

THE ANALYTIC THEORY OF ALGEBRAIC NUMBERS

BY H. M. STARK

1. The basics of algebraic number theory. An algebraic number field is a field $K = \mathbf{Q}(\alpha)$ where α is a zero of an irreducible (over \mathbf{Q}) polynomial $f(x)$ with integral coefficients. The degree of K , which we denote by $n = n(K) = [K : \mathbf{Q}]$, is the degree of $f(x)$. We write the roots of $f(x) = 0$ as $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(n)}$ in such a way that for $1 \leq j \leq r_1 = r_1(K)$, $\alpha^{(j)}$ is real, while for $j > r_1$, $\alpha^{(j)}$ is complex. If we let $n = r_1 + 2r_2$, then it is customary to order the $r_2 = r_2(K)$ complex conjugate pairs of roots so that for $r_1 + 1 \leq j \leq r_1 + r_2$, $\alpha^{(j)} = \overline{\alpha^{(j+r_2)}}$. The $\alpha^{(j)}$'s are called the conjugates of α and the fields $K^{(j)} = \mathbf{Q}(\alpha^{(j)})$ are called the conjugate fields of K . If $r_2 = 0$, we say K is totally real and if $r_1 = 0$, we say K is totally complex.

The integers of K are those elements of K which are zeros of a polynomial with integer coefficients and leading coefficient 1. The integers of K form a ring which we denote by \mathfrak{o} . As is well known, factorization of the integers of K into prime integers is not necessarily unique. Various equivalent ways of remedying this have been used; we follow Dedekind's method. If $\alpha_1, \dots, \alpha_k$ are elements of K , the set

$$\mathfrak{a} = [\alpha_1, \dots, \alpha_k] = \left\{ \sum_{i=1}^k a_i \alpha_i \mid a_i \in \mathbf{Z} \right\}$$

is called the module generated by $\alpha_1, \dots, \alpha_k$ (today it would be called a finitely generated \mathbf{Z} module). The ring \mathfrak{o} is an example of such a module; on the other hand, K is not an example since it is not finitely generated over \mathbf{Z} . If $\mathfrak{b} = [\beta_1, \dots, \beta_m]$ is another module, we define the product $\mathfrak{a}\mathfrak{b}$ to be the module generated by the km numbers $\alpha_i \beta_j$.

Since 1 is in \mathfrak{o} , we always have $\mathfrak{o}\mathfrak{a} \supset \mathfrak{a}$ for any module \mathfrak{a} . If $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$ then we say \mathfrak{a} is a fractional ideal of K . The nonzero fractional ideals of K form an abelian group under multiplication with identity element \mathfrak{o} . An integral ideal, or just ideal for short, is a fractional ideal of K which is contained in \mathfrak{o} . The integral ideals of K are precisely the ideals of \mathfrak{o} in the sense of ring theory today. Every fractional ideal is a quotient of two integral ideals and factorization of ideals into prime ideals is unique.

Among the fractional ideals of K are the principal fractional ideals. If α is in K then the principal fractional ideal generated by α is

$$(\alpha) = \alpha \mathfrak{o} = [\alpha] \mathfrak{o}.$$

This is a slightly expanded version of an invited address delivered at the Summer 1973 Meeting of the Society in Missoula, Montana.

AMS (MOS) subject classifications (1970). Primary 12-02, 12A50, 12A70.

Key words and phrases. Algebraic number theory, class-number, discriminant, Dirichlet unit theorem, Dedekind zeta function.

Copyright © American Mathematical Society 1975