $a, b \in A$ which is integral over A, and a prime element p in A which divides b but not a. We have, for some integer $n \geqq 1$,

$$(a/b)^n + a_{n-1}(a/b)^{n-1} + \cdots + a_0 = 0,$$

whence

$$a^n + a_{n-1}ba^{n-1} + \cdots + a_0 b^n = 0.$$

Since p divides b, it must divide a^n, and hence must divide a, contradiction.

THEOREM 1. *Let A be a principal ideal ring, and L a finite separable extension of its quotient field, of degree n. Let B be the integral closure of A in L. Then B is a free module of rank n over A.*

Proof. As a module over A, the integral closure is torsion-free, and by the general theory of principal ideal rings, any torsion-free finitely generated module is in fact a free module. It is obvious that the rank is equal to the degree $[L : K]$.

Theorem 1 is applied to the ring of ordinary integers $\mathbf{Z}$. A finite extension of the rational numbers $\mathbf{Q}$ is called a *number field.* The integral closure of $\mathbf{Z}$ in a number field K is called the ring of *algebraic integers* of that field, and is denoted by I_K, or occasionally $\mathfrak{o}_K$.

PROPOSITION 8. *Let A be a subring of a ring B, integral over A. Let S be a multiplicative subset of A. Then $S^{-1}B$ is integral over $S^{-1}A$. If A is integrally closed, then $S^{-1}A$ is integrally closed.*

Proof. If $x \in B$ and $s \in S$, and if M is a finitely generated A-module such that $xM \subset M$, then $S^{-1}M$ is a finitely generated $S^{-1}A$-module which is mapped into itself by $s^{-1}x$, so that $s^{-1}x$ is integral over $S^{-1}A$. As to the second assertion, let x be integral over $S^{-1}A$, with x in the quotient field of A. We have an equation

$$x^n + \frac{b_{n-1}}{s_{n-1}} x^{n-1} + \cdots + \frac{b_0}{s_0} = 0,$$

$b_i \in A$ and $s_i \in S$. Thus there exists an element $s \in S$ such that sx is integral over A, hence lies in A. This proves that x lies in $S^{-1}A$.

COROLLARY. *If B is the integral closure of A in some field extension L of the quotient field of A, then $S^{-1}B$ is the integral closure of $S^{-1}A$ in L.*

§3. *Prime ideals*

Let $\mathfrak{p}$ be a prime ideal of a ring A and let $S = A - \mathfrak{p}$. If B is a ring containing A, we denote by $B_{\mathfrak{p}}$ the ring $S^{-1}B$.

Let B be a ring containing a ring A. Let $\mathfrak{p}$ be a prime ideal of A and $\mathfrak{P}$ a prime ideal of B. We say that $\mathfrak{P}$ *lies above* $\mathfrak{p}$ if $\mathfrak{P} \cap A = \mathfrak{p}$. If that is the case, then the injection

$$A \to B$$

induces an injection of the factor rings

$$A/\mathfrak{p} \to B/\mathfrak{P},$$

and in fact we have a commutative diagram:

$$\begin{array}{ccc} B & \to & B/\mathfrak{P} \\ \uparrow & & \uparrow \\ A & \to & A/\mathfrak{p} \end{array}$$

the horizontal arrows being the canonical homomorphisms, and the vertical arrows being inclusions.

If B is integral over A, then $B/\mathfrak{P}$ is integral over $A/\mathfrak{p}$ (by Proposition 4).

NAKAYAMA'S LEMMA. *Let A be a ring, $\mathfrak{a}$ an ideal contained in all maximal ideals of A, and M a finitely generated A-module. If $\mathfrak{a}M = M$, then $M = 0$.*

Proof. Induction on the number of generators of M. Say M is generated by $w_1, \ldots, w_m$. There exists an expression

$$w_1 = a_1 w_1 + \cdots + a_m w_m$$

with $a_i \in \mathfrak{a}$. Hence

$$(1 - a_1)w_1 = a_2 w_2 + \cdots + a_m w_m.$$

If $1 - a_1$ is not a unit in A, then it is contained in a maximal ideal $\mathfrak{p}$. Since $a_1 \in \mathfrak{p}$ by hypothesis, we have a contradiction. Hence $1 - a_1$ is a unit, and dividing by it shows that M can be generated by $m - 1$ elements, thereby concluding the proof.

PROPOSITION 9. *Let A be a ring, $\mathfrak{p}$ a prime ideal, and B a ring containing A and integral over A. Then $\mathfrak{p}B \neq B$, and there exists a prime ideal $\mathfrak{P}$ of B lying above $\mathfrak{p}$.*

Proof. We know that $B_{\mathfrak{p}}$ is integral over $A_{\mathfrak{p}}$, and that $A_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{m}_{\mathfrak{p}}$. Since we obviously have

$$\mathfrak{p}B_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}B = \mathfrak{p}A_{\mathfrak{p}}B_{\mathfrak{p}} = \mathfrak{m}_{\mathfrak{p}}B_{\mathfrak{p}},$$

it will suffice to prove our first assertion when A is a local ring. In that case, if $\mathfrak{p}B = B$, then 1 has an expression as a finite linear combination of elements of B with coefficients in $\mathfrak{p}$,

$$1 = a_1b_1 + \cdots + a_nb_n$$

with $a_i \in \mathfrak{p}$ and $b_i \in B$. Let $B_0 = A[b_1, \ldots, b_n]$. Then $\mathfrak{p}B_0 = B_0$ and B_0 is a finite A-module by Proposition 2. Hence $B_0 = 0$, contradiction.

To prove our second assertion, we go back to the original notation, and note the following commutative diagram:

$$\begin{array}{ccc} B & \to & B_{\mathfrak{p}} \\ \uparrow & & \uparrow \\ A & \to & A_{\mathfrak{p}} \end{array} \qquad \text{(all arrows inclusions).}$$

We have just proved that $\mathfrak{m}_{\mathfrak{p}}B_{\mathfrak{p}} \neq B_{\mathfrak{p}}$. Hence $\mathfrak{m}_{\mathfrak{p}}B_{\mathfrak{p}}$ is contained in a maximal ideal $\mathfrak{M}$ of $B_{\mathfrak{p}}$, and $\mathfrak{M} \cap A_{\mathfrak{p}}$ therefore contains $\mathfrak{m}_{\mathfrak{p}}$. Since $\mathfrak{m}_{\mathfrak{p}}$ is maximal, it follows that

$$\mathfrak{m}_{\mathfrak{p}} = \mathfrak{M} \cap A_{\mathfrak{p}}.$$

Let $\mathfrak{P} = \mathfrak{M} \cap B$. Then $\mathfrak{P}$ is a prime ideal of B, and taking intersections with A going both ways around our diagram shows that $\mathfrak{M} \cap A = \mathfrak{p}$, so that

$$\mathfrak{P} \cap A = \mathfrak{p},$$

as was to be shown.

Remark. Let B be integral over A, and let $\mathfrak{b}$ be an ideal of B, $\mathfrak{b} \neq 0$. Then $\mathfrak{b} \cap A \neq 0$.

To prove this, let $b \in \mathfrak{b}$, $b \neq 0$. Then b satisfies an equation

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$

with $a_i \in A$, and $a_0 \neq 0$. But a_0 lies in $\mathfrak{b} \cap A$.

PROPOSITION 10. *Let A be a subring of B, and assume B integral over A. Let $\mathfrak{P}$ be a prime ideal of B lying over a prime ideal $\mathfrak{p}$ of A. Then $\mathfrak{P}$ is maximal if and only if $\mathfrak{p}$ is maximal.*

Proof. Assume $\mathfrak{p}$ maximal in A. Then $A/\mathfrak{p}$ is a field. We are reduced to proving that a ring which is integral over a field is a field. If k is a field and x is integral over k, then it is standard from elementary field theory that the ring $k[x]$ is itself a field, so x is invertible in the ring. Conversely, assume that $\mathfrak{P}$ is maximal in B. Then $B/\mathfrak{P}$ is a field, which is integral over the ring $A/\mathfrak{p}$. If $A/\mathfrak{p}$ is not a field, it has a non-zero maximal ideal $\mathfrak{m}$. By Proposition 9, there exists a maximal ideal $\mathfrak{M}$ of $B/\mathfrak{P}$ lying above $\mathfrak{m}$, contradiction.