

Chapter 2

Norms, Traces and Discriminants

We continue building our algebraic background to prepare for algebraic number theory.

2.1 Norms and Traces

2.1.1 Definitions and Comments

If E/F is a field extension of finite degree n , then in particular, E is a finite-dimensional vector space over F , and the machinery of basic linear algebra becomes available. If x is any element of E , we can study the F -linear transformation $m(x)$ given by multiplication by x , that is, $m(x)y = xy$. We define the *norm* and the *trace* of x , relative to the extension E/F , as

$$N_{E/F}(x) = \det m(x) \text{ and } T_{E/F}(x) = \text{trace } m(x).$$

We will write $N(x)$ and $T(x)$ if E/F is understood. If the matrix $A(x) = [a_{ij}(x)]$ represents $m(x)$ with respect to some basis for E over F , then the norm of x is the determinant of $A(x)$ and the trace of x is the trace of $A(x)$, that is, the sum of the main diagonal entries. The *characteristic polynomial* of x is defined as the characteristic polynomial of the matrix $A(x)$, that is,

$$\text{char}_{E/F}(x) = \det[XI - A(x)]$$

where I is an n by n identity matrix. It follows from the definitions that the norm, the trace and the coefficients of the characteristic polynomial are elements belonging to the base field F .

2.1.2 Example

Let $E = \mathbb{C}$ and $F = \mathbb{R}$. A basis for \mathbb{C} over \mathbb{R} is $\{1, i\}$ and, with $x = a + bi$, we have

$$(a + bi)(1) = a(1) + b(i) \text{ and } (a + bi)(i) = -b(1) + a(i).$$

Thus

$$A(a + bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

The norm, trace and characteristic polynomial of $a + bi$ are

$$N(a + bi) = a^2 + b^2, \quad T(a + bi) = 2a, \quad \text{char}(a + bi) = X^2 - 2aX + a^2 + b^2.$$

The computation is exactly the same if $E = \mathbb{Q}(i)$ and $F = \mathbb{Q}$.

2.1.3 Some Basic Properties

Notice that in (2.1.2), the coefficient of the second highest power of X in the characteristic polynomial is minus the trace, and the constant term is the norm. In general, it follows from the definition of characteristic polynomial that

$$\text{char}(x) = X^n - T(x)X^{n-1} + \cdots + (-1)^n N(x). \quad (1)$$

[The only terms multiplying X^{n-1} in the expansion of the determinant defining the characteristic polynomial are $-a_{ii}(x)$, $i = 1, \dots, n$. Set $X = 0$ to show that the constant term of $\text{char}(x)$ is $(-1)^n \det A(x)$.]

If $x, y \in E$ and $a, b \in F$, then

$$T(ax + by) = aT(x) + bT(y) \quad \text{and} \quad N(xy) = N(x)N(y). \quad (2)$$

[This holds because $m(ax + by) = am(x) + bm(y)$ and $m(xy) = m(x) \circ m(y)$.]

If $a \in F$, then

$$N(a) = a^n, \quad T(a) = na, \quad \text{and} \quad \text{char}(a) = (X - a)^n. \quad (3)$$

[Note that the matrix representing multiplication by the element a in F is aI .]

It is natural to look for a connection between the characteristic polynomial of x and the minimal polynomial $\min(x, F)$ of x over F .

2.1.4 Proposition

$\text{char}_{E/F}(x) = [\min(x, F)]^r$, where $r = [E : F(x)]$.

Proof. First assume that $r = 1$, so that $E = F(x)$. By the Cayley-Hamilton theorem, the linear transformation $m(x)$ satisfies $\text{char}(x)$. Since $m(x)$ is multiplication by x , it follows that x itself is a root of $\text{char}(x)$. Thus $\min(x, F)$ divides $\text{char}(x)$, and since both polynomials are monic of degree n , the result follows. In the general case, let y_1, \dots, y_s be a basis for $F(x)$ over F , and let z_1, \dots, z_r be a basis for E over $F(x)$. Then the $y_i z_j$ form a basis for E over F . Let $A = A(x)$ be the matrix representing multiplication by x in the extension $F(x)/F$, so that $xy_i = \sum_k a_{ki} y_k$ and $x(y_i z_j) = \sum_k a_{ki} (y_k z_j)$. Order the

basis for E/F as $y_1z_1, y_2z_1, \dots, y_s z_1; y_1z_2, y_2z_2, \dots, y_s z_2; \dots; y_1z_r, y_2z_r, \dots, y_s z_r$. Then $m(x)$ is represented in E/F as

$$\begin{bmatrix} A & 0 & \cdots & 0 \\ 0 & A & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & A \end{bmatrix}$$

with r blocks, each consisting of the s by s matrix A . Thus $\text{char}_{E/F}(x) = [\det(XI - A)]^r$, which by the $r = 1$ case coincides with $[\min(x, F)]^r$. ♣

2.1.5 Corollary

Let $[E : F] = n$ and $[F(x) : F] = d$. Let x_1, \dots, x_d be the roots of $\min(x, F)$, counting multiplicity, in a splitting field. Then

$$N(x) = \left(\prod_{i=1}^d x_i \right)^{n/d}, \quad T(x) = \frac{n}{d} \sum_{i=1}^d x_i, \quad \text{char}(x) = \left[\prod_{i=1}^d (X - x_i) \right]^{n/d}.$$

Proof. The formula for the characteristic polynomial follows from (2.1.4). By (2.1.3), the norm is $(-1)^n$ times the constant term of $\text{char}(x)$. Evaluating the characteristic polynomial at $X = 0$ produces another factor of $(-1)^n$, which yields the desired expression for the norm. Finally, if $\min(x, F) = X^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0$, then the coefficient of X^{n-1} in $[\min(x, F)]^{n/d}$ is $(n/d)a_{d-1} = -(n/d) \sum_{i=1}^d x_i$. Since the trace is the negative of this coefficient [see (2.1.3)], the result follows. ♣

If E is a separable extension of F , there are very useful alternative expressions for the trace, norm and characteristic polynomial.

2.1.6 Proposition

Let E/F be a separable extension of degree n , and let $\sigma_1, \dots, \sigma_n$ be the distinct F -embeddings (that is, F -monomorphisms) of E into an algebraic closure of E , or equally well into a normal extension L of F containing E . Then

$$N_{E/F}(x) = \prod_{i=1}^n \sigma_i(x), \quad T_{E/F}(x) = \sum_{i=1}^n \sigma_i(x), \quad \text{char}_{E/F}(x) = \prod_{i=1}^n (X - \sigma_i(x)).$$

Proof. Each of the d distinct F -embeddings τ_i of $F(x)$ into L takes x into a unique conjugate x_i , and extends to exactly $n/d = [E : F(x)]$ F -embeddings of E into L , all of which also take x to x_i . Thus the list of elements $\{\sigma_1(x), \dots, \sigma_n(x)\}$ consists of the $\tau_i(x) = x_i, i = 1, \dots, d$, each appearing n/d times. The result follows from (2.1.5). ♣

We may now prove a basic transitivity property.

2.1.7 Transitivity of Trace and Norm

If $F \leq K \leq E$, where E/F is finite and separable, then

$$T_{E/F} = T_{K/F} \circ T_{E/K} \text{ and } N_{E/F} = N_{K/F} \circ N_{E/K}.$$

Proof. Let $\sigma_1, \dots, \sigma_n$ be the distinct F -embeddings of K into L , and let τ_1, \dots, τ_m be the distinct K -embeddings of E into L , where L is the normal closure of E over F . Then L/F is Galois, and each mapping σ_i and τ_j extends to an automorphism of L . Therefore it makes sense to allow the mappings to be composed. By (2.1.6),

$$T_{K/F}(T_{E/K}(x)) = \sum_{i=1}^n \sigma_i \left(\sum_{j=1}^m \tau_j(x) \right) = \sum_{i=1}^n \sum_{j=1}^m \sigma_i(\tau_j(x)).$$

Each $\sigma_i \tau_j = \sigma_i \circ \tau_j$ is an F -embedding of E into L , and the number of mappings is given by $mn = [E : K][K : F] = [E : F]$. Furthermore, the $\sigma_i \tau_j$ are distinct when restricted to E . For if $\sigma_i \tau_j = \sigma_k \tau_l$ on E , then $\sigma_i = \sigma_k$ on K , because τ_j and τ_k coincide with the identity on K . Thus $i = k$, so that $\tau_j = \tau_l$ on E . But then $j = l$. By (2.1.6), $T_{K/F}(T_{E/K}(x)) = T_{E/F}(x)$. The norm is handled the same way, with sums replaced by products. ♣

Here is another application of (2.1.6).

2.1.8 Proposition

If E/F is a finite separable extension, then the trace $T_{E/F}(x)$ cannot be 0 for every $x \in E$.

Proof. If $T(x) = 0$ for all x , then by (2.1.6), $\sum_{i=1}^n \sigma_i(x) = 0$ for all x . This contradicts Dedekind's lemma on linear independence of monomorphisms. ♣

2.1.9 Remark

A statement equivalent to (2.1.8) is that if E/F is finite and separable, then the *trace form*, that is, the bilinear form $(x, y) \rightarrow T_{E/F}(xy)$, is nondegenerate. In other words, if $T(xy) = 0$ for all y , then $x = 0$. Going from (2.1.9) to (2.1.8) is immediate, so assume $T(xy) = 0$ for all y , with $x \neq 0$. Let x_0 be an element with nonzero trace, as provided by (2.1.8). Choose y so that $xy = x_0$ to produce a contradiction.

2.1.10 Example

Let $x = a + b\sqrt{m}$ be an element of the quadratic extension $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$, where m is a square-free integer. We will find the trace and norm of x .

The Galois group of the extension consists of the identity and the automorphism $\sigma(a + b\sqrt{m}) = a - b\sqrt{m}$. Thus by (2.1.6),

$$T(x) = x + \sigma(x) = 2a, \text{ and } N(x) = x\sigma(x) = a^2 - mb^2.$$

Problems For Section 2.1

1. If $E = \mathbb{Q}(\theta)$ where θ is a root of the irreducible cubic $X^3 - 3X + 1$, find the norm and trace of θ^2 .
2. Find the trace of the primitive 6th root of unity ω in the cyclotomic extension $\mathbb{Q}_6 = \mathbb{Q}(\omega)$.
3. Let θ be a root of $X^4 - 2$ over \mathbb{Q} . Find the trace over \mathbb{Q} of $\theta, \theta^2, \theta^3$ and $\sqrt{3}\theta$.
4. Continuing Problem 3, show that $\sqrt{3}$ cannot belong to $\mathbb{Q}[\theta]$.

2.2 The Basic Setup For Algebraic Number Theory

2.2.1 Assumptions

Let A be an integral domain with fraction field K , and let L be a finite separable extension of K . Let B be the set of elements of L that are integral over A , that is, B is the integral closure of A in L . The diagram below summarizes the information.

$$\begin{array}{ccc} L & \text{---} & B \\ | & & | \\ K & \text{---} & A \end{array}$$

In the most important special case, $A = \mathbb{Z}$, $K = \mathbb{Q}$, L is a *number field*, that is, a finite (necessarily separable) extension of \mathbb{Q} , and B is the ring of algebraic integers of L . From now on, we will refer to (2.2.1) as the *AKLB setup*.

2.2.2 Proposition

If $x \in B$, then the coefficients of $\text{char}_{L/K}(x)$ and $\text{min}(x, K)$ are integral over A . In particular, $T_{L/K}(x)$ and $N_{L/K}(x)$ are integral over A , by (2.1.3). If A is integrally closed, then the coefficients belong to A .

Proof. The coefficients of $\text{min}(x, K)$ are sums of products of the roots x_i , so by (2.1.4), it suffices to show that the x_i are integral over A . Each x_i is a conjugate of x over K , so there is a K -isomorphism $\tau_i : K(x) \rightarrow K(x_i)$ such that $\tau_i(x) = x_i$. If we apply τ_i to an equation of integral dependence for x over A , we get an equation of integral dependence for x_i over A . Since the coefficients belong to K [see (2.1.1)], they must belong to A if A is integrally closed. ♣

2.2.3 Corollary

Assume A integrally closed, and let $x \in L$. Then x is integral over A , that is, $x \in B$, if and only if the minimal polynomial of x over K has coefficients in A .

Proof. If $\text{min}(x, K) \in A[X]$, then x is integral over A by definition of integrality. (See (1.1.1); note also that A need not be integrally closed for this implication.) The converse follows from (2.2.2). ♣

2.2.4 Corollary

An algebraic integer a that belongs to \mathbb{Q} must in fact belong to \mathbb{Z} .

Proof. The minimal polynomial of a over \mathbb{Q} is $X - a$, so by (2.2.3), $a \in \mathbb{Z}$. ♣

2.2.5 Quadratic Extensions of the Rationals

We will determine the algebraic integers of $L = \mathbb{Q}(\sqrt{m})$, where m is a square-free integer (a product of distinct primes). The restriction on m involves no loss of generality, for example, $\mathbb{Q}(\sqrt{12}) = \mathbb{Q}(\sqrt{3})$.

A remark on notation: To make sure there is no confusion between algebraic integers and ordinary integers, we will often use the term “rational integer” for a member of \mathbb{Z} .

Now by direct verification or by (2.1.10) and (2.1.3), the minimal polynomial over \mathbb{Q} of the element $a + b\sqrt{m} \in L$ (with $a, b \in \mathbb{Q}$) is $X^2 - 2aX + a^2 - mb^2$. By (2.2.3), $a + b\sqrt{m}$ is an algebraic integer if and only if $2a$ and $a^2 - mb^2$ are rational integers. In this case, we also have $2b \in \mathbb{Z}$. For we have $(2a)^2 - m(2b)^2 = 4(a^2 - mb^2) \in \mathbb{Z}$, so $m(2b)^2 \in \mathbb{Z}$. If $2b$ is not a rational integer, its denominator would include a prime factor p , which would appear as p^2 in the denominator of $(2b)^2$. Multiplication of $(2b)^2$ by m cannot cancel the p^2 because m is square-free, and the result follows.

Here is a more convenient way to characterize the algebraic integers of a quadratic field.

2.2.6 Proposition

The set B of algebraic integers of $\mathbb{Q}(\sqrt{m})$, m square-free, can be described as follows.

- (i) If $m \not\equiv 1 \pmod{4}$, then B consists of all $a + b\sqrt{m}$, $a, b \in \mathbb{Z}$;
- (ii) If $m \equiv 1 \pmod{4}$, then B consists of all $(u/2) + (v/2)\sqrt{m}$, $u, v \in \mathbb{Z}$, where u and v have the same parity (both even or both odd).

[Note that since m is square-free, it is not divisible by 4, so the condition in (i) can be written as $m \equiv 2$ or $3 \pmod{4}$.]

Proof. By (2.2.5), the algebraic integers are of the form $(u/2) + (v/2)\sqrt{m}$, where $u, v \in \mathbb{Z}$ and $(u^2 - mv^2)/4 \in \mathbb{Z}$, that is, $u^2 - mv^2 \equiv 0 \pmod{4}$. It follows that u and v have the same parity. [The square of an even number is congruent to 0 mod 4, and the square of an odd number is congruent to 1 mod 4.] Moreover, the “both odd” case can only occur when $m \equiv 1 \pmod{4}$. The “both even” case is equivalent to $u/2, v/2 \in \mathbb{Z}$, and we have the desired result. ♣

When we introduce integral bases in the next section, we will have an even more convenient way to describe the algebraic integers of $\mathbb{Q}(\sqrt{m})$.

If $[L : K] = n$, then a basis for L/K consists of n elements of L that are linearly independent over K . In fact we can assemble a basis using only elements of B .

2.2.7 Proposition

There is a basis for L/K consisting entirely of elements of B .

Proof. Let x_1, \dots, x_n be a basis for L over K . Each x_i is algebraic over K , and therefore satisfies a polynomial equation of the form

$$a_m x_i^m + \cdots + a_1 x_i + a_0 = 0$$

with $a_m \neq 0$ and the $a_i \in A$. (Initially, we only have $a_i \in K$, but then a_i is the ratio of two elements of A , and we can form a common denominator.) Multiply the equation by a_m^{m-1} to obtain an equation of integral dependence for $y_i = a_m x_i$ over A . The y_i form the desired basis. ♣

2.2.8 Corollary of the Proof

If $x \in L$, then there is a nonzero element $a \in A$ and an element $y \in B$ such that $x = y/a$. In particular, L is the fraction field of B .

Proof. In the proof of (2.2.7), take $x_i = x$, $a_m = a$, and $y_i = y$. ♣

In Section 2.3, we will need a standard result from linear algebra. We state the result now, and an outline of the proof is given in the exercises.

2.2.9 Theorem

Suppose we have a nondegenerate symmetric bilinear form on an n -dimensional vector space V , written for convenience using inner product notation (x, y) . If x_1, \dots, x_n is any basis for V , then there is a basis y_1, \dots, y_n for V , called the *dual basis referred to V* , such that

$$(x_i, y_j) = \delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j. \end{cases}$$

Problems For Section 2.2

1. Let $L = \mathbb{Q}(\alpha)$, where α is a root of the irreducible quadratic $X^2 + bX + c$, with $b, c \in \mathbb{Q}$. Show that $L = \mathbb{Q}(\sqrt{m})$ for some square-free integer m . Thus the analysis of this section covers all possible quadratic extensions of \mathbb{Q} .
2. Show that the quadratic extensions $\mathbb{Q}(\sqrt{m})$, m square-free, are all distinct.
3. Continuing Problem 2, show that in fact no two distinct quadratic extensions of \mathbb{Q} are \mathbb{Q} -isomorphic.

Cyclotomic fields do not exhibit the same behavior. Let $\omega_n = e^{i2\pi/n}$, a primitive n^{th} root of unity. By a direct computation, we have $\omega_{2n}^2 = \omega_n$ and

$$-\omega_{2n}^{n+1} = -e^{i\pi(n+1)/n} = e^{i\pi} e^{i\pi} e^{i\pi/n} = \omega_{2n}.$$

4. Show that if n is odd, then $\mathbb{Q}(\omega_n) = \mathbb{Q}(\omega_{2n})$.
5. Give an example of a quadratic extension of \mathbb{Q} that is also a cyclotomic extension.

We now indicate how to prove (2.2.9).

6. For any y in the finite-dimensional vector space V , the mapping $x \rightarrow (x, y)$ is a linear form $l(y)$ on V , that is, a linear map from V to the field of scalars. Show that the linear

transformation $y \rightarrow l(y)$ from V to V^* (the space of all linear forms on V) is injective.

7. Show that any linear form on V is $l(y)$ for some y .

8. Let f_1, \dots, f_n be the dual basis corresponding to x_1, \dots, x_n . Thus each f_j belongs to V^* (not V) and $f_j(x_i) = \delta_{ij}$. If $f_j = l(y_j)$, show that y_1, \dots, y_n is the required dual basis referred to V .

9. Show that $x_i = \sum_{j=1}^n (x_i, x_j)y_j$. Thus in order to compute the dual basis referred to V , we must invert the matrix $((x_i, x_j))$.

2.3 The Discriminant

The discriminant of a polynomial is familiar from basic algebra, and there is also a discriminant in algebraic number theory. The two concepts are unrelated at first glance, but there is a connection between them. We assume the basic *AKLB* setup of (2.2.1), with $n = [L : K]$.

2.3.1 Definition

If $n = [L : K]$, the *discriminant* of the n -tuple $x = (x_1, \dots, x_n)$ of elements of L is

$$D(x) = \det(T_{L/K}(x_i x_j)).$$

Thus we form a matrix whose ij entry is the trace of $x_i x_j$, and take the determinant of the matrix; by (2.1.1), $D(x) \in K$. If the $x_i \in B$, then by (2.2.2), $D(x)$ is integral over A , that is, $D(x) \in B$. Thus if A is integrally closed and the $x_i \in B$, then $D(x)$ belongs to A .

The discriminant behaves quite reasonably under linear transformation.

2.3.2 Lemma

If $y = Cx$, where C is an n by n matrix over K and x and y are n -tuples written as column vectors, then $D(y) = (\det C)^2 D(x)$.

Proof. The trace of $y_r y_s$ is

$$T\left(\sum_{i,j} c_{ri} c_{sj} x_i x_j\right) = \sum_{i,j} c_{ri} T(x_i x_j) c_{sj}$$

hence

$$(T(y_r y_s)) = C(T(x_i x_j))C'$$

where C' is the transpose of C . The result follows upon taking determinants. ♣

Here is an alternative expression for the discriminant.

2.3.3 Lemma

Let $\sigma_1, \dots, \sigma_n$ be the distinct K -embeddings of L into an algebraic closure of L , as in (2.1.6). Then $D(x) = [\det(\sigma_i(x_j))]^2$.

Thus we form the matrix whose ij element is $\sigma_i(x_j)$, take the determinant and square the result.

Proof. By (2.1.6),

$$T(x_i x_j) = \sum_k \sigma_k(x_i x_j) = \sum_k \sigma_k(x_i) \sigma_k(x_j)$$

so if H is the matrix whose ij entry is $\sigma_i(x_j)$, then $(T(x_i x_j)) = H'H$, and again the result follows upon taking determinants. ♣

The discriminant “discriminates” between bases and non-bases, as follows.

2.3.4 Proposition

If $x = (x_1, \dots, x_n)$, then the x_i form a basis for L over K if and only if $D(x) \neq 0$.

Proof. If $\sum_j c_j x_j = 0$, with the $c_j \in K$ and not all 0, then $\sum_j c_j \sigma_i(x_j) = 0$ for all i , so the columns of the matrix $H = (\sigma_i(x_j))$ are linearly dependent. Thus linear dependence of the x_i implies that $D(x) = 0$. Conversely, assume that the x_i are linearly independent, and therefore a basis because $n = [L : K]$. If $D(x) = 0$, then the rows of H are linearly dependent, so for some $c_i \in K$, not all 0, we have $\sum_i c_i \sigma_i(x_j) = 0$ for all j . Since the x_j form a basis, it follows that $\sum_i c_i \sigma_i(u) = 0$ for all $u \in L$, so the monomorphisms σ_i are linearly dependent. This contradicts Dedekind’s lemma. ♣

We now make the connection between the discriminant defined above and the discriminant of a polynomial.

2.3.5 Proposition

Assume that $L = K(x)$, and let f be the minimal polynomial of x over K . Let D be the discriminant of the basis $1, x, x^2, \dots, x^{n-1}$ over K , and let x_1, \dots, x_n be the roots of f in a splitting field, with $x_1 = x$. Then D coincides with $\prod_{i < j} (x_i - x_j)^2$, the discriminant of the polynomial f .

Proof. Let σ_i be the K -embedding that takes x to x_i , $i = 1, \dots, n$. Then $\sigma_i(x^j) = x_i^j$, $0 \leq j \leq n-1$. By (2.3.3), D is the square of the determinant of the matrix

$$V = \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{bmatrix}.$$

But $\det V$ is a Vandermonde determinant, whose value is $\prod_{i < j} (x_j - x_i)$, and the result follows. ♣

Proposition 2.3.5 yields a formula that is often useful in computing the discriminant.

2.3.6 Corollary

Under the hypothesis of (2.3.5),

$$D = (-1)^{\binom{n}{2}} N_{L/K}(f'(x))$$

where f' is the derivative of f .

Proof. Let $c = (-1)^{\binom{n}{2}}$. By (2.3.5),

$$D = \prod_{i < j} (x_i - x_j)^2 = c \prod_{i \neq j} (x_i - x_j) = c \prod_i \prod_{j \neq i} (x_i - x_j).$$

But $f(X) = (X - x_1) \cdots (X - x_n)$, so

$$f'(x_i) = \sum_k \prod_{j \neq k} (X - x_j)$$

with X replaced by x_i . When the substitution $X = x_i$ is carried out, only the $k = i$ term is nonzero, hence

$$f'(x_i) = \prod_{j \neq i} (x_i - x_j).$$

Consequently,

$$D = c \prod_{i=1}^n f'(x_i).$$

But

$$f'(x_i) = f'(\sigma_i(x)) = \sigma_i(f'(x))$$

so by (2.1.6),

$$D = c N_{L/K}(f'(x)). \clubsuit$$

2.3.7 Definitions and Comments

In the *AKLB* setup with $[L : K] = n$, suppose that B turns out to be a free A -module of rank n . A basis for this module is said to be an *integral basis* of B (or of L). An integral basis is, in particular, a basis for L over K , because linear independence over A is equivalent to linear independence over the fraction field K . We will see shortly that an integral basis always exists when L is a number field. In this case, the discriminant is the same for all integral bases. It is called the *field discriminant*.

2.3.8 Theorem

If A is integrally closed, then B is a submodule of a free A -module of rank n . If A is a PID, then B itself is free of rank n over A , so B has an integral basis.

Proof. By (2.1.9), the trace is a nondegenerate symmetric bilinear form defined on the n -dimensional vector space L over K . By (2.2.2), the trace of any element of B belongs to A . Now let x_1, \dots, x_n be any basis for L over K consisting of elements of B [see (2.2.7)], and let y_1, \dots, y_n be the dual basis referred to L [see (2.2.9)]. If $z \in B$, then we can write $z = \sum_{j=1}^n a_j y_j$ with the $a_j \in K$. We know that the trace of $x_i z$ belongs to A , and we also have

$$T(x_i z) = T\left(\sum_{j=1}^n a_j x_i y_j\right) = \sum_{j=1}^n a_j T(x_i y_j) = \sum_{j=1}^n a_j \delta_{ij} = a_i.$$

Thus each a_i belongs to A , so that B is an A -submodule of the free A -module $\bigoplus_{j=1}^n A y_j$. Moreover, B contains the free A -module $\bigoplus_{j=1}^n A x_j$. Consequently, if A is a principal ideal domain, then B is free over A of rank exactly n . ♣

2.3.9 Corollary

The set B of algebraic integers in any number field L is a free \mathbb{Z} -module of rank $n = [L : \mathbb{Q}]$. Therefore B has an integral basis. The discriminant is the same for every integral basis.

Proof. Take $A = \mathbb{Z}$ in (2.3.8) to show that B has an integral basis. The transformation matrix C between two integral bases [see (2.3.2)] is invertible, and both C and C^{-1} have rational integer coefficients. Take determinants in the equation $CC^{-1} = I$ to conclude that $\det C$ is a unit in \mathbb{Z} . Therefore $\det C = \pm 1$, so by (2.3.2), all integral bases have the same discriminant. ♣

2.3.10 Remark

An invertible matrix C with coefficients in \mathbb{Z} is said to be *unimodular* if C^{-1} also has coefficients in \mathbb{Z} . We have just seen that a unimodular matrix has determinant ± 1 . Conversely, a matrix over \mathbb{Z} with determinant ± 1 is unimodular, by Cramer's rule.

2.3.11 Theorem

Let B be the algebraic integers of $\mathbb{Q}(\sqrt{m})$, where m is a square-free integer.

(i) If $m \not\equiv 1 \pmod{4}$, then 1 and \sqrt{m} form an integral basis, and the field discriminant is $d = 4m$.

(ii) If $m \equiv 1 \pmod{4}$, then 1 and $(1 + \sqrt{m})/2$ form an integral basis, and the field discriminant is $d = m$.

Proof.

(i) By (2.2.6), 1 and \sqrt{m} span B over \mathbb{Z} , and they are linearly independent because \sqrt{m} is irrational. By (2.1.10), the trace of $a + b\sqrt{m}$ is $2a$, so by (2.3.1), the field discriminant

is

$$\begin{vmatrix} 2 & 0 \\ 0 & 2m \end{vmatrix} = 4m.$$

(ii) By (2.2.6), 1 and $(1 + \sqrt{m})/2$ are algebraic integers. To show that they span B , consider $(u + v\sqrt{m})/2$, where u and v have the same parity. Then

$$\frac{1}{2}(u + v\sqrt{m}) = \left(\frac{u-v}{2}\right)(1) + v \left[\frac{1}{2}(1 + \sqrt{m})\right]$$

with $(u - v)/2$ and v in \mathbb{Z} . To prove linear independence, assume that $a, b \in \mathbb{Z}$ and

$$a + b \left[\frac{1}{2}(1 + \sqrt{m})\right] = 0.$$

Then $2a + b + b\sqrt{m} = 0$, which forces $a = b = 0$. Finally, by (2.1.10), (2.3.1), and the computation $[(1 + \sqrt{m})/2]^2 = (1 + m)/4 + \sqrt{m}/2$, the field discriminant is

$$\begin{vmatrix} 2 & 1 \\ 1 & (1 + m)/2 \end{vmatrix} = m. \spadesuit$$

Problems For Section 2.3

Problems 1-3 outline the proof of *Stickelberger's theorem*, which states that the discriminant of any n -tuple in a number field is congruent to 0 or 1 mod 4.

1. Let x_1, \dots, x_n be arbitrary algebraic integers in a number field, and consider the determinant of the matrix $(\sigma_i(x_j))$, as in (2.3.3). The direct expansion of the determinant has $n!$ terms. Let P be the sum of those terms in the expansion that have plus signs in front of them, and N the sum of those terms prefixed by minus signs. Thus the discriminant D of (x_1, \dots, x_n) is $(P - N)^2$. Show that $P + N$ and PN are fixed by each σ_i , and deduce that $P + N$ and PN are rational numbers.
2. Show that $P + N$ and PN are rational integers.
3. Show that $D \equiv 0$ or 1 mod 4.
4. Let L be a number field of degree n over \mathbb{Q} , and let y_1, \dots, y_n be a basis for L over \mathbb{Q} consisting of algebraic integers. Let x_1, \dots, x_n be an integral basis. Show that if the discriminant $D(y_1, \dots, y_n)$ is square-free, then each x_i can be expressed as a linear combination of the y_j with integer coefficients.
5. Continuing Problem 4, show that if $D(y_1, \dots, y_n)$ is square-free, then y_1, \dots, y_n is an integral basis.
6. Is the converse of the result of problem 5 true?