Algebraic Number Theory

summary of notes

Robin Chapman

3 May 2000, revised 28 March 2004, corrected 4 January 2005

This is a summary of the 1999–2000 course on algebraic number theory. Proofs will generally be sketched rather than presented in detail. Also, examples will be very thin on the ground.

I first learnt algebraic number theory from Stewart and Tall's textbook *Algebraic Number Theory* (Chapman & Hall, 1979) (latest edition retitled *Algebraic Number Theory and Fermat's Last Theorem* (A. K. Peters, 2002)) and these notes owe much to this book.

I am indebted to Artur Costa Steiner for pointing out an error in an earlier version.

1 Algebraic numbers and integers

We say that $\alpha \in \mathbf{C}$ is an *algebraic number* if $f(\alpha) = 0$ for some monic polynomial $f \in \mathbf{Q}[X]$. We say that $\beta \in \mathbf{C}$ is an *algebraic integer* if $g(\alpha) = 0$ for some monic polynomial $g \in \mathbf{Z}[X]$. We let $\mathbf{A}$ and $\mathbf{B}$ denote the sets of algebraic numbers and algebraic integers respectively. Clearly $\mathbf{B} \subseteq \mathbf{A}$, $\mathbf{Z} \subseteq \mathbf{B}$ and $\mathbf{Q} \subseteq \mathbf{A}$.

Lemma 1.1 *Let $\alpha \in \mathbf{A}$. Then there is $\beta \in \mathbf{B}$ and a nonzero $m \in \mathbf{Z}$ with $\alpha = \beta/m$.*

Proof There is a monic polynomial $f \in \mathbf{Q}[X]$ with $f(\alpha) = 0$. Let m be the product of the denominators of the coefficients of f. Then $g = mf \in \mathbf{Z}[X]$. Write $g = \sum_{j=0}^{n} a_j X^j$. Then $a_n = m$. Now

$$h(X) = m^{n-1} g(X/m) = \sum_{j=0}^{n} m^{n-1+j} a_j X^j$$

is monic with integer coefficients (the only slightly problematical coefficient is that of X^n which equals $m^{-1}A_m = 1$). Also $h(m\alpha) = m^{n-1}g(\alpha) = 0$. Hence $\beta = m\alpha \in \mathbf{B}$ and $\alpha = \beta/m$. □

Let $\alpha \in \mathbf{A}$. Then there is a monic polynomial $f \in \mathbf{Q}[X]$ of least degree such that $f(\alpha) = 0$. This polynomial is uniquely determined.

Proposition 1.1 *Let $\alpha \in \mathbf{A}$. Then there is precisely one monic polynomial $f \in \mathbf{Q}[X]$ of minimum degree with $f(\alpha) = 0$. This polynomial f has the property that if $g \in \mathbf{Q}[X]$ and $g(\alpha) = 0$ then $f \mid g$.*

Proof Note first that if $h \in \mathbf{Q}[X]$ is a nonzero polynomial with $\deg(h) < \deg(f)$, then $h(\alpha) \neq 0$ since otherwise $h_1 = a^{-1}h$ is a monic polynomial, where a is the leading coefficient of h, with the property that $\deg(h_1) < \deg(f)$ and $h_1(\alpha) = 0$. That would contradict the definition of f. Now f is unique, since if f_1 had the same degree as f and also satisfied the same conditions then $h = f - f_1$, if nonzero, has $h \in \mathbf{Q}[X]$, $h(\alpha) = 0$ and $\deg(h) < \deg(g)$ which is impossible.

Now let $g \in \mathbf{Q}[X]$ and suppose that $g(\alpha) = 0$. By the division algorithm (Proposition A.1), $g = qf + h$ where q, $h \in \mathbf{Q}[X]$, and either $h = 0$ (which means that $f \mid g$ as we want) or $h \neq 0$ and $\deg(h) < \deg(f)$. But as $h(\alpha) = g(\alpha) - f(\alpha)q(\alpha) = 0$ this is impossible. □

We call this f the *minimum polynomial* of α and call its degree the *degree* of α. Minimum polynomials are always irreducible.

Lemma 1.2 *Let f be the minimum polynomial of $\alpha \in \mathbf{A}$. Then f is irreducible over $\mathbf{Q}$.*

Proof If f is not irreducible then $f = gh$ where g, $h \in \mathbf{Q}[X]$ are monic polynomials of degree less than that of f. Then $0 = f(\alpha) = g(\alpha)h(\alpha)$ and so either $g(\alpha) = 0$ or $h(\alpha) = 0$. We may assume $g(\alpha) = 0$. Then $f \mid g$ which is impossible since $\deg(g) < \deg(f)$. □

Suppose the minimum polynomial f of α lies in $\mathbf{Z}[X]$. Then, since f is monic and $f(\alpha) = 0$, α is an algebraic integer. In fact the converse holds: if $\alpha \in \mathbf{B}$ then its minimum polynomial lies in $\mathbf{Z}[X]$. We need to study integer polynomials in more detail to prove this.

A nonzero polynomial $f \in \mathbf{Z}[X]$ is *primitive* if the greatest common divisor of its coefficients is 1. Equivalently f is primitive if there is no prime number dividing all its coefficients.

Lemma 1.3 (Gauss's Lemma) *Let f, $g \in \mathbf{Z}[X]$ be primitive polynomials. Then fg is also a primitive polynomial.*

Proof Write

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_mX^m$$

and

$$g(X) = b_0 + b_1X + b_2X^2 + \cdots + b_nX^n.$$

We show that there is no prime p dividing all the coefficients of fg. Take a prime p. As f is primitive there is a coefficient of f not divisible by p; let a_r be the **first** such. Similarly let b_s be the first coefficient of g not divisible by p. Then $p \mid a_i$ for $i < r$ and $p \mid b_j$ for $j < s$. The coefficient of X^{r+s} in fg is

$$c_{r+s} = \sum_{i+j=r+s} a_ib_j.$$

This sum contains the term a_rb_s, which is not divisible by p. Its other terms a_ib_j are all divisible by p, since they either have $i < r$ or $j < s$. Hence c_{r+s} is not divisible by p.

As there is no prime dividing all the coefficients of fg, the polynomial fg is primitive. □

If $f \in \mathbf{Z}[X]$ is nonzero, let a be the greatest common divisor of the coefficients of f. Then $f = af_1$ where f_1 is primitive. We call a the *content* of f and denote it by $c(f)$. More generally, let g be a nonzero element of $\mathbf{Q}[X]$. Then $bg \in \mathbf{Z}[X]$ where the positive integer b is the product of the denominators of the coefficients of f. Then $bg = cg_1$ where c is the content of bg and g_1 is primitive. Hence $g = (c/b)g_1$ where q_1 is primitive polynomial in $\mathbf{Z}[X]$ and c/b is a positive rational. We can write any nonzero $g \in \mathbf{Z}[X]$ as $g = rg_1$ with $r \in \mathbf{Q}$, $r > 0$ and $g_1 \in \mathbf{Z}[X]$ being primitive. It's an instructive exercise to show that this r is uniquely determined; hence it makes sense to call r the *content* of g. Putting $s = 1/r$ we see that there is a positive rational s with sg a primitive element of $\mathbf{Z}[X]$.

We now show that if a monic polynomial in $\mathbf{Z}[X]$ factors over the rationals then it factors over the integers.

Proposition 1.2 *Let f and g be monic polynomials with $f \in \mathbf{Z}[X]$ and $g \in \mathbf{Q}[X]$. If $g \mid f$ then $g \in \mathbf{Z}[X]$.*

Proof Suppose that $g \mid f$. Then $f = gh$ where $h \in \mathbf{Q}[X]$. Then h is monic, as both f and g are. There are positive rationals r and s with rg and sh primitive elements of $\mathbf{Z}[X]$. The leading coefficients of rg and sh are r and s respectively, so that r, $s \in \mathbf{Z}$. By Gauss's lemma, $(rg)(sh) = (rs)f$ is primitive. But since $f \in \mathbf{Z}[X]$ all coefficients of $(rs)f$ are divisible by rs.

Hence $rs = 1$ (as rs is a positive integer) and so $r = s = 1$ (as r and s are positive integers). Thus $g = rg \in \mathbf{Z}[X]$ as required. □

An immediate corollary is this important characterization of algebraic integers.

Theorem 1.1 *Let $\alpha \in \mathbf{A}$ have minimum polynomial f. Then $\alpha \in \mathbf{B}$ if and only if $f \in \mathbf{Z}[X]$.*

Proof Suppose $f \in \mathbf{Z}[X]$. Since f is monic and $f(\alpha) = 0$ then $\alpha \in \mathbf{B}$.

Conversely suppose that $\alpha \in \mathbf{B}$. There is a monic $g \in \mathbf{Z}[X]$ with $g(\alpha) = 0$. Then $f \mid g$, since f is the minimum polynomial of α. By Proposition 1.2, $f \in \mathbf{Z}[X]$. □

Another corollary is this useful criterion for irreducibility.

Proposition 1.3 (Eisenstein's criterion) *Let p be a prime number and let*

$$f(X) = X^n + \sum_{j=0}^{n-1} a_j X^j \in \mathbf{Z}[X].$$

If

- *$p \mid a_j$ when $0 \leq j < n$, and*
- *$p^2 \nmid a_0$*

then f is irreducible over $\mathbf{Q}$.

Proof Suppose that f is reducible over $\mathbf{Q}$. Then $f = gh$ where $g, h \in \mathbf{Q}[X]$, g and h are monic, and also $0 < r = \deg(g) < n$ and $\deg(g) = s = n - r$. By Proposition 1.2, $g, h \in \mathbf{Z}[X]$. Write

$$g(X) = \sum_{i=0}^{r} b_i X^i \qquad \text{and} \qquad h(X) = \sum_{j=0}^{s} c_j X^j.$$

Note that $b_r = 1 = c_s$. Certainly $p \nmid b_r$ and $p \nmid c_s$. Let u and v be the least nonnegative integers with $p \nmid b_u$ and $p \nmid c_v$. Then $u \leq r$ and $v \leq s$. I claim that $u = r$ and $v = s$. Otherwise $u + v < r + s = n$ and

$$a_{u+v} = \sum_{i+j=u+v} b_i c_j.$$

This sum contains the term $b_u c_v$ which which is not divisible by p. The remaining terms have the form $b_i c_j$ with either $i < u$ or $j < v$. In each case

one of b_i and c_j is divisible by p. Hence a_{u+v} is the sum of a nonmultiple of p with a collection of multiples of p and so $p \nmid a_{u+v}$ contrary to hypothesis. Hence $u = r$ and $v = s$. As r, $s > 0$ both b_0 and c_0 are divisible by p so that $a_0 = b_0 c_0$ is divisible by p^2 again contrary to hypothesis. This contradiction shows that f is irreducible over $\mathbf{Q}$. □

Example Let p be a prime number and let

$$f(X) = 1 + X + X^2 + \cdots + X^{p-1} = \sum_{j=0}^{p-1} X^j = \frac{X^p - 1}{X - 1}.$$

We cannot apply Eisenstein to f directly, but if we set $f_1(X) = f(X + 1)$ we get

$$f_1(X) = \frac{(X+1)^p - 1}{(X+1) - 1} = \frac{(X+1)^p - 1}{X} = \sum_{j=0}^{p-1} \binom{p}{j} X^{p-j-1}.$$

This is a monic polynomial, but its remaining coefficients have the form $\binom{p}{j}$ for $0 < j < p$ and so are divisible by p. The final coefficient is $\binom{p}{p-1} = p$ which is not divisible by p^2. By Eisenstein's criterion, f_1 is irreducible over $\mathbf{Q}$. It follows that f is irreducible over $\mathbf{Q}$, for if $f(X) = g(X)h(X)$ were a nontrivial factorization of f, then $f_1(X) = g(X + 1)h(X + 1)$ would be a nontrivial factorization of f_1.

We now show that $\mathbf{A}$ is a subfield of $\mathbf{C}$ and $\mathbf{B}$ is a subring of $\mathbf{C}$.

Theorem 1.2 (i) *Let α, $\beta \in \mathbf{A}$. Then $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta \in \mathbf{A}$, and if $\alpha \neq 0$ then $\alpha^{-1} \in \mathbf{A}$.*
(ii) *Let α, $\beta \in \mathbf{B}$. Then $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta \in \mathbf{B}$.*

Proof We first prove (ii) in detail, since the bulk of the proof of (i) follows *mutatis mutandis*.

Let α and β have minimum polynomials f and g of degrees m and n respectively. Write

$$f(X) = X^m + \sum_{i=0}^{m-1} a_i X^i \qquad \text{and} \qquad g(X) = X^n + \sum_{j=0}^{n-1} b_j X^j.$$

Then the a_i and b_j are integers and

$$\alpha^m = -\sum_{i=0}^{m-1} a_i \alpha^i \qquad \text{and} \qquad \beta^n = -\sum_{j=0}^{n-1} b_j \beta^j. \qquad (*)$$

Let $\mathbf{v}$ be the column vector of height mn given by

$$\mathbf{v}^\top = (1\ \alpha\ \alpha^2\ \cdots\ \alpha^{m-1}\ \beta\ \alpha\beta\ \alpha^2\beta\ \cdots\ \alpha^{m-1}\beta\ \beta^2\ \cdots\ \alpha^{m-1}\beta^{n-1}).$$

In other words the entries of $\mathbf{v}$ are the numbers $\alpha^i\beta^j$ for $0 \le i < m$ and $0 \le j < n$. I claim that there are (mn-by-mn) matrices A and B with entries in $\mathbf{Z}$ such that $A\mathbf{v} = \alpha\mathbf{v}$ and $B\mathbf{v} = \beta\mathbf{v}$. The typical entry in $\alpha\mathbf{v}$ has the form $\alpha^i\beta^j$ where $1 \le i \le m$ and $0 \le j < n$. If $i < m$ this already is an entry of $\mathbf{v}$ while if $i = m$, $(*)$ gives

$$\alpha^m\beta^j = -\sum_{k=0}^{m-1} a_k\alpha^k\beta^j.$$

In any case this entry $\alpha^i\beta^j$ of $\alpha\mathbf{v}$ is a linear combination, with integer coefficients, of the entries of $\mathbf{v}$. Putting these coefficients into a matrix A we get $\alpha\mathbf{v} = A\mathbf{v}$. Similarly there is a matrix B with integer entries with $\beta\mathbf{v} = B\mathbf{v}$.

Now $(A+B)\mathbf{v} = (\alpha+\beta)\mathbf{v}$, $(A-B)\mathbf{v} = (\alpha-\beta)\mathbf{v}$ and $(AB)\mathbf{v} = (\alpha\beta)\mathbf{v}$. As $\mathbf{v} \neq 0$ the numbers $\alpha+\beta$, $\alpha-\beta$ and $\alpha\beta$ are eigenvalues of the matrices $A+B$, $A-B$ and AB each of which has integer entries. But if the matrix C has integer entries, its eigenvalues are algebraic integers, since the characteristic polynomial of C is a monic polynomial with integer coefficients. It follows that $\alpha+\beta$, $\alpha-\beta$ and $\alpha\beta$ are all algebraic integers.

If we assume instead that $\alpha,\ \beta \in \mathbf{A}$, the above argument shows (when we replace 'integer' by 'rational' etc.) that $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$ are all algebraic numbers.

Finally suppose that α is a nonzero algebraic number with minimum polynomial

$$f(X) = X^n + \sum_{i=0}^{n-1} a_i X^i.$$

Then $a_0 \neq 0$ (why?) and dividing the equation $f(\alpha) = 0$ by $a_0\alpha^n$ gives

$$\alpha^{-n} + \sum_{i=1}^{n-1} \frac{a_{n-i}}{a_0}\alpha^{-i} + \frac{1}{a_0} = 0$$

so that $\alpha^{-1} \in \mathbf{A}$. □

Example Let us see what the matrices A and B are for say $\alpha = \sqrt{2}$ and $\beta = \frac{1}{2}(1+\sqrt{5})$. The minimum polynomials of α and β are X^2-2 and X^2-X-1 respectively so that $\alpha^2 = 2$ and $\beta^2 = \beta+1$. Let $\mathbf{v}^\top = (1\ \alpha\ \beta\ \alpha\beta)$.

Then

$$\alpha\mathbf{v} = \begin{pmatrix} \alpha \\ \alpha^2 \\ \alpha\beta \\ \alpha^2\beta \end{pmatrix} = \begin{pmatrix} \alpha \\ 2 \\ \alpha\beta \\ 2\beta \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \beta \\ \alpha\beta \end{pmatrix}$$

and

$$\beta\mathbf{v} = \begin{pmatrix} \beta \\ \alpha\beta \\ \beta^2 \\ \alpha\beta\beta^2 \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha\beta \\ 1+\beta \\ \alpha+\alpha\beta \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \beta \\ \alpha\beta \end{pmatrix}.$$

We can take

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Then, for instance, $\alpha\beta$ is an eigenvalue of

$$AB = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 1 \\ 2 & 0 & 2 & 0 \end{pmatrix}$$

so that $h(\alpha\beta) = 0$ where h is the characteristic polynomial of AB.

2 Number fields

The set $\mathbf{A}$ of algebraic numbers is too large to handle all at once. We restrict our consideration to looking at smaller subfields of $\mathbf{A}$ which contain all the algebraic numbers "generated" from a given one. For instance consider

$$K_1 = \mathbf{Q}(i) = \{a + bi : a, b \in \mathbf{Q}\}$$

and

$$K_2 = \mathbf{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbf{Q}\}.$$

It is apparent that both K_1 and K_2 are rings, being closed under addition, subtraction and multiplication. It's not hard to see that K_1 is a field since if $a + bi$ is a nonzero element of K_1 then

$$\frac{1}{a+bi} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i \in \mathbf{Q}(i).$$

But it is not so obvious that $1/(a + b\sqrt[3]{2} + c\sqrt[3]{4})$ is an element of K_2. But this is in fact so, and is an example of a general phenomenon.

Let α be an algebraic number of degree n. Define

$$\mathbf{Q}(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} : a_0, a_1, \ldots, a_{n-1} \in \mathbf{Q}\}.$$

Proposition 2.1 *For each $\alpha \in \mathbf{A}$, $\mathbf{Q}(\alpha)$ is a subfield of $\mathbf{A}$.*

Proof Since $\mathbf{A}$ is closed under addition and multiplication, and $\alpha \in \mathbf{A}$ and $\mathbf{Q} \subseteq \mathbf{A}$ then it is apparent that $\mathbf{Q}(\alpha) \subseteq \mathbf{A}$.

Let α have degree n and minimum polynomial f. Then by definition

$$\mathbf{Q}(\alpha) = \{g(\alpha) : g \in \mathbf{Q}[X], \text{ and either } g = 0 \text{ or } \deg(g) < n\}.$$

I claim that in fact

$$\mathbf{Q}(\alpha) = \{g(\alpha) : g \in \mathbf{Q}[X]\}.$$

Certainly $\mathbf{Q}(\alpha) \subseteq \{g(\alpha) : g \in \mathbf{Q}[X]\}$ so that to prove equality we need to show that $g(\alpha) \in \mathbf{Q}(\alpha)$ whenever $g \in \mathbf{Q}[X]$. By the division algorithm (Proposition A.1) there is $q \in \mathbf{Q}[X]$ such that $h = g - qf$ either vanishes or has $\deg(h) < n$. Then $h(\alpha) \in \mathbf{Q}(\alpha)$ but $h(\alpha) = g(\alpha) - f(\alpha)q(\alpha) = g(\alpha)$ as $f(\alpha) = 0$. This proves that $\mathbf{Q}(\alpha) = \{g(\alpha) : g \in \mathbf{Q}[X]\}$.

It is now clear that, since $\mathbf{Q}[X]$ is closed under addition, subtraction and multiplication then so is $\mathbf{Q}(\alpha)$. Hence $\mathbf{Q}(\alpha)$ is a subring of $\mathbf{A}$. (Alternatively, one sees that the map $g \mapsto g(\alpha)$ from $\mathbf{Q}[X]$ to $\mathbf{A}$ is a ring homomorphism with image $\mathbf{Q}(\alpha)$ which must therefore be a subring of $\mathbf{A}$.)

To complete the proof that $\mathbf{Q}(\alpha)$ is a field, we must show that $1/\beta \in \mathbf{Q}(\alpha)$ whenever β is a nonzero element of $\mathbf{Q}(\alpha)$. Write $\beta = g(\alpha)$ with $g \in \mathbf{Q}[X]$ and note that $f \nmid g$ since otherwise $g(\alpha) = 0$. Let h be the greatest common divisor of f and g. By Proposition A.2, there exist u, $v \in \mathbf{Q}[X]$ with $h = uf + vg$. But f is irreducible, and so either $h = 1$ or $h = f$. But this latter is impossible since $h \nmid f$. Hence $1 = uf + vg$ and so $1 = u(\alpha)f(\alpha) + v(\alpha)g(\alpha) = v(\alpha)\beta$. It follows that $1/\beta = v(\alpha) \in \mathbf{Q}(\alpha)$ and so K is a field. □

The numbers $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, where n is the degree of α, form a basis of $\mathbf{Q}(\alpha)$ as a vector space over $\mathbf{Q}$. Thus the degree n is also the dimension of $\mathbf{Q}(\alpha)$ as a vector space over $\mathbf{Q}$, and so we call n the *degree* of $\mathbf{Q}(\alpha)$. In general when we speak of a *basis* for a number field $K = \mathbf{Q}(\alpha)$ me mean a basis for K as a vector space over $\mathbf{Q}$.

Given $\alpha \in \mathbf{A}$ of degree n, its minimum polynomial f factors over $\mathbf{C}$ as

$$f(X) = \prod_{j=1}^{n}(X - \alpha_j)$$

where $\alpha = \alpha_1$ say. The numbers $\alpha_1, \ldots, \alpha_n$ are the *conjugates* of α. They are all algebraic numbers with minimal polynomial f. It is important to note that the conjugates of α are all distinct. This follows from the following lemma.

Lemma 2.1 *Let $f \in \mathbf{Q}[X]$ be a monic polynomial and suppose that f is irreducible over $\mathbf{Q}$. Then $f(X) = 0$ has n distinct roots in $\mathbf{C}$.*

Proof Suppose that α is a repeated root of $f(X) = 0$. Then $f(X) = (X-\alpha)^2 g(X)$ where $g(X) \in \mathbf{C}[X]$. Consequently $f'(X) = (X-\alpha)^2 g'(X) + 2(X-\alpha)g(X)$ and so $f(\alpha) = f'(\alpha) = 0$. Let h be the greatest common divisor of f and f'. Then $h = uf + vf'$ for some $u,\ v \in \mathbf{Q}[X]$. Thus $h(\alpha) = u(\alpha)f(\alpha) + v(\alpha)f'(\alpha) = 0$. But as $h \mid f$ and f is irreducible, then $h = 1$ of $h = f$. Since $h(\alpha) = 0$, $h = f$. But then $f \mid f'$ and as f' has leading term nX^{n-1} this is impossible. □

The field $\mathbf{Q}(\alpha)$ forms the set of numbers which can be expressed in terms of rational numbers and α using the standard arithmetic operations. We might instead consider what happens when we take two algebraic numbers α and β and consider which numbers can be expressed in terms of both. Suppose α and β have degrees m and n respectively, and define

$$\mathbf{Q}(\alpha,\beta) = \left\{ \sum_{j=0}^{m-1} \sum_{k=0}^{n-1} c_{jk}\alpha^j\beta^k : c_{jk} \in \mathbf{Q} \right\}.$$

It is readily apparent that $\mathbf{Q}(\alpha,\beta)$ is a ring; less apparent but nonetheless true that it is a field. However this field can be expressed in terms of one generator.

Theorem 2.1 (Primitive element) *Let $\alpha,\ \beta \in \mathbf{A}$. Then there is $\gamma \in \mathbf{A}$ with $\mathbf{Q}(\alpha,\beta) = \mathbf{Q}(\gamma)$.*

Proof We show that for a suitable rational number c, $\gamma = \alpha + c\beta$ suffices. Let α and β have degrees m and n respectively, and let their minimum polynomials be

$$f(X) = \prod_{j=1}^{m}(X-\alpha_j) \quad \text{and} \quad g(X) = \prod_{k=1}^{n}(X-\beta_k)$$

respectively, with $\alpha = \alpha_1$ and $\beta = \beta_1$. Suppose that $1 \le j \le m$ and $2 \le k \le n$. The equation

$$\alpha + x\beta = \alpha_j + x\beta_k$$

can be rewritten as

$$(\beta_1 - \beta_k)x = \alpha_1 - \alpha_j$$

and so has exactly one solution $x = x_{jk}$ as $\beta_1 \neq \beta_k$. Choose c to be a nonzero rational which is not equal to any of the x_{jk}. This is possible as $\mathbf{Q}$ is an infinite set. Then

$$\alpha + c\beta \neq \alpha_j + c\beta_k$$

whenever $k \neq 1$, by the choice of c. Let $\gamma = \alpha + c\beta$. For convenience put $K = \mathbf{Q}(\gamma)$. I claim that $\mathbf{Q}(\alpha, \beta) = K$.

Certainly $\gamma \in \mathbf{Q}(\alpha, \beta)$ and as $\mathbf{Q}(\alpha, \beta)$ is a ring, then $K \subseteq \mathbf{Q}(\alpha, \beta)$. To prove that $K \supseteq \mathbf{Q}(\alpha, \beta)$ it suffices to show that $\alpha \in K$ and $\beta \in K$. Let $h(X) = f(\gamma - cX)$. Then h has degree m, as $c \neq 0$, and $h \in K[X]$. Also $h(\beta) = f(\gamma - c\beta) = f(\alpha) = 0$. But of course $g(\beta) = 0$ so that g and h have β as a common zero. Suppose that it had another one, so that $g(\delta) = h(\delta) = 0$. Then $\delta = \beta_k$ for some $k \geq 2$ as $g(\delta) = 0$. But then $0 = h(\beta_k) = f(\gamma - c\beta_k)$ so that $\gamma - c\beta_k = \alpha_j$ for some j. Thus $\gamma = \alpha_j + c\beta_k$ which is false by the choice of c.

The greatest common divisor of $g(X)$ and $h(X)$ must be $X - \beta$. As $g \in \mathbf{Q}[X] \subseteq K[X]$ and $h \in K[X]$ there exists $u, v \in K[X]$ with $u(X)g(X) + h(X)v(X) = X - \beta$. Thus $\beta = -(u(0)g(0) + h(0)v(0)) \in K$, and it follows that $\alpha = \gamma - c\beta \in K$. This completes the proof. □

More generally we can consider fields $\mathbf{Q}(\beta_1, \ldots, \beta_n)$ generated by any finite number of algebraic numbers. But by using the primitive element theorem and induction we see that each such field still has the form $\mathbf{Q}(\gamma)$. We call a field of the form $\mathbf{Q}(\alpha)$ for $\alpha \in \mathbf{A}$ an *algebraic number field* or simply a *number field*.

Let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α. The fields $\mathbf{Q}(\alpha_j)$ are very similar to $\mathbf{Q}(\alpha)$ each being generated by an element with minimum polynomial f. In fact they are all isomorphic. We define an isomorphism $\sigma_j : \mathbf{Q}(\alpha) \to \mathbf{Q}(\alpha_j)$ by setting $\sigma_j(g(\alpha)) = g(\alpha_j)$ when $g \in \mathbf{Q}[X]$. It is perhaps not immediately evident that σ_j is well-defined. But this follows since if g_1, $g_2 \in \mathbf{Q}[X]$ and $g_1(\alpha) = g_2(\alpha)$ then $g_1(\alpha_j) = g_2(\alpha_j)$. This is a consequence of α and α_j having the same minimum polynomial. Once σ_j is seen to be well-defined, then it is straightforward to prove it is an isomorphism. As $\alpha_1 = \alpha$ then σ_1 is the identity map on $\mathbf{Q}(\alpha)$.

Let $\beta \in \mathbf{Q}(\alpha)$. We define the *norm* $N(\beta)$ and *trace* $T(\beta)$ of β as follows. Let

$$N(\beta) = \prod_{j=1}^{n} \sigma_j(\beta)$$

and

$$T(\beta) = \sum_{j=1}^{n} \sigma_j(\beta).$$

Since the σ_j preserve addition and multiplication, the following properties are almost immediate:

- $N(\beta\gamma) = N(\beta)N(\gamma)$ for all β, $\gamma \in \mathbf{Q}(\alpha)$,
- $N(c\beta) = c^n N(\beta)$ for all $c \in \mathbf{Q}$ and $\beta \in \mathbf{Q}(\alpha)$,
- $T(\beta + \gamma) = T(\beta)T(\gamma)$ for all β, $\gamma \in \mathbf{Q}(\alpha)$, and
- $T(c\beta) = cT(\beta)$ for all $c \in \mathbf{Q}$ and $\beta \in \mathbf{Q}(\alpha)$.

Clearly $N(0) = 0$ and $N(1) = 1$. If $\beta \neq 0$ then $1 = N(1) = N(\beta)N(1/\beta)$ so that $N(\beta) \neq 0$.

A word of warning: the norm $N(\beta)$ and trace $T(\beta)$ depend on the field $\mathbf{Q}(\alpha)$ as well as the number β. If we wish to be strict we should use the notation $N_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\beta)$ and $T_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\beta)$ instead.

The crucial property of the norm and trace is that they are both rational.

Theorem 2.2 *Let $\beta \in \mathbf{Q}(\alpha)$. Then $N(\beta) \in \mathbf{Q}$ and $T(\beta) \in \mathbf{Q}$.*

Proof Write $\beta = \sum_{k=0}^{n-1} b_k \alpha^k$ where the $b_j \in \mathbf{Q}$. Then

$$N(\beta) = \prod_{j=1}^{n} \sum_{k=0}^{n-1} b_k \alpha_j^k \qquad \text{and} \qquad T(\beta) = \sum_{j=1}^{n} \sum_{k=0}^{n-1} b_k \alpha_j^k.$$

Both $N(\beta)$ and $T(\beta)$ are symmetric polynomials with rational coefficients in the variables $\alpha_1, \ldots, \alpha_n$. By Newton's theorem on symmetric polynomials (Theorem A.2), $N(\beta) = g_1(e_1, e_2, \ldots, e_n)$ and $T(\beta) = g_2(e_1, e_2, \ldots, e_n)$ where g_1 and g_2 are polynomials in n variables with rational coefficients and $e_1, \ldots, e_n$ are the elementary symmetric polynomials in the variables $\alpha_1, \ldots, \alpha_n$. But

$$X^n + \sum_{j=1}^{n} (-1)^j e_j X^{n-j} = \prod_{j=1}^{n} (X - \alpha_j) = f(X)$$

which is the minimum polynomial of α. Hence $e_j \in \mathbf{Q}$ and so $N(\beta)$, $T(\beta) \in \mathbf{Q}$. □

More generally we can consider the *field polynomial*

$$\prod_{j=1}^{n}(X - \sigma_j(\beta)) = X^n - T(\beta)X^{n-1} + \cdots + (-1)^n N(\beta)$$

of β. Using the same argument as Theorem 2.2 one shows that all its coefficients are rational.

One gets similar results on replacing $\mathbf{A}$ by $\mathbf{B}$ and $\mathbf{Q}$ by $\mathbf{Z}$. Before proving them it's convenient to prove, in essence, that $\sigma_j(\beta)$ is always a conjugate of β.

Lemma 2.2 *Let $\alpha \in \mathbf{A}$ and $\beta \in \mathbf{Q}(\alpha)$. For each j, β and $\sigma_j(\beta)$ have the same minimum polynomial.*

Proof Let g be the minimum polynomial of β. Then

$$g(X) = X^n + \sum_{k=0}^{n-1} b_k X^k$$

where each $b_j \in \mathbf{Q}$. For any $\gamma \in \mathbf{Q}(\alpha)$ we have, since σ_j is a ring homomorphism and $\sigma_j(b) = b$ whenever $b \in \mathbf{Q}$,

$$\sigma_j(g(\gamma)) = \sigma_j(\gamma^n) + \sum_{k=0}^{n-1} \sigma_j(b_k\gamma^k) = \sigma_j(\gamma)^n + \sum_{k=0}^{n-1} b_k\sigma_j(\gamma)^k = g(\sigma_j(\gamma)).$$

In particular $g(\sigma_j(\beta)) = \sigma_j(g(\beta)) = \sigma_j(0) = 0$. As g is irreducible over $\mathbf{Q}$ then g is the minimum polynomial of $\sigma(\beta)$. □

If $\beta \in \mathbf{Q}(\alpha)$ is an algebraic integer then its minimum polynomial has integer coefficients. As $\sigma_j(\beta)$ shares this minimum polynomial, then $\sigma_j(\beta)$ is also an algebraic integer.

Proposition 2.2 *Let $\alpha \in \mathbf{A}$ and $\beta \in \mathbf{Q}(\alpha) \cap \mathbf{B}$. Then $T(\beta)$, $N(\beta) \in \mathbf{Z}$.*

Proof We already know that $T(\beta)$, $N(\beta) \in \mathbf{Q}$. But $T(\beta)$ is the sum, and $N(\beta)$ is the product of the $\sigma_j(\beta)$. As $\beta \in \mathbf{B}$ then all $\sigma_j(\beta) \in \mathbf{B}$ and so $T(\beta)$, $N(\beta) \in \mathbf{B}$. Thus $T(\beta)$, $N(\beta) \in \mathbf{Q} \cap \mathbf{B}$. But $\mathbf{Q} \cap \mathbf{B} = \mathbf{Z}$ since if $a \in \mathbf{Q}$ its minimum polynomial is $X - a$ and this has integer coefficients if and only if $a \in \mathbf{Z}$. Hence $T(\beta)$, $N(\beta) \in \mathbf{Z}$. □

More generally the same argument shows that the field polynomial of $\beta \in \mathbf{Q}(\alpha) \cap \mathbf{B}$ has integer coefficients.

Given a number field $K = \mathbf{Q}(\alpha)$ we define its *ring of integers* as $\mathcal{O}_K = K \cap \mathbf{B}$, that is the set of algebraic integers in K. In the proof of Proposition 2.2 we see that if $K = \mathbf{Q}$ then $\mathcal{O}_K = \mathbf{Z}$. We aim to develop the concepts of number theory (primes, congruences, factorizations) in the rings $\mathcal{O}_K$, just as standard number theory does for $\mathbf{Z}$.

Example A *quadratic field* is a number field of the form $\mathbf{Q}(\sqrt{m})$ where $m \in \mathbf{Q}$ but $\sqrt{m} \notin \mathbf{Q}$. Since it is easy to see that $\mathbf{Q}(\sqrt{r^2 m}) = \mathbf{Q}(\sqrt{m})$ for any nonzero rational r, each quadratic field has the form $K = \mathbf{Q}(\sqrt{m})$ where m is a *squarefree* integer, that is, m is not divisible by the square of any prime number. We shall always assume this is the case when we discuss quadratic fields.

When $m > 0$, $\mathbf{Q}(\sqrt{m})$ is a *real quadratic field* since $\mathbf{Q}(\sqrt{m}) \subseteq \mathbf{R}$, and when $m < 0$, $\mathbf{Q}(\sqrt{m})$ is an *imaginary quadratic field* since $\mathbf{Q}(\sqrt{m}) \not\subseteq \mathbf{R}$.

We shall compute $\mathcal{O}_K$ whenever $K = \mathbf{Q}(\sqrt{m})$ is a quadratic field. Let $\beta = a + b\sqrt{m} \in K$ with a, $b \in \mathbf{Q}$. For $\alpha \in \mathcal{O}_K$ it is necessary that $T(\beta)$, $N(\beta) \in \mathbf{Z}$ and this is sufficient too, since $\beta^2 - T(\beta)\beta + N(\beta) = 0$. Suppose that $T(\beta)$, $N(\beta) \in \mathbf{Z}$. Then $2a = T(\beta) \in \mathbf{Z}$ and $a^2 - mb^2 = N(\beta) \in \mathbf{Z}$. It follows that $m(2b)^2 = T(\beta)^2 - 4N(\beta) \in \mathbf{Z}$. Since m is squarefree, $2b \in \mathbf{Z}$ for otherwise, $2b$ would have a power of a prime p dividing its denominator. But then, since $p^2 \nmid m$, so would $m(2b)^2$. We can write $\beta = \frac{1}{2}(c + d\sqrt{m})$ with c, $d \in \mathbf{Z}$. Finally $c^2 - md^2 = 4N(\beta) \equiv 0 \pmod 4$. Since m is squarefree, $m \not\equiv 0 \pmod 4$. As odd squares are congruent to 1 modulo 4, and even squares are divisible by 4, then $c^2 - md^2 \equiv 0 \pmod 4$ is only possible if c and d are both even, or if they are both odd and $m \equiv 1 \pmod 4$.

To conclude, when $m \not\equiv 1 \pmod 4$ then

$$\mathcal{O}_K = \{a + b\sqrt{m} : a, b \in \mathbf{Z}\} = \mathbf{Z}[\sqrt{m}]$$

and when $m \equiv 1 \pmod 4$ then

$$\begin{aligned} \mathcal{O}_K &= \left\{ \frac{c + d\sqrt{m}}{2} : c, d \in \mathbf{Z}, c \equiv d \pmod 2 \right\} \\ &= \left\{ a + b\left(\frac{1 + \sqrt{m}}{2} \right) : a, b \in \mathbf{Z} \right\} \\ &= \mathbf{Z}\left[\frac{1 + \sqrt{m}}{2} \right]. \end{aligned}$$

For quadratic fields K we have show that there exist β_1 and β_2 such that $\mathcal{O}_K = \{a_1\beta_1 + a_2\beta_2 : a_1, a_2 \in \mathbf{Z}\}$. (We have $\beta_1 = 1$ and $\beta_2 = \sqrt{m}$ or $\frac{1}{2}(1+\sqrt{m})$ as appropriate.) Our aim will be to show that the corresponding property

holds for every number field. Indeed if K is a number field of degree n, then there exist $\beta_1, \ldots, \beta_n \in \mathcal{O}_K$ with the property that each element of $\mathcal{O}_K$ can be uniquely expressed in the form $\sum_{j=1}^{n} a_j \beta_j$ where the $a_j \in \mathbf{Z}$. To this end we need to introduce the concept of discriminant.

Let $K = \mathbf{Q}(\alpha)$ be a number field of degree n. Let $\beta_1, \ldots, \beta_n \in K$. We define $M(\beta_1, \ldots, \beta_n)$ as the matrix whose (j,k)-entry is $T(\beta_j \beta_k)$. We the define the *discriminant* of the sequence $\beta_1, \ldots, \beta_n$ as $\Delta(\beta_1, \ldots, \beta_n) = \det(M(\beta_1, \ldots, \beta_n))$. Then as each $T(\beta_j \beta_k) \in \mathbf{Q}$, $\Delta(\beta_1, \ldots, \beta_n) \in \mathbf{Q}$.

Lemma 2.3 *Let K be a number field of degree n and let $\beta_1, \ldots, \beta_n \in K$. Then*

$$\Delta(\beta_1, \ldots, \beta_n) = \det(N(\beta_1, \ldots, \beta_n))^2$$

where $N(\beta_1, \ldots, \beta_n)$ is the matrix whose (j,k)-entry is $\sigma_k(\beta_j)$.

Proof Let $M = M(\beta_1, \ldots, \beta_n)$ and $N = N(\beta_1, \ldots, \beta_n)$. The (j,k)-entry of $NN^\top$ is

$$\sum_{i=1}^{n} \sigma_i(\beta_j)\sigma_i(\beta_k) = \sum_{i=1}^{n} \sigma_i(\beta_j \beta_k) = T(\beta_j \beta_k)$$

so that $NN^\top = M$. Hence $\det(M) = \det(N)\det(N^\top) = \det(N)^2$. □

Example Suppose that $K = \mathbf{Q}(\alpha)$ has degree n. We shall compute $\Delta(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$. By the Lemma,

$$\Delta(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 \\ \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & \cdots & \alpha_n^3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \alpha_3^{n-1} & \cdots & \alpha_n^{n-1} \end{vmatrix}^2$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the conjugates of α. But this is a Vandermonde determinant, and so by Proposition A.5

$$\Delta(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \prod_{1 \le j < k \le n} (\alpha_k - \alpha_j)^2.$$

In particular $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$ since the α_j are distinct.

We can continue to get a simpler formula. We have

$$\begin{aligned} \prod_{1 \le j < k \le n} (\alpha_k - \alpha_j)^2 &= (-1)^{n(n-1)/2} \prod_{1 \le j < k \le n} (\alpha_j - \alpha_k)(\alpha_k - \alpha_j) \\ &= (-1)^{n(n-1)/2} \prod_{\substack{1 \le j,k \le n \\ j \neq k}} (\alpha_j - \alpha_k). \end{aligned}$$

Let $f(X) = \prod_{k=1}^{n}(X - \alpha_k)$ be the minimum polynomial of α. Then by the product rule for differentiation

$$f'(X) = \sum_{j=1}^{n} \prod_{\substack{k=1 \\ k \neq k}}^{n} (X - \alpha_k).$$

When $X = \alpha_j$ only the j-th summand is nonzero, so

$$f'(\alpha_j) = \prod_{\substack{k=1 \\ k \neq k}}^{n} (\alpha_j - \alpha_k).$$

Hence

$$\Delta(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = (-1)^{n(n-1)/2} \prod_{j=1}^{n} f'(\alpha_j) = (-1)^{n(n-1)/2} N(f'(\alpha_j)).$$

Since $\Delta(\beta_1, \ldots, \beta_n) \neq 0$ for some choice of the β_j, then $\Delta(\beta_1, \ldots, \beta_n) \neq 0$ in many other cases. The following lemma enables us to relate the discriminants of different sequences.

Lemma 2.4 *Let K be a number field of degree n and let $\beta_1, \ldots, \beta_n \in K$. If $B = (b_{jk})$ is an n-by-n matrix over $\mathbf{Q}$ and $\gamma_j = \sum_{k=1}^{n} b_{jk}\beta_k$ then*

$$\Delta(\gamma_1, \ldots, \gamma_n) = \det(B)^2 \Delta(\beta_1, \ldots, \beta_n).$$

Proof We have $\Delta(\beta_1, \ldots, \beta_n) = \det(N(\beta_1, \ldots, \beta_n))^2$ where the (j, k) entry of $N(\beta_1, \ldots, \beta_n)$ is $\sigma_k(\beta_j)$. Now $\sigma_k(\gamma_j) = \sum_{i=1}^{n} b_{ji}\sigma_k(\beta_i)$ so that

$$N(\gamma_1, \ldots, \gamma_n) = BN(\beta_1, \ldots, \beta_n).$$

Taking determinants and squaring completes the proof. □

We can now show how the discriminant discriminates between bases and nonbases.

Proposition 2.3 *Let K be a number field of degree n and let $\beta_1, \ldots, \beta_n \in K$. Then $\beta_1, \ldots, \beta_n$ form a basis of K as a vector space over $\mathbf{Q}$ if and only if $\Delta(\beta_1, \ldots, \beta_n) \neq 0$.*

Proof Certainly we can write $\beta_j = \sum_{k=1}^{n} b_{jk}\alpha^{k-1}$ with $b_{jk} \in \mathbf{Q}$. Let B be the matrix with the b_{jk} as entries. Then by Lemma 2.4

$$\Delta(\beta_1, \ldots, \beta_n) = \det(B)^2 \Delta(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$$

and so $\Delta(\beta_1, \ldots, \beta_n) \neq 0$ if and only if $\det(B) \neq 0$. But $\det(B) \neq 0$ if and only if the β_j form a basis of K as a vector space over $\mathbf{Q}$. $\square$

Let K be a number field of degree n. Certainly $\mathcal{O}_K$ is a subgroup of K under the operation of addition. We aim to show that there are $\beta_1, \ldots, \beta_n \in \mathcal{O}_K$ with each element of $\mathcal{O}_K$ uniquely expressible in the form $\sum_{j=1}^{n} b_j \beta_j$ where the $\beta_j \in \mathbf{Z}$. A sequence $\beta_1, \ldots, \beta_n$ satisfying this is called an *integral basis* of $\mathcal{O}_K$. More generally if G is an abelian group under the operation of addition, then an *integral basis* of G is a sequence $\gamma_1, \ldots, \gamma_m$ of elements of G such that each element of G uniquely expressible as $\sum_{j=1}^{m} c_j \gamma_j$ with the $\gamma_j \in \mathbf{Z}$. If G has an integral basis with m elements then we say that G is a *free abelian group of rank* m. The basic theory of free abelian groups is outlined in Appendix A.3.

Theorem 2.3 *Let K be a number field of degree n. Then $\mathcal{O}_K$ is a free abelian group of rank n.*

Proof Let $\beta_1, \ldots, \beta_n$ be a basis of K. Then for positive integers $r_1, \ldots, r_n$ the sequence $r_1\beta_1, \ldots, r_n\beta_n$ is also a basis of K. By Lemma 1.1 we may choose the r_j such that $r_j\beta_j \in \mathcal{O}_K$ for each j. Replacing β_j by $r_j\beta_j$ we see that there is a basis $\beta_1, \ldots, \beta_n$ of K with each $\beta_j \in \mathcal{O}_K$.

Suppose that $\gamma = \sum_{k=1}^{n} c_k\beta_k \in \mathcal{O}_K$ where the $c_k \in \mathbf{Q}$. Then for each k, $\beta_j\gamma \in \mathcal{O}_K$ and so $T(\beta_j\gamma) \in \mathbf{Z}$. Thus $d_j = \sum_{k=1}^{n} c_k T(\beta_j\beta_k) \in \mathbf{Z}$ for all j. Let M be the matrix with (j,k)-entry $T(\beta_j\beta_k)$. Then $\mathbf{d} = M\mathbf{c}$ where $\mathbf{c}$ and $\mathbf{d}$ are the column vectors with j-th entries c_j and d_j respectively. Now $\det(M) = \Delta(\beta_1, \ldots, \beta_n) \neq 0$ as the β_j form a basis. Hence $\mathbf{c} = M^{-1}\mathbf{d}$. The matrix M has integer entries so that $M^{-1} = (\det(M))^{-1}\mathrm{adj}(M)$. Let $\Delta = \det(M)$. Then $\mathrm{adj}(M)$ and $\mathbf{d}$ have integer entries and so $\Delta\mathbf{c}$ has integer entries. Hence $\Delta c_j \in \mathbf{Z}$ for all j.

Let $A = \{a_1\beta_1 + \cdots + a_n\beta_n : a_j \in \mathbf{Z}\}$ and $B = \{\Delta^{-1}(a_1\beta_1 + \cdots + a_n\beta_n) : a_j \in \mathbf{Z}\}$. Since the β_j form a basis of K, the β_j form an integral basis of A and the β_j/Δ form an integral basis of B. We have shown that $A \subseteq \mathcal{O}_K \subseteq B$. Since B is free abelian of rank n, then $\mathcal{O}_K$ is free abelian of rank m where $m \leq n$ by Proposition A.3. Again by this proposition, since $A \subseteq \mathcal{O}_K$, $n \leq m$. Hence $m = n$. $\square$

The choice of integral basis for the ring of integers of a number field K is not unique. However, the discriminant of each integral basis is the same.

Proposition 2.4 *Let K be a number field of degree n, and let $\beta_1, \ldots, \beta_n$ and $\gamma_1, \ldots, \gamma_n$ be integral bases of $\mathcal{O}_K$. Then $\Delta(\beta_1, \ldots, \beta_n) = \Delta(\gamma_1, \ldots, \gamma_n)$.*

Proof We can write $\gamma_j = \sum_{k=1}^n b_{jk}\beta_k$ and $\beta_j = \sum_{k=1}^n c_{jk}\gamma_k$ where all the b_{jk} and c_{jk} are integers. Let B and C be the matrices with (j,k)-entries b_{jk} and c_{jk} respectively. Now

$$\beta_j = \sum_{k=1}^n c_{jk}\gamma_k = \sum_{k=1}^n \sum_{i=1}^n c_{jk}b_{ki}\beta_i = \sum_{i=1}^n d_{ji}\beta_i$$

where $d_{ji} = \sum_{k=1}^n c_{jk}b_{ki} \in \mathbf{Z}$. From the uniqueness of representations of elements of $\mathcal{O}$ in terms of the β_i we must have $d_{jj} = 1$ and $d_{ji} = 0$ whenever $j \neq i$. But d_{ji} is the (j,i) entry of the matrix CB. Hence $CB = I$, the identity matrix. Thus $\det(C)\det(B) = \det(I) = 1$ and as $\det(B)$ and $\det(C)$ are integers $\det(B) = \det(C) = \pm 1$. But by Proposition 2.4,

$$\Delta(\gamma_1, \ldots, \gamma_n) = \det(B)^2\Delta(\beta_1, \ldots, \beta_n) = \Delta(\beta_1, \ldots, \beta_n).$$

□

The nonzero integer

$$\Delta_K = \Delta(\beta_1, \ldots, \beta_n),$$

where $\beta_1, \ldots, \beta_n$ form an integral basis of $\mathcal{O}_K$, only depends (as the notation suggests) on the field K. We call Δ_K the *discriminant* of K. After the degree, it is the most important numerical invariant of the field.

Let $\beta_1, \ldots, \beta_n$ be an integral basis for $\mathcal{O}_K$ and suppose that $\gamma_1, \ldots, \gamma_n \in \mathcal{O}_K$ and that $\gamma_1, \ldots, \gamma_n$ are linearly independent over $\mathbf{Q}$. Then $\gamma_1, \ldots, \gamma_n$ form an integral basis of the subgroup $H = \{\sum_{j=1}^n a_j\gamma_j : a_j \in \mathbf{Z}\}$ of $\mathcal{O}_K$. However, it may happen that $H \neq \mathcal{O}_K$. We have $\Delta(\gamma_1, \ldots, \gamma_n) = \det(B)^2\Delta_K$ by Lemma 2.4, where the matrix B has integer entries b_{jk} and $\gamma_j = \sum_{k=1}^n b_{jk}\beta_k$. But by Proposition A.4, $\det(B) = |\mathcal{O}_K : H|$. Hence

$$\Delta(\gamma_1, \ldots, \gamma_n) = |\mathcal{O}_K : H|^2\Delta_K.$$

Hence the index $|\mathcal{O}_K : H|$ is a number whose square divides $\Delta(\gamma_1, \ldots, \gamma_n)$. In particular if $\Delta(\gamma_1, \ldots, \gamma_n)$ is squarefree, then $|\mathcal{O}_K : H| = 1$ and $\gamma_1, \ldots, \gamma_n$ form an integral basis of $\mathcal{O}_K$.

3 Factorization

In ordinary number theory we study the integers $\mathbf{Z}$, in particular the positive integers. In algebraic number theory we study rings of integers $\mathcal{O}_K$. Each positive integer is a product of prime numbers p which have the two properties

- if $p = ab$ with a, $b \in \mathbf{Z}$ then $a = \pm 1$ or $b = \pm 1$,
- If $p \mid cd$ with c, $d \in \mathbf{Z}$ then $p \mid c$ or $p \mid d$.

These two properties are equivalent, but while it is easy to prove that the second implies the first, the converse requires the Euclidean algorithm. However the corresponding properties in $\mathcal{O}_K$ are not equivalent.

We need some definitions. A *unit* in $\mathcal{O}_K$ is an element $\beta \in \mathcal{O}_K$ such that $1/\beta \in \mathcal{O}_K$. The set of units of $\mathcal{O}_K$ is denoted by $U(\mathcal{O}_K)$ and it is apparent that it forms a group under multiplication. There is a nice characterization of units.

Lemma 3.1 *Suppose that K is a number field of degree n and let $\beta \in \mathcal{O}_K$. Then $\beta \in U(\mathcal{O}_K)$ if and only if $N(\beta) = \pm 1$.*

Proof If $\beta \in \mathcal{O}_K$, then $1/\beta \in \mathcal{O}_K$ and so $N(\beta)$, $N(1/\beta) \in \mathbf{Z}$. But $N(\beta)N(1/\beta) = N(1) = 1$ so that $N(\beta) = N(1/\beta) = \pm 1$.

Conversely suppose that $N(\beta) = \pm 1$. Then

$$\pm 1 = \prod_{j=1}^{n} \sigma_j(\beta) = \beta \prod_{j=2}^{n} \sigma_j(\beta).$$

Thus $1/\beta = \pm \prod_{j=2}^{n} \sigma_j(\beta)$ which is an algebraic integer because each $\sigma_j(\beta) \in \mathbf{B}$. Hence $\beta \in \mathcal{O}_K$. □

For $\mathbf{Z} = \mathcal{O}_{\mathbf{Q}}$, the only units are ± 1. But the unit group of $\mathcal{O}_K$ can be infinite. For example $\beta = 1 + \sqrt{2} \in K = \mathbf{Q}(\sqrt{2})$ is a unit as $N(\beta) = -1$. But $\beta > 1$ so that $\beta^m \to \infty$ as $m \to \infty$. But when m is a positive integer, $\beta^m \in U(\mathcal{O}_K)$ so that $U(\mathcal{O}_K)$ is infinite.

As for the integers we define a divisibility relation on $\mathcal{O}_K$. For β, $\gamma \in \mathcal{O}_K$ with $\beta \neq 0$ we say that $\beta \mid \gamma$ (β *divides* γ or γ *is divisible by* β) if $\gamma/\beta \in \mathcal{O}_K$ and $\beta \nmid \gamma$ otherwise. Similarly we write $\gamma \equiv \delta \pmod{\beta}$ (γ *is congruent to* δ *modulo* β) if $\beta \mid (\gamma - \delta)$. Divisibility and congruences have all the formal properties familiar from $\mathbf{Z}$ so we shall not repeat them. Note that β is a unit if and only if $\beta \mid 1$. One useful new property of divisibility is the following.

Lemma 3.2 *Let β, $\gamma \in \mathcal{O}_K$. If $\beta \mid \gamma$ then $N(\beta) \mid N(\gamma)$ as integers.*

Proof If $\beta \mid \gamma$ then $\delta = \gamma/\beta \in \mathcal{O}_K$ and $N(\gamma) = N(\beta)N(\delta)$. As $N(\beta)$, $N(\delta) \in \mathbf{Z}$ then $N(\beta) \mid N(\gamma)$. □

We can now define what turns out to be our first analogue of prime numbers. Let $\beta \in \mathcal{O}_K$. We say that β is *irreducible* if

- $\beta \neq 0$,
- β is not a unit, and
- if $\beta = \gamma\delta$ with γ, $\delta \in \mathcal{O}_K$ then either γ or δ is a unit.

In $\mathbf{Z}$, the irreducible elements have the form $\pm p$ where p is a prime number. From Lemma 3.2 it follows that if $N(\beta)$ is a prime number then β is irreducible. The converse is not true; take the example $K = \mathbf{Q}(i)$ so that $\mathcal{O}_K = \mathbf{Z}[i]$. Then 3 is irreducible in $\mathcal{O}_K$ but $N(3) = 9$ is not prime.

In each $\mathcal{O}_K$ we can achieve factorization into irreducibles.

Lemma 3.3 *Let K be a number field. Suppose that $\beta \in \mathcal{O}_K$ and that $\beta \neq 0$ and $\beta \notin U(\mathcal{O}_K)$. Then there are irreducible elements $\gamma_1, \ldots, \gamma_k \in \mathcal{O}_K$ with $\beta = \gamma_1 \cdots \gamma_k$.*

Proof By induction on $|N(\beta)|$ which is a positive integer. Since $\beta \neq 0$ and β is not a unit then $|N(\beta)| \geq 2$. If β is irreducible then take $k = 1$ and $\gamma_1 = \beta$. If β is reducible then $\beta = \beta_1\beta_2$ where β_1, $\beta_2 \in \mathcal{O}_K$ and β_1, $\beta_2 \notin U(\mathcal{O}_K)$. Then $|N(\beta_1)|$, $|N(\beta_2)| > 1$ and as $|N(\beta)| = |N(\beta_1)||N(\beta_2)|$ it follows that $|N(\beta_1)|$, $|N(\beta_2)| < |N(\beta)|$. By the induction hypothesis both β_1 and β_2 are products of irreducible elements, and by combining these factorizations we see that β is also a product of irreducible elements. □

We turn to the question of uniqueness. It is easy to see that if β is irreducible and $\xi \in U(\mathcal{O}_K)$ then $\xi\beta$ is also irreducible. Hence we can adjust factorizations by multiplying factors by units. For instance if $\beta = \gamma_1\gamma_2\gamma_3$ is a factorization into irreducibles and $\xi \in \mathcal{O}_K$ then $\beta = (\xi\gamma_1)\gamma_2(\xi^{-1}\gamma_3)$ is also a factorization into irreducibles. If we can go from one factorization to another by introducing unit factors and/or permuting the order of factors then we say that the factorizations are equivalent. From standard number theory we know that in $\mathbf{Z}$ all factorizations of a given number into irreducibles are equivalent. However this does **not** hold in all $\mathcal{O}_K$.

Example Let $K = \mathbf{Q}(\sqrt{-6})$. Then $\mathcal{O}_K = \mathbf{Z}[\sqrt{-6}]$. Now $6 = 2 \times 3 = \sqrt{-6}(-\sqrt{-6})$. I claim that these are inequivalent factorizations of 6 into irreducibles. Now $N(2) = 4$, $N(3) = 9$ and $N(\pm\sqrt{-6}) = 6$. If any of 2, 3 or $\pm\sqrt{-6}$ were reducible, their nontrivial factors would have norms 2 or 3. But suppose that $\beta \in \mathbf{Z}[\sqrt{-6}]$ has $N(\beta) = 2$ or 3. Then $\beta = a + b\sqrt{-6}$ with a, $b \in \mathbf{Z}$ and $a^2 + 6b^2 = 2$ or 3 which is impossible. Hence 2, 3 and $\pm\sqrt{-6}$ and as the norms of the factors on both sides of $2 \times 3 = \sqrt{-6}(-\sqrt{-6})$ are different then the two factorizations are inequivalent.

In this example we have $\sqrt{-6}$ is irreducible, but that $\sqrt{-6} \mid (2\times3)$, $\sqrt{-6} \nmid 2$ and $\sqrt{-6} \nmid 3$. If we study the proof of uniqueness of prime factorization

in $\mathbf{Z}$ we see that it relies on the fact that if a prime p divides a product of integers ab then it divides (at least) one of the integers a and b. This property is not shared by the irreducible element $\sqrt{-6}$ of $\mathbf{Z}[\sqrt{-6}]$. We thus make a definition. Let $\beta \in \mathcal{O}_K$. We say that β is *prime* if

- $\beta \neq 0$,
- β is not a unit, and
- if $\beta \mid \gamma\delta$ with γ, $\delta \in \mathcal{O}_K$ then either $\beta \mid \gamma$ or $\beta \mid \delta$.

From standard number theory an integer is irreducible in $\mathbf{Z}$ if and only if it is prime. However $\sqrt{-6}$ is irreducible but not prime in $\mathbf{Z}[\sqrt{-6}]$. However primes are always irreducible.

Lemma 3.4 *Let K be a number field. If β is a prime element of $\mathcal{O}_K$ then β is irreducible in $\mathcal{O}_K$.*

Proof Let β be prime and suppose that $\beta = \gamma\delta$ with γ, $\delta \in \mathcal{O}_K$. Then $\beta \mid \gamma\delta$ so that $\beta \mid \gamma$ or $\beta \mid \delta$ by primality. Without loss of generality suppose that $\beta \mid \gamma$. Then as $\gamma \mid \beta$, $\delta = \beta/\gamma$ is a unit. Hence β is irreducible. □

If in a given $\mathcal{O}_K$ every irreducible is prime then we achieve unique factorization, by an argument similar to that of unique factorization in $\mathbf{Z}$.

Proposition 3.1 *Let K be a number field and suppose that every irreducible element of $\mathcal{O}_K$ is prime. Then $\mathcal{O}_K$ has unique factorization: any two factorization of an element into irreducibles are equivalent.*

Proof Let

$$\beta = \prod_{j=1}^{r} \gamma_j = \prod_{k=1}^{s} \delta_k$$

be two factorizations of β into irreducibles. We argue that these are equivalent by induction on $|N(\beta)|$. Since γ_1 is prime and $\gamma_1 \mid \delta_1 \cdots \delta_s$ then $\gamma_1 \mid \delta_k$ for some k. By shuffling the δs we may assume that $\gamma_1 \mid \delta_1$ and as δ_1 is irreducible then $\delta_1 = \xi\gamma_1$ where ξ is a unit. Hence

$$\beta/\gamma_1 = \prod_{j=2}^{r} \gamma_j = (\xi\delta_2) \prod_{k=3}^{s} \delta_k$$

is a factorization into irreducibles and $|N(\beta/\gamma_1)| < |N(\beta)|$. By the inductive hypothesis these factorizations of β/γ_1 are equivalent, and so the given factorizations of β are equivalent. □

For some fields K, for instance $K = \mathbf{Q}$ every irreducible in $\mathcal{O}_K$ is prime and for these fields $\mathcal{O}_K$ has the unique factorization property. The reason $\mathbf{Z}$ has unique factorization is because of the Euclidean algorithm. This works as if a, $b \in \mathbf{Z}$, $a \neq 0$ and $a \nmid b$ then there is $c \in \mathbf{Z}$ with $|b - ac| < |a|$. Some other number fields have the analogous property. We say that K is *norm-Euclidean* if when β, $\gamma \in \mathcal{O}_K$ with $\beta \neq 0$, then there exists $\delta \in \mathcal{O}_K$ with $|N(\gamma - \delta\beta)| < |N(\beta)|$. In other words we get the "remainder" $\gamma - \delta\beta$ when dividing γ by β and this remainder is "smaller" than β. There is a useful alternative characterization.

Lemma 3.5 *The number field K is norm-Euclidean if and only if for all $\xi \in K$ there is $\delta \in \mathcal{O}_K$ with $|N(\xi - \delta)| < 1$.*

Proof Suppose that K is norm-Euclidean. Let $\xi \in K$. Then $\xi = \gamma/\beta$ for some β, $\gamma \in \mathcal{O}_K$ with $\beta \neq 0$. By the norm-Euclidean property, there is $\delta \in \mathcal{O}_K$ with $|N(\gamma - \delta\beta)| < |N(\beta)|$. Thus

$$1 > \left| \frac{N(\gamma - \delta\beta)}{N(\beta)} \right| = |N(\gamma/\beta - \delta)| = |N(\xi - \delta)|.$$

Conversely, suppose that for all $\xi \in K$ there is $\delta \in K$ with $|N(\xi - \delta)| < 1$. Let β, $\gamma \in \mathcal{O}_K$ with $\beta \neq 0$. Put $\xi = \gamma/\beta$. Then there is $\delta \in \mathcal{O}_K$ with $|N(\xi - \delta)| < 1$. Hence

$$|N(\gamma - \beta\delta)| = |N(\beta)||N(\xi - \delta)| < |N(\beta)|$$

as so K is norm-Euclidean. □

Example We show that $\mathbf{Q}$ is norm-Euclidean. Let $x \in \mathbf{Q}$. Then $n \leq x \leq n + 1$ for some $n \in \mathbf{Z}$. Now $|N(x - n)| = |x - n| = x - n$ and $|N(x - (n+1))| = |x - (n+1)| = n + 1 - x$. As $(x - n) + (n + 1 - x) = 1$ then one of these numbers is $\leq 1/2$. So for $a = n$ or $a = n+1$, $|N(x-a)| \leq 1/2 < 1$.

Example Consider $K = \mathbf{Q}(\sqrt{-d})$ where $d = 1$ or $d = 2$. For $\xi \in K$, $|N(\xi)| = |\xi|^2$ where $|\xi|$ denotes the absolute value of the complex number ξ. We have $\mathcal{O}_K = \mathbf{Z}[\sqrt{-d}] = \{a + b\sqrt{-d} : a, b \in \mathbf{Z}\}$. Let $\xi = x + y\sqrt{-d}$ with x, $y \in \mathbf{Q}$. There are integers a, b with $|x - a|$, $|y - b| \leq 1/2$. Let $\delta = a + b\sqrt{-d} \in \mathcal{O}_K$. Then

$$|N(\xi - \delta)| = (x - a)^2 + d(y - b)^2 \leq \frac{1 + d}{4} < 1.$$

Hence $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{-2})$ are norm-Euclidean.

Example Consider $K = \mathbf{Q}(\sqrt{-d})$ where $d = 3$, 7 or 11. We have $\mathcal{O}_K = \mathbf{Z}[\alpha] = \{a + b\alpha : a, b \in \mathbf{Z}\}$ where $\alpha = \frac{1}{2}(1 + \sqrt{-d})$. Let $\xi = x + y\sqrt{-d}$ with x, $y \in \mathbf{Q}$. There is an integer b with $|2y - b| \leq 1/2$. Then $\xi - b\alpha = \frac{1}{2}(2x - b) + \frac{1}{2}(2y - b)\sqrt{-d}$. There is an integer a with $|\frac{1}{2}(2x - b) - a| < 1/2$. Let $\delta = a + b\alpha$. Then

$$|N(\xi - \delta)| = \frac{(2x - 2a - b)^2 + d(2y - b)^2}{4} \leq \frac{1 + d/4}{4} < 1.$$

Hence $\mathbf{Q}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{-7})$ and $\mathbf{Q}(\sqrt{-11})$ are all norm-Euclidean.

Example Let $K = \mathbf{Q}(\sqrt{-6})$. Then $\mathcal{O}_K = \mathbf{Z}[\sqrt{-6}]$. Let $\xi = \frac{1}{2}(1 + \sqrt{-6})$. If $\delta = a + b\sqrt{-6} \in \mathcal{O}_K$ with a, $b \in \mathbf{Z}$, then

$$|N(\xi - \delta)| = (1/2 - a)^2 + 6(1/2 - b)^2 \geq \frac{1 + 6}{4} > 1$$

since $|c - 1/2| \geq 1/2$ for all $c \in \mathbf{Z}$. Hence $\mathbf{Q}(\sqrt{-6})$ is not norm-Euclidean.

Example Consider $K = \mathbf{Q}(\sqrt{m})$ where $m = 2$ or $m = 3$. Then $\mathcal{O}_K = \mathbf{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbf{Z}\}$. Let $\xi = x + y\sqrt{m}$ with x, $y \in \mathbf{Q}$. There are integers a, b with $|x - a|$, $|y - b| \leq 1/2$. Let $\delta = a + b\sqrt{m} \in \mathcal{O}_K$. Then

$$N(\xi - \delta) = (x - a)^2 - m(y - b)^2.$$

Thus

$$-m/4 \leq N(\xi - \delta) \leq 1/4$$

and consequently

$$|N(\xi - \delta)| \leq \max(1/4, m/4) < 1.$$

Hence $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{3})$ are norm-Euclidean.

It is apparent that if K is norm-Euclidean then $\mathcal{O}_K$ is a Euclidean domain with respect to the Euclidean function $\phi(\beta) = |N(\beta)|$. Every ideal in a Euclidean domain is principal (Proposition A.6). If all ideals of $\mathcal{O}_K$ are principal then every irreducible in $\mathcal{O}_K$ is prime.

Proposition 3.2 *Suppose that the number field K has the property that each ideal of $\mathcal{O}_K$ is principal. Then every irreducible element of $\mathcal{O}_K$ is prime.*

Proof Suppose that each ideal of $\mathcal{O}_K$ is principal. Suppose that $\beta \in \mathcal{O}_K$ is irreducible and that $\beta \mid \gamma\delta$. We must show that if $\beta \nmid \gamma$ then $\beta \mid \delta$. Let $I = \{\xi\beta + \eta\gamma : \xi, \eta \in \mathcal{O}_K\}$ be the ideal generated by β and γ. Then I is principal: $I = \langle\lambda\rangle$ say. As $\beta \in I$ then $\lambda \mid \beta$. But as β is irreducible either

$\lambda = \varepsilon\beta$ or $\lambda = \varepsilon$ where ε is a unit. If $\lambda = \varepsilon\beta$ then $\beta \mid \lambda$, but also $\lambda \mid \gamma$ as $\gamma \in I$. Hence $\beta \mid \gamma$ which is false. Hence $\lambda = \varepsilon$ and so $I = R$. Therefore $1 \in I$ so that $1 = \xi\beta + \eta\gamma$ for some ξ, $\eta \in \mathcal{O}_K$. Hence $\delta = \xi\beta\delta + \eta\gamma\delta$ from which it follows that $\beta \mid \delta$ as $\delta \mid \gamma\delta$. Hence β is prime. $\square$

When K is norm-Euclidean we get the following chain of implications. First $\mathcal{O}_K$ is a Euclidean domain. Then every ideal of $\mathcal{O}_K$ is principal. Then every irreducible in $\mathcal{O}_K$ is prime. Finally $\mathcal{O}_K$ has the unique factorization property. However not all these implications are reversible. When $K = \mathbf{Q}(\sqrt{-19})$, $\mathcal{O}_K$ has unique factorization but is not a Euclidean domain. Clark proved in 1993 that when $K = \mathbf{Q}(\sqrt{69})$ then $\mathcal{O}_K$ is a Euclidean domain despite the fact that K is not norm-Euclidean.

As an application we look at an equation where to find all integer solutions it is useful to work in a number field.

Example We wish to find all solutions of

$$x^3 = y^2 + 2 \qquad (*)$$

with x, $y \in \mathbf{Z}$.

The presence of the 2 in $(*)$ suggests that we see whether we can restrict the parity of x and y. If y is even, then $4 \mid y^2$ and so $y^2 + 2 \equiv 2 \pmod 4$. But $x^3 \not\equiv 2 \pmod 4$ so y must be odd. This forces x^3 to be odd and so x is odd.

Next we factor $(*)$ as

$$x^3 = (y + \sqrt{-2})(y - \sqrt{-2}). \qquad (\dagger)$$

This is a factorization in $K = \mathbf{Q}(\sqrt{-2})$. Note that $\mathcal{O}_K = \mathbf{Z}[\sqrt{-2}]$ and that $\mathcal{O}_K$ has unique factorization as we have seen that K is Euclidean. It is easy to see that the only units of $\mathcal{O}_K$ are ± 1. Let us write out the factorization of $y + \sqrt{-2}$ into primes, putting together repeated occurrences and also putting together occurrences of π and $-\pi$ as $-\pi^2$. We get

$$y + \sqrt{-2} = \pm\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_m^{a_m} \qquad (\ddagger)$$

where if $j \neq k$ then $\pi_j \neq \pm\pi_k$. Then $(\dagger)$ implies that

$$x^3 = \pi_1^{a_1}\pi_2^{a_2}\cdots\pi_k^{a_k}\overline{\pi}_1^{a_1}\overline{\pi}_2^{a_2}\cdots\overline{\pi}_k^{a_k}.$$

I claim that no π_j equals $\pm\overline{\pi}_k$. If this happened then $\pi_j \mid (y + \sqrt{-2})$ and $\pi_j \mid (y - \sqrt{-2})$. Thus π_j would be a factor of $(y + \sqrt{-2}) - (y - \sqrt{-2}) = 2\sqrt{-2}$. But as $\pi_j \mid (y + \sqrt{-2})$ then $N(\pi_j) \mid N(y + \sqrt{-2}) = y^2 + 2$, which is odd, and as $\pi_j \mid 2\sqrt{-2}$ then $N(\pi_j) \mid N(2\sqrt{-2}) = 8$. Hence $N(\pi_j) = 1$, which means that π_j is a unit, and not an irreducible.

Since x^3 is a cube, when we write it as a power of irreducibles, the exponent of each is a multiple of 3. From unique factorization then each a_j is divisible by 3. Consequently from (‡), $y + \sqrt{-2} = \pm\beta^3 = (\pm\beta)^3$ where $\beta \in \mathcal{O}_K$. Write $\pm\beta = a + b\sqrt{-2}$ with a, $b \in \mathbf{Z}$. Then

$$y + \sqrt{-2} = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}$$

and so $y = a(a^2 - 6b^2)$ and $1 = b(3a^2 - 2b^2)$. Hence $b = \pm 1$ and $\pm 1 = 3a^2 - 2b^2 = 3a^2 - 2$. This can only happen when $3a^2 = 3$ and $a = \pm 1$. Then $y = \pm(-5) = \pm 5$. Thus $x^3 = 27$ and $x = 3$. We conclude that the only integer solutions of $(*)$ are $(x, y) = (5, 3)$ and $(x, y) = (-5, 3)$.

4 Ideals

Recall that an *ideal* of a (commutative) ring R is a subset I of R such that

- I is a subgroup of R (under the operation of addition),
- if $a \in I$ and $x \in R$ then $xa \in I$.

A *principal ideal* is one of the form

$$\langle a \rangle = \{xa : x \in R\}$$

for some $a \in R$. The trivial cases are $\langle 0 \rangle = \{0\}$ and $\langle 1 \rangle = R$. All other ideals of R are called *nontrivial*.

Let I and J be ideals of R. It is easy to see that their *sum* $I + J = \{a + b : a \in I, b \in J\}$ is an ideal of R. The sum of I and J is the smallest ideal containing both I and J. It is even easier to see that their intersection $I \cap J$ is an ideal of R. Ideals can be multiplied, but this is more difficult. If I and J are ideals of R then the set $\{ab : a \in I, b \in J\}$ is not in general an ideal of R (although if one if I and J is principal it is). The problem is that the sum $a_1b_1 + a_2b_2$ where a_1, $a_2 \in I$ and b_1, $b_2 \in J$ may not be expressible as ab for $a \in I$ and $n \in J$. However the additive group generated by the elements ab for $a \in I$, $b \in J$ is an ideal of R, and we call this ideal the product IJ of I and J. Symbolically

$$IJ = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n : a_1, \ldots, a_n \in I,\, b_1, \ldots, b_n \in J\}.$$

The product IJ is the smallest ideal containing all ab with $a \in I$ and $b \in J$.

The sum and product satisfy a number of formal properties:

- $I + I = I$ when I is an ideal of R,

- $I + J = J + I$ when I and J are ideals of R,
- $I_1 + (I_2 + I_3) = (I_1 + I_2) + I_3$ when I_1, I_2 and I_3 are ideals of R,
- $IJ \subseteq I \cap J$ when I and J are ideals of R,
- $IJ = JI$ when I and J are ideals of R,
- $I_1(I_2I_3) = (I_1I_2)I_3$ when I_1, I_2 and I_3 are ideals of R, and
- $I(J_1 + J_2) = IJ_1 + IJ_2$ when I, J_1 and J_2 are ideals of R.

We abbreviate the sum of a number of principal ideals as follows:

$$\langle a_1, a_2, \ldots, a_r \rangle = \langle a_1 \rangle + \langle a_2 \rangle + \cdots + \langle a_r \rangle .$$

Then $\langle a_1, a_2, \ldots, a_r \rangle$ is the smallest ideal containing each of the a_j. An ideal of this form is called *finitely generated*. By using the above properties of the ideal sum and product we find that

$$\langle a_1, a_2, \ldots, a_r \rangle + \langle b_1, b_2, \ldots, b_s \rangle = \langle a_1, a_2, \ldots, a_r, b_1, b_2, \ldots, b_s \rangle$$

and

$$\langle a_1, a_2, \ldots, a_r \rangle \langle b_1, b_2, \ldots, b_s \rangle = \langle a_1b_1, a_1b_2, \ldots, a_1b_s, a_2b_1, a_2b_2, \ldots, a_rb_s \rangle .$$

We now turn to the ideal theory of $\mathcal{O}_K$ for number fields K. Two elements of $\mathcal{O}_K$ generate the same principal ideal when they differ by a unit factor.

Lemma 4.1 *Let β and γ be nonzero elements of $\mathcal{O}_K$ where K is a number field. Then $\langle \beta \rangle = \langle \gamma \rangle$ if and only if γ/β is a unit in $\mathcal{O}_K$.*

Proof If $\langle \beta \rangle = \langle \gamma \rangle$ then $\beta \in \langle \gamma \rangle$ and $\gamma \in \langle \beta \rangle$. Hence $\gamma/\beta \in \mathcal{O}_K$ and $\beta/\gamma \in \mathcal{O}_K$ and so $\gamma/\beta \in U(\mathcal{O}_K)$.

Conversely if $\gamma/\beta \in U(\mathcal{O}_K)$ then β/γ, $\gamma/\beta \in \mathcal{O}_K$ and so $\beta \mid \gamma$ and $\gamma \mid \beta$. Hence $\langle \beta \rangle \subseteq \langle \gamma \rangle \subseteq \langle \beta \rangle$ so that $\langle \beta \rangle = \langle \gamma \rangle$. □

The concepts of divisibility and primality in $\mathcal{O}_K$ can be expressed in terms of ideals. For instance $\beta \mid \gamma$ if and only if $\gamma \in \langle \beta \rangle$ which occurs if and only if $\langle \gamma \rangle \mid \langle \beta \rangle$. Similarly $\gamma \equiv \delta \pmod{\beta}$ if and only if $\gamma - \delta \in \langle \beta \rangle$. We can generalize the notion of congruences modulo an element to congruences modulo an ideal; if I is an ideal then we write $\gamma \equiv \delta \pmod{I}$ whenever $\gamma - \delta \in I$. Hence $\gamma \equiv \delta \pmod{\langle \beta \rangle}$ means the same as $\gamma \equiv \delta \pmod{\beta}$. The relation of congruence modulo an ideal has the same formal properties as congruence modulo an element, which I shall not list.

The condition for β to be a prime element of $\mathcal{O}_K$ becomes the following:

- $\langle\beta\rangle \neq \langle 0\rangle$,
- $\langle\beta\rangle \neq \langle 1\rangle$, and
- if γ, $\delta \in \mathcal{O}_K$ and $\gamma\delta \in \langle\beta\rangle$ then either $\gamma \in \langle\beta\rangle$ or $\delta \in \langle\beta\rangle$.

Note that here β only enters through the ideal $\langle\beta\rangle$. We say that an ideal P of $\mathcal{O}_K$ is *prime* if

- $P \neq \langle 0\rangle$,
- $P \neq \langle 1\rangle$, and
- if γ, $\delta \in \mathcal{O}_K$ and $\gamma\delta \in P$ then either $\gamma \in P$ or $\delta \in P$.

Thus the principal prime ideals are those of the form $\langle\beta\rangle$ with β prime. When every ideal of $\mathcal{O}_K$ is principal then every irreducible element of $\mathcal{O}_K$ is prime by Proposition 3.2. But then factorizations into irreducibles are always unique up to equivalence by Proposition 3.1. We can put these results together and rephrase in the language of ideals.

Proposition 4.1 *Let K be a number field, and suppose that each ideal of $\mathcal{O}_K$ is principal. Each nontrivial ideal of $\mathcal{O}_K$ is a product of prime ideals and all such expressions are unique up to the order of the factors.*

Proof Each nontrivial ideal I has the form $I = \langle\beta\rangle$ where $\beta \neq 0$ and $\beta \notin U(\mathcal{O}_K)$. Then by Lemma 3.3, $\beta = \gamma_1\gamma_2\cdots,\gamma_r$ where the γ_j are irreducible. Then $I = \langle\gamma_1\rangle\langle\gamma_2\rangle\cdots\langle\gamma_r\rangle$ and by Proposition 3.2 the γ_j are primes. But then the $\langle\gamma_j\rangle$ are prime ideals so that I is a product of prime ideals.

Let

$$I = P_1P_2\cdots P_r = Q_1Q_2\cdots Q_s \qquad (*)$$

be two factorizations of I into prime ideals. Write $P_i = \langle\gamma_i\rangle$ and $Q_j = \langle\delta_j\rangle$. Then β, $\gamma_1\gamma_2\cdots\gamma_r$ and $\delta_1\delta_2\cdots\delta_s$ differ only by unit factors. By absorbing these into γ_1 and δ_1 we may assume that

$$\beta = \gamma_1\gamma_2\cdots\gamma_r = \delta_1\delta_2\cdots\delta_s.$$

By Proposition 3.1, these factorizations are equivalent which means that in $(*)$, $r = s$ and the P_i and Q_j are the same up to order. □

But not every K has the property that each ideal of $\mathcal{O}_K$ is principal. Remarkably, Proposition 4.1 is still valid for these fields, although the proof is harder. The unique factorization property for prime ideals compensates in part for the failure of unique factorization into irreducible elements. It is time to see some examples of nonprincipal ideals.

Example Let $K = \mathbf{Q}(\sqrt{-6})$. Then $\mathcal{O}_K = \{a + b\sqrt{-6}\}$. We define two subsets of $\mathcal{O}_K$ which will turn out to be nonprincipal ideals. Let

$$I = \{a + b\sqrt{-6} : a, b \in \mathbf{Z},\ a \text{ is even}\} = \{2c + b\sqrt{-6} : b, c \in \mathbf{Z}\}$$

and

$$J = \{a + b\sqrt{-6} : a, b \in \mathbf{Z}, 3 \mid a\} = \{3c + b\sqrt{-6} : b, c \in \mathbf{Z}\}.$$

It is easy to see that I and J are subgroups of $\mathcal{O}_K$ under addition. Suppose $\beta = 2c + b\sqrt{-6} \in I$ and $\gamma = r + s\sqrt{-6} \in \mathcal{O}_K$. Then

$$\gamma\beta = (r + s\sqrt{-6})(2c + b\sqrt{-6}) = 2(rs - 3sb) + (rb + 2sc)\sqrt{-6} \in I$$

and so I is an ideal of $\mathcal{O}_K$. A similar argument shows that J is an ideal of $\mathcal{O}_K$. In fact I claim that $I = \left\langle 2, \sqrt{-6}\right\rangle$. Certainly $2 \in I$ and $\sqrt{-6} \in I$ so that $\left\langle 2, \sqrt{-6}\right\rangle \subseteq I$. On the other hand each element of I has the form $2c + b\sqrt{-6}$ for b, $c \in \mathbf{Z}$. *A fortiori* each element of I has the form $2\gamma + \delta\sqrt{-6}$ with γ, $\delta \in \mathcal{O}_K$ and so $I \subseteq \left\langle 2, \sqrt{-6}\right\rangle$. Indeed then, $I = \left\langle 2, \sqrt{-6}\right\rangle$. Similarly $J = \left\langle 3, \sqrt{-6}\right\rangle$.

We now show that I and J are nonprincipal. Suppose that I were principal. Then $I = \langle\beta\rangle$ for some $\beta \in \mathcal{O}_K$. Then as $2 \in I$ and $\sqrt{-6} \in I$, $\beta \mid 2$ and $\beta \mid \sqrt{-6}$. Hence $N(\beta) \mid N(2) = 4$ and $N(\beta) \mid N(\sqrt{-6}) = 6$. It follows that $N(\beta) = \pm 1$ or ± 2. But $N(\beta) = a^2 + 6b^2$ where $\beta = a + b\sqrt{-6}$ and a, $b \in \mathbf{Z}$. The only possibility is $a = \pm 1$ and $b = 0$. But then $\beta = \pm 1$ and $\pm 1 \notin I$ so this is false. Hence I is nonprincipal. A similar argument shows that J is also nonprincipal.

We shall compute the products of I and J. First of all consider I^2. We have

$$I^2 = \left\langle 2, \sqrt{-6}\right\rangle \left\langle 2, \sqrt{-6}\right\rangle = \left\langle 4, 2\sqrt{-6}, 2\sqrt{-6}, -6\right\rangle.$$

By inspection we see that 4, -6 and $2\sqrt{-6}$ are all elements of $\langle 2\rangle$ so that $I^2 \subseteq \langle 2\rangle$. But $2 = (-1)4 - (-1)(-6) \in I^2$. Hence $\langle 2\rangle \subseteq I^2$ and we conclude that $I^2 = \langle 2\rangle$. Similarly $J^2 = \langle 3\rangle$. Now consider IJ. We have

$$IJ = \left\langle 2, \sqrt{-6}\right\rangle \left\langle 3, \sqrt{-6}\right\rangle = \left\langle 6, 2\sqrt{-6}, 3\sqrt{-6}, -6\right\rangle.$$

As $\sqrt{-6} \mid \pm 6$ in $\mathcal{O}_K$ we see that $IJ \subseteq \left\langle \sqrt{-6}\right\rangle$. But $\sqrt{-6} = 3\sqrt{-6} + (-1)2\sqrt{-6} \in IJ$ and so $\left\langle \sqrt{-6}\right\rangle \subseteq IJ$. Hence $IJ = \left\langle \sqrt{-6}\right\rangle$.

We now show that I and J are prime ideals. Let $\beta = a + b\sqrt{-6}$, $\gamma = c + d\sqrt{-6} \in \mathcal{O}_K$ and suppose that $\beta \notin I$ and $\gamma \notin I$. Then a and c are odd. Thus $\beta\gamma = (ac - 6bd) + (ad + bd)\sqrt{-6}$. But $ac - 6cd$ is odd so $\beta\gamma \notin I$. Hence I is prime. Now suppose that $\beta \notin J$ and $\gamma \notin J$. Then $3 \nmid a$ and $3 \nmid c$. But then $3 \nmid (ac - 6bd)$ so that $\beta\gamma \notin J$. Hence J is prime.

We have already seen the example

$$6 = 2 \times 3 = (\sqrt{-6})(-\sqrt{-6})$$

of nonunique factorization into irreducibles in $\mathcal{O}_K$. This gives the ideal factorization

$$\langle 6 \rangle = \langle 2 \rangle \langle 3 \rangle = \left\langle \sqrt{-6} \right\rangle^2. \qquad (*)$$

But none of $\langle 2 \rangle$, $\langle 3 \rangle$ and $\left\langle \sqrt{-6} \right\rangle$ is "irreducible" as an ideal. The factorization $(*)$ can be rewritten as

$$(I^2)(J^2) = (IJ)(IJ)$$

and is now seen to be exhibit two ways of regrouping the nonprincipal prime ideals in the factorization $\langle 6 \rangle = I^2 J^2$ into pairs multiplying to principal ideals.

We need a technical result about ideals in $\mathcal{O}_K$.

Lemma 4.2 *Let K be a number field of degree n. Each nonzero ideal of $\mathcal{O}_K$ is a free abelian group of rank n under the operation of addition.*

Proof Let I be a nonzero ideal of $\mathcal{O}_K$. Let $\beta_1, \beta_2, \ldots, \beta_n$ form an integral basis of $\mathcal{O}_K$ and let γ be a nonzero element of I. Then it is plain that $\gamma\beta_1, \gamma\beta_2, \ldots, \gamma\beta_n$ form an integral basis of $\langle \gamma \rangle$. Hence $\langle \gamma \rangle$ is free abelian of rank m. Since I is a subgroup of $\mathcal{O}_K$ then by Proposition A.3, I is free abelian of rank m where $m \leq n$. But $\langle \gamma \rangle$ is a subgroup of I and so the rank of $\langle \gamma \rangle$, that is n, does not exceed m. Hence $n \leq m \leq n$ so that $m = n$. $\square$

Let K be a number field. Each nonzero ideal of $\mathcal{O}_K$ has the same rank as an abelian group as $\mathcal{O}_K$. By Proposition A.4 each ideal I has finite index as a subgroup of $\mathcal{O}_K$. We call this index the *norm* of I, and denote it as $N(I)$. That is, $N(I) = |\mathcal{O}_K : I|$. What this means is that if $N(I) = m$, then there are $\gamma_1, \ldots, \gamma_m \in \mathcal{O}_K$ which form a *system of coset representatives* for I in $\mathcal{O}_K$. That is, each $\beta \in \mathcal{O}_K$ is congruent to exactly one γ_j modulo I.

Example Let $K = \mathbf{Q}(\sqrt{-6})$ so that $\mathcal{O}_K = \mathbf{Z}[\sqrt{-6}]$. Consider the principal ideal $\left\langle 1 + \sqrt{-6} \right\rangle$. Let $\beta = 1 + \sqrt{-6}$. Then $\gamma \in \langle \beta \rangle$ if and only if $\gamma/\beta \in \mathbf{Z}[\sqrt{-6}]$. If $\gamma = a + b\sqrt{-6}$ then

$$\frac{\gamma}{\beta} = \frac{a + b\sqrt{-6}}{1 + \sqrt{-6}} = \frac{(a + b\sqrt{-6})(1 - \sqrt{-6})}{(1 + \sqrt{-6})(1 - \sqrt{-6})} = \frac{a + 6b}{7} + \frac{b - a}{7}\sqrt{-6}.$$

Thus $\gamma \in \langle \beta \rangle$ if and only if $a + 6b \equiv 0 \pmod 7$ and $b - a \equiv 0 \pmod 7$. Both conditions are equivalent to $a \equiv b \pmod 7$. Consequently $a + b\sqrt{-6} \equiv c + d\sqrt{-6} \pmod{\langle \beta \rangle}$ if and only if $b - a \equiv d - c \pmod 7$. Hence 0, 1, 2,

3, 4, 5, 6 form a system of coset representatives for $\langle\beta\rangle$ in $\mathbf{Z}[\sqrt{-6}]$ and so $N(\langle 1+\sqrt{-6}\rangle) = 7$.

Example Again let $K = \mathbf{Q}(\sqrt{-6})$, and consider the nonprincipal ideal $I = \langle 2, \sqrt{-6}\rangle$. We have seen that $a + b\sqrt{-6} \in I$ if and only if a is even. Hence $a + b\sqrt{-6} \equiv c + d\sqrt{-6} \pmod{I}$ if and only if $a \equiv c \pmod 2$. Hence 0 and 1 form a system of coset representatives for I in $\mathbf{Z}[\sqrt{-6}]$ and so $N(I) = 2$. A similar argument gives $N(J) = 3$ when $J = \langle 3, \sqrt{-6}\rangle$.

We list some formal properties of the norm. Let I and J be nonzero ideals of $\mathcal{O}_K$.

- $N(I)$ is a positive integer, and $N(I) = 1$ only when $I = \langle 1\rangle = \mathcal{O}_K$,
- if $I \subseteq J$ then $N(J) \mid N(I)$ with equality only when $I = J$; *a fortiori* $N(J) < N(I)$ with equality only when $I = J$.

The latter of these is because $|\mathcal{O}_K : I| = |\mathcal{O}_K : J||J : I|$.

So far we have two notions of norm. The norm of an element of K, and the form of a nonzero ideal of $\mathcal{O}_K$. As one might expect these notions are linked.

Theorem 4.1 *Let K be a number field. If γ is a nonzero element of $\mathcal{O}_K$ then*

$$N(\langle\gamma\rangle) = |N(\gamma)|. \qquad (*)$$

(Note that on the left of $(*)$ we have the norm of an ideal, and on the right we have the norm of an element.)

Proof Let $\beta_1, \ldots, \beta_n$ form an integral basis of $\mathcal{O}_K$. Then $\gamma\beta_1, \ldots, \gamma\beta_n$ forms an integral basis of $\langle\gamma\rangle$. We can write $\gamma\beta_j = \sum_{j=1}^n a_{jk}\beta_k$ where the $a_{jk} \in \mathbf{Z}$. By Proposition A.4, $N(\langle\gamma\rangle) = |\mathcal{O}_K : \langle\gamma\rangle\,| = |\det(A)|$ where A is the n-by-n matrix with (j,k)-entry a_{jk}. It suffices to show that $\det(A) = N(\gamma)$.

We have the matrix equation $\gamma\mathbf{v} = A\mathbf{v}$ where $\mathbf{v}$ is the column vector $(\beta_1\ \beta_2\ \cdots\ \beta_n)^\top$. Applying the homomorphism σ_k to this equation gives $\sigma_k(\gamma)\mathbf{v}_k = A\mathbf{v}_k$ where $\mathbf{v}_k = (\sigma_k(\beta_1)\ \sigma_k(\beta_2)\ \cdots\ \sigma_k(\beta_n))^\top$. Thus the $\mathbf{v}_k$ are eigenvectors of A with eigenvalues $\sigma_k(\gamma)$. The n-by-n matrix B with columns the $\mathbf{v}_k$ has (j,k)-entry $\sigma_k(\beta_j)$. Then $BB^\top$ has (j,k)-entry $\sum_{i=1}^n \sigma_i(\beta_j)\sigma_i(\beta_k) = T(\beta_j\beta_k)$ and so $\det(BB^\top) = \Delta(\beta_1, \ldots, \beta_n) \neq 0$. Hence B is nonsingular. But then BAB^{-1} is a diagonal matrix with entries $\sigma_j(\gamma)$ and so $\det(A) = \det(BAB^{-1}) = \prod_{j=1}^n \sigma_j(\gamma) = N(\gamma)$. □

A similar argument shows that $N(\langle\gamma\rangle\, I) = |N(\gamma)|N(I)$. Later we shall show that $N(IJ) = N(I)N(J)$ is general, but our proof will be very indirect.

Our aim is to show that each nontrivial ideal of $\mathcal{O}_K$ can be uniquely represented as a product of prime ideals. We need many preliminary results alas. By definition if P is a prime ideal, β, $\gamma \in \mathcal{O}_K$ and $\beta\gamma \in P$, then either $\beta \in P$ or $\gamma \in P$. Equivalently if $\langle\beta\rangle\langle\gamma\rangle = \langle\beta\gamma\rangle \subseteq P$ then either $\langle\beta\rangle \subseteq P$ or $\langle\gamma\rangle \subseteq P$. This can be extended to nonprincipal ideals.

Lemma 4.3 *Let K be a number field and let P be a prime ideal of $\mathcal{O}_K$. If I and J are ideals of $\mathcal{O}_K$ and $IJ \subseteq P$ then either $I \subseteq P$ or $J \subseteq P$.*

More generally if $I_1, \ldots, I_m$ are ideals and $I_1 \cdots I_m \subseteq P$ then $I_k \subseteq J$ for some k.

Proof Suppose, for a contradiction, that $IJ \subseteq P$ but $I \not\subseteq P$ and $J \not\subseteq P$. Then there exist $\beta \in I$, $\gamma \in J$ with $\beta \notin P$ and $\gamma \notin P$. But then $\beta\gamma \in IJ$, but $\beta\gamma \notin P$, since P is prime, contradicting the hypothesis $IJ \subseteq P$.

The case of an m-term product $I_1 \cdots I_m$ now follows by induction. □

Primality is also equivalent to maximality. An ideal I of $\mathcal{O}_K$ is *maximal* if I is nontrivial but the only ideals J of $\mathcal{O}_K$ with $I \subseteq J$ are $J = I$ and $J = \mathcal{O}_K$.

Lemma 4.4 *Let K be a number field. An ideal I of $\mathcal{O}_K$ is prime if and only if it is maximal.*

Proof First suppose that I is maximal. Let β, $\gamma \in \mathcal{O}_K$ with $\beta\gamma \in I$ and $\beta \notin I$. To show that I is prime it suffices to show that $\gamma \in I$. Let $J = I + \langle\beta\rangle$. Then J is an ideal and $I \subseteq J$, but $I \neq J$ since $\beta \in J$. By maximality of I, $J = \mathcal{O}_K$. Hence $1 \in J$ so $1 = \eta + \delta\beta$ where $\eta \in I$ and $\delta \in \mathcal{O}_K$. Then $1 \equiv \delta\beta \pmod{I}$. Consequently, $\gamma = 1\gamma \equiv \delta\beta\gamma \equiv 0 \pmod{I}$, as $\beta\gamma \in I$. We conclude that $\gamma \in I$ and that I is prime.

Conversely suppose that I is prime. Suppose that J is an ideal of $\mathcal{O}_K$ with $I \subseteq J$ and $I \neq J$. We need to show that $J = \mathcal{O}_K$, or equivalently, that $1 \in \mathcal{O}_K$. Let $\beta \in J$ and $\beta \notin I$. Then $J \supseteq I + \langle\beta\rangle$ so all we need to do is to show that $1 \in I + \langle\beta\rangle$. The ideal I has finite index, m say, in $\mathcal{O}_K$. Let $\gamma_1, \ldots, \gamma_m$ be coset representatives for I in $\mathcal{O}_K$. That is to say that each element of $\mathcal{O}_K$ is congruent modulo I to exactly one γ_j. In particular $\gamma_j \equiv \gamma_k \pmod{I}$ if and only if $j = k$. If $\beta\gamma_j \equiv \beta\gamma_k \pmod{I}$ then $\beta(\gamma_j - \gamma_k) \in I$ and as I is prime and $\beta \notin I$ then $\gamma_j - \gamma_k \in I$ and so $j = k$. The numbers $\beta\gamma_1, \ldots, \beta\gamma_m$ lie in distinct cosets of I, and so they represent all cosets. In particular $1 \equiv \beta\gamma_j \pmod{I}$ for some j, and so $1 = \eta + \gamma_j\beta$ for some $\eta \in I$. Thus $1 \in I + \langle\beta\rangle$ and I is maximal. □

As an immediate consequence, if P and Q are prime ideals of $\mathcal{O}_K$ and $P \subseteq Q$ then $P = Q$ due to the maximality of P.

Due to maximality being the same as primality, every nontrivial ideal is contained in a prime ideal.

Lemma 4.5 *Let K be a number field, and let I be a nontrivial ideal of $\mathcal{O}_K$. Then there is a prime ideal P of $\mathcal{O}_K$ with $I \subseteq P$.*

Proof Consider the nontrivial ideals J of $\mathcal{O}_K$ with $I \subseteq J$. There is certainly at least one namely I itself. Take one, P, with least possible norm. Then P is maximal, for if $P \subseteq J_1$ with $J_1 \neq P$ an ideal of $\mathcal{O}_K$, then $N(J_1) < N(P)$ and so $J_1 = \mathcal{O}_K$. □

We would like to show that each nontrivial ideal is a product of prime ideals. We cannot do so yet, but we can prove a first approximation to this result.

Lemma 4.6 *Let K be a number field, and let I be a nontrivial ideal of $\mathcal{O}_K$. Then $I \supseteq P_1 P_2 \cdots P_m$ where the P_j are prime ideals of $\mathcal{O}_K$.*

Proof We use induction on $N(I)$. If I is prime, then we can take $m = 1$ and $P_1 = I$. If I is not prime, then there exist β, $\gamma \in \mathcal{O}_K$ with $\beta \notin I$, $\gamma \notin I$ but $\beta\gamma \in I$. Let $J_1 = \langle \beta \rangle + I$ and $J_2 = \langle \gamma \rangle + I$. Then $I \subseteq J_1$ and $I \subseteq J_2$, but $I \neq J_1$ and $I \neq J_2$. Hence $N(J_1) < N(I)$ and $N(J_2) < N(I)$. But $J_1 J_2 = \langle \beta\gamma \rangle + \beta I + \gamma I + I^2 \subseteq I$ as $\beta\gamma \in I$. By the inductive hypothesis, $J_1 \supseteq P_1 \cdots P_r$ and $J_2 \supseteq Q_1 \cdots Q_s$ where the P_j and Q_k are prime. Hence $I \supseteq J_1 J_2 \supseteq P_1 \cdots P_r Q_1 \cdots Q_s$ as required. □

As a technical convenience we extend the notion of ideals in $\mathcal{O}_K$ to that of fractional ideal. It will turn out that the set of fractional ideals forms a group under multiplication, which it is clear that the set of ideals do not.

A *fractional ideal* of K is a set of the form βI where β is a nonzero element of K and I is a nonzero ideal of $\mathcal{O}_K$. Note that we do not assume that $\beta \in \mathcal{O}_K$. In particular $\beta\mathcal{O}_K = \langle \beta \rangle$ is a fractional ideal of K for all nonzero $\beta \in K$. We call such a fractional ideal *principal*. If all ideals of $\mathcal{O}_K$ are principal, for instance if $K = \mathbf{Q}$, then so are all fractional ideals, for the fractional ideal $\beta I = \langle \beta\gamma \rangle$ if $I = \langle \gamma \rangle$. We define the sum and product of fractional ideals in the same way as for ideals. In particular if $\beta \in K$, $\beta \neq 0$ then $\langle \beta \rangle \langle 1/\beta \rangle = \langle 1 \rangle = \mathcal{O}_K$, so that principal fractional ideals are invertible. We shall show that all fractional ideals are invertible.

We start with an alternative characterization of fractional ideals.

Lemma 4.7 *Let K be a number field. Then I is a fractional ideal of K if and only if*

- *I is a nonzero subgroup of K under addition,*

- *if $\beta \in I$ and $\gamma \in \mathcal{O}_K$ then $\gamma\beta \in I$, and*
- *there is a nonzero $\eta \in K$ such that $\beta/\eta \in \mathcal{O}_K$ for each $\beta \in I$.*

Proof If $I = \eta J$ is a fractional ideal of K, with $\eta \in K$ and J an ideal of $\mathcal{O}_K$, then the three properties follow with the same value of η.

Conversely suppose the three properties hold. Then $J = \eta^{-1}I = \{\beta/\eta : \beta \in I\}$ is a nonzero ideal of $\mathcal{O}_K$ and so $I = \eta J$ is a fractional ideal. □

We shall show that all fractional ideals are *invertible*, that is given a fractional ideal I, there is a fractional ideal J with $IJ = \langle 1 \rangle$. It is easy to write down a candidate for the inverse of a fractional ideal I; define $I^* = \{\beta \in K : \beta I \subseteq \mathcal{O}_K\}$. It is clear that I^* is an additive subgroup of K and is nonzero since it contains $1/\eta$ whenever $I = \eta J$ with J an ideal of $\mathcal{O}_K$. Also it is clear that if $\beta \in I^*$ and $\gamma \in \mathcal{O}_K$ then $\beta\gamma \in I^*$. If δ is a nonzero element of I then $\delta I^* \subseteq \mathcal{O}_K$ and so $(1/\delta)I^* \subseteq \mathcal{O}_K$. Thus I^* is a fractional ideal of K. Also $II^* \subseteq \mathcal{O}_K$ so that II^* is an ideal of $\mathcal{O}_K$. The hard part is to show that $II^* = \mathcal{O}_K$.

We first prove the invertibility for prime ideals. Let P be a prime ideal of $\mathcal{O}_K$. Then $P^* \supseteq \mathcal{O}_K$ since $\beta P \subseteq P$ for all $\beta \in \mathcal{O}_K$. Thus $PP^* \supseteq P\mathcal{O}_K = P$. But $PP^* \subseteq \mathcal{O}_K$. By the maximality of P, either $PP^* = \mathcal{O}_K$ (as we want) or $PP^* = P$. We dispose of the possibility that $PP^* = P$ in two stages: first we show that $PP^* = P$ implies that $P^* = \mathcal{O}_K$, then we show that $P^* \neq \mathcal{O}_K$.

Lemma 4.8 *Let K be a number field and let I be a nonzero ideal of $\mathcal{O}_K$. If $\gamma I \subseteq I$ for some $I \in K$, then $\gamma \in \mathcal{O}_K$.*

Proof By Lemma 4.2, I is a free abelian group, so let $\beta_1, \ldots, \beta_n$ form an integral basis of I. Then $\gamma\beta_j \in I$ for all j, so $\gamma\beta_j = \sum_{k=1}^{n} a_{jk}\beta_k$ where the $a_{jk} \in \mathbf{Z}$. Thus $\gamma\mathbf{v} = A\mathbf{v}$ where $\mathbf{v}$ is the column vector with entries the β_j and A is the matrix with entries the a_{jk}. Thus γ is an eigenvalue of A which is a matrix with integer entries. Thus γ is an algebraic integer and so $\gamma \in K \cap \mathbf{B} = \mathcal{O}_K$. □

We now show that prime ideals are invertible.

Proposition 4.2 *Let K be a number field and let P be a prime ideal of $\mathcal{O}_K$. Then there is a fractional ideal J of K with $PJ = \langle 1 \rangle$.*

Proof We let $P^* = \{\beta \in K : \beta P \subseteq \mathcal{O}_K\}$. Then P^* is a fractional ideal of K, $\mathcal{O}_K \subseteq P^*$ and $P \subseteq PP^* \subseteq \mathcal{O}_K$. By the maximality of the prime ideal P, either $PP^* = P$ or $PP^* = \mathcal{O}_K$. We show that the latter is true, so to obtain a contradiction, suppose that $PP^* = P$.

Then $\gamma \in P^*$ implies that $\gamma P \subseteq P$ and so $\gamma \in \mathcal{O}_K$ by Lemma 4.8. Hence $P^* \subseteq \mathcal{O}_K$ and we conclude that $P^* = \mathcal{O}_K$. To obtain the desired contradiction, it suffices to find an element in P^* but not in $\mathcal{O}_K$.

Let β be a nonzero element of P. Then by Lemma 4.6, $\langle\beta\rangle$ contains a product $P_1P_2\cdots P_r$ of prime ideals. Choose such a product with fewest possible factors. Then $P \supseteq \langle\beta\rangle \supseteq P_1P_2\cdots P_r$ and so $P \supseteq P_j$ for some j by Lemma 4.3. We shall assume, without loss of generality, that $P \supseteq P_1$. Then by maximality of the prime ideal P_1, $P = P_1$. Thus $\langle\beta\rangle \supseteq PI$ where $I = P_2\cdots P_r$. As r was chosen to be minimal then $\langle\beta\rangle \not\supseteq I$. Thus there exists $\gamma \in I$ but $\gamma \notin \langle\beta\rangle$. Hence $\delta = \gamma/\beta \notin \mathcal{O}_K$. But $\gamma P \subseteq PI \subseteq \langle\beta\rangle$ and so $\delta P = \beta^{-1}\gamma P \subseteq \mathcal{O}_K$. Hence $\delta \in P^*$. But as $\gamma \notin \langle\beta\rangle$ then $\delta \notin \mathcal{O}_K$.

The assumption that $P^* = \mathcal{O}_K$ has led to a contradiction. We cannot then have $PP^* = P$ and we conclude that $PP^* = \mathcal{O}_K = \langle 1\rangle$ as required. □

The inverse of a prime ideal P is uniquely determined, for if $PJ = \mathcal{O}_K$ then $J = JPP^* = P^*$. We can now show that every nontrivial ideal is a product of prime ideals.

Theorem 4.2 *Let K be a number field, and suppose that I is a nontrivial ideal of $\mathcal{O}_K$. Then $I = P_1P_2\cdots P_m$ where the P_j are prime ideals.*

Proof We use induction on $N(I)$. There is nothing to prove when I is prime so assume that it is not. By Lemma 4.5 $I \subseteq P$ for some prime ideal P. Let P^{-1} be the inverse of P as a fractional ideal. As $P \subseteq \mathcal{O}_K$ then $\mathcal{O}_K = PP^{-1} \subseteq \mathcal{O}_KP^{-1} = P^{-1}$. Let $J = IP^{-1}$. As $I \subseteq P$ then $J \subseteq PP^{-1} = \mathcal{O}_K$ and J is an ideal of $\mathcal{O}_K$. Also $I = PJ$. Thus J is a proper ideal of $\mathcal{O}_K$.

We know $P^{-1} \supseteq \mathcal{O}_K$ but $P^{-1} \not\subseteq \mathcal{O}_K$ for otherwise P^{-1} would be $\mathcal{O}_K$ which is not an inverse of P. Thus $J = IP^{-1} \supseteq I\mathcal{O}_K = I$. If we had $J = I$ then $\gamma I \subseteq I$ for all $\gamma \in P^{-1}$ and so $P^{-1} \subseteq \mathcal{O}_K$ by Lemma 4.8. This contradicts $P^{-1} \not\subseteq \mathcal{O}_K$. Hence $I \subseteq J$ but $I \neq J$ and so $N(J) < N(I)$. By the inductive hypothesis J is a product of primes, and so $I = PJ$ is also. □

We can conclude that every fractional ideal is invertible.

Proposition 4.3 *Let K be a number field, and let I be a fractional ideal of K. Then I is invertible.*

Proof Write $I = \beta J$ where $\beta \neq 0$ and J is an ideal of $\mathcal{O}_K$. By Theorem 4.2 $J = P_1P_2\cdots P_r$ where the P_j are prime, and by Lemma 4.5, each P_j is invertible with inverse P_j^{-1} say. Then the fractional ideal $\beta^{-1}P_1^{-1}P_2^{-1}\cdots P_j^{-1}$ is an inverse of I. □

It is now plain that the fractional ideals of K form a group under multiplication and the principal fractional ideals form a subgroup. One useful consequence is that ideals satisfy the maxim, "to contain is to divide".

Proposition 4.4 *Let K be a number field, and let I_1, I_2 be nonzero ideals of $\mathcal{O}_K$. Then $I_1 \supseteq I_2$ if and only if there is an ideal J of $\mathcal{O}_K$ with $I_2 = I_1 J$.*

Proof If $I_2 = I_1 J$ for an ideal J then $I_2 \subseteq I_1$. Conversely suppose that $I_1 \supseteq I_2$. Then $\mathcal{O}_K = I_1 I_1^{-1} \supseteq I_2 I_1^{-1} = J$ say. Then J is an ideal of $\mathcal{O}_K$ and $I_1 J = I_1 I_2 I^{-1} = I_2$. □

After all this hard work it is now easy to conclude that factorizations into prime ideals are unique.

Theorem 4.3 *Let K be a number field, and suppose that I is a nontrivial ideal of $\mathcal{O}_K$. If*

$$I = P_1 P_2 \cdots P_r = Q_1 Q_2 \cdots Q_s \qquad (*)$$

where the P_j and Q_k are prime ideals of $\mathcal{O}_K$, then $r = s$ and the Q_k can be reordered so that $P_j = Q_j$ for each j.

Proof We use induction on r. Certainly $P_1 \supseteq I = Q_1 Q_2 \cdots Q_s$. By Lemma 4.3, $P_1 \supseteq Q_k$ for some k. We reorder the Q_j so that $P_1 \supseteq Q_1$. By maximality of Q_1 then $P_1 = Q_1$. Multiplying $(*)$ by P_1^{-1} gives

$$P_2 \cdots P_r = Q_2 \cdots Q_s$$

and the result now follows from the inductive hypothesis. □

We can also repair an earlier omission; we can show that the ideal norm is multiplicative.

Proposition 4.5 *Let K be a number field, and let I and J be nonzero ideals of $\mathcal{O}_K$. Then $N(IJ) = N(I)N(J)$.*

Proof If $I = \mathcal{O}_K$ there is nothing to prove, so we can write I as a product of prime ideals. Using induction on the number of prime ideals it plainly suffices to prove the result in the special case where $I = P$ is a prime ideal.

By definition $N(P) = |\mathcal{O}_K : P|$, $N(J) = |\mathcal{O}_K : J|$ and $N(PJ) = |\mathcal{O}_K : PJ|$. From the transitivity of index we have

$$N(PJ) = |\mathcal{O}_K : PJ| = |\mathcal{O}_K : J||J : PJ| = |J : PJ|N(J).$$

It suffices to show that $|J : PJ| = N(P)$. Certainly $J \supseteq PJ$ and $J \neq PJ$ (why?). Let $\beta \in J$ with $\beta \notin PJ$. Then $J \supseteq \langle \beta \rangle + PJ \supseteq PJ$ and so

$J = \langle\beta\rangle + PJ$ (why?). Let $\gamma_1, \ldots, \gamma_m$ be a system of coset representatives for P in $\mathcal{O}_K$, so that $m = N(P)$. We shall show that $\beta\gamma_1, \ldots, \beta\gamma_m$ form a system of coset representatives for PJ in J.

If $\delta \in J$ then $\delta = \xi\beta + \eta$ with $\xi \in \mathcal{O}_K$ and $\eta \in PJ$ as $J = \langle\beta\rangle + PJ$. Now $\xi - \gamma_k \in P$ for some k, and so $\beta(\xi - \gamma_k) \in PJ$. Hence $\delta \equiv \beta\gamma_k \pmod{PJ}$ so that each coset of PJ in J is represented by some $\beta\gamma_k$.

We need to show that the $\beta\gamma_k$ represent distinct cosets of PJ. Suppose that $\beta\gamma_i \equiv \beta\gamma_k \pmod{PJ}$ with $i \neq k$. Then $\beta(\gamma_i - \gamma_k) \in PJ$. Let $\delta = \gamma_i - \gamma_k$. Then $\delta \notin P$, and as P is maximal $\langle\delta\rangle + P = \mathcal{O}_K$. There exists $\lambda \in \mathcal{O}_K$ with $\lambda\delta \equiv 1 \pmod{P}$ and so $(\lambda\delta - 1)\beta \in PJ$. But $\delta\beta \in PJ$ and so $\beta \in PJ$ which is a contradiction.

Since $\beta\gamma_1, \ldots, \beta\gamma_m$ form a system of coset representatives for PJ in J with $m = N(P)$ then the index $|J : PJ| = m = N(P)$ and this completes the proof. □

It is important to know how to find prime ideals in $\mathcal{O}_K$. The following lemma shows they are all obtained from factorization of ordinary prime numbers.

Lemma 4.9 *Let K be a number field, and let P be a prime ideal of $\mathcal{O}_K$. Then P occurs in the ideal factorization of $\langle p\rangle$ for a unique prime number p. Also $N(P)$ is a power of p.*

Proof By Proposition 4.4, P occurs in the prime factorization of $\langle p\rangle$ if and only if $P \supseteq \langle p\rangle$ which occurs if and only if $p \in P$. Let P have norm m. Then the index of P as a subgroup of $\mathcal{O}_K$ is m. Consequently $m\beta \in P$ for all $\beta \in \mathcal{O}_K$; in particular $m \in P$. Write $m = p_1 p_2 \cdots p_r$ with the p_j prime. Then $p_j \in P$ for some j since P is a prime ideal. Write $p_j = p$.

Since $P \supseteq \langle p\rangle$, $N(P)$ is a factor of $N(\langle p\rangle) = |N(p)| = p^n$ where n is the degree of K. Hence $N(P) = p^k$ for some k with $1 \leq k \leq n$. This also shows that the prime p is uniquely determined. □

One corollary of this is the fact that there are only a finite number of ideals of a given norm (one can also prove this directly from the definition of norm).

Lemma 4.10 *Let K be a number field and m a positive integer. There are only finitely many ideals I of $\mathcal{O}_K$ with $N(I) = m$.*

Proof Write $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ as a product of primes. Then I is a product of at most a_1 prime ideals dividing $\langle p_1\rangle$, at most a_2 prime ideals dividing $\langle p_2\rangle$, and so on. There are only finitely many ways of choosing these prime ideals, and consequently only finitely many possibilities for I. □

Hence we can determine all the prime ideals of $\mathcal{O}_K$ by resolving each $\langle p \rangle$ into its prime ideal factors.

When $\mathcal{O}_K = \mathbf{Z}[\alpha]$ for some α, that is when $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ forms an integral basis of $\mathcal{O}_K$, then the prime ideal factorization of p can be computed from the minimum polynomial of α. In general we cannot always find an integral basis of this form for a given K. But in special cases, for instance the important case of quadratic fields, we can.

We will need to factorize polynomials modulo p. Recall that for a prime number p, the set $\mathbf{F}_p = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}\}$ with addition and multiplication modulo p forms a field. Here we have written elements of $\mathbf{F}_p$ in the form $\overline{a}$ to distinguish them from integers, but in practice we are usually sloppy and write a both for an integer and the corresponding element of $\mathbf{F}_p$. If $f \in \mathbf{Z}[X]$ is a polynomial with integer coefficients then $\overline{f} \in \mathbf{F}_p[X]$ denotes its *reduction* modulo p, that is $\overline{a_0 + a_1 X + a_2 X^2 + \cdots + A_m X^m} = \overline{a_0} + \overline{a_1} X + \overline{a_2} X^2 + \cdots + \overline{a_m} X^m$.

When $\mathcal{O}_K = \mathbf{Z}[\alpha]$ we can classify all ideals containing $\langle p \rangle$.

Proposition 4.6 *Let K be a number field of degree n, and suppose that there is $\alpha \in \mathcal{O}_K$ with $\mathcal{O}_K = \mathbf{Z}[\alpha]$. Let f be the minimum polynomial of α, and let p be a prime number. Then each ideal of $\mathcal{O}_K$ which contains $\langle p \rangle$ has the form*

$$I_g = \langle p, g(\alpha) \rangle$$

where $g \in \mathbf{Z}[X]$ is monic and $\overline{g} \mid \overline{f}$ in $\mathbf{F}_p[X]$. Also $I_{g_1} = I_{g_2}$ if and only if $\overline{g_1} = \overline{g_2}$ in $\mathbf{F}_p[X]$.

The norm of I_g is p^d where $d = \deg(g)$, and $I_{g_1} \supseteq I_{g_2}$ if and only if $\overline{g_1} \mid \overline{g_2}$ in $\mathbf{F}_p[X]$.

Proof Suppose that $I \supseteq \langle p \rangle$. Since $f(\alpha) = 0 \in I$, there are certainly monic polynomials $g \in \mathbf{Z}[X]$ with $g(\alpha) \in I$. Fix such a polynomial g of least possible degree. Certainly $I \supseteq I_g = \langle p, g(\alpha) \rangle$. I claim that, for $h \in \mathbf{Z}[X]$, $h(\alpha) \in I$ if and only if $\overline{g} \mid \overline{h}$ in $\mathbf{F}_p[X]$. Let $d = \deg(g) = \deg(\overline{g})$. Suppose first that $\deg(\overline{h}) < d$. Then for some integer a we have $\overline{ah}$ monic, so $ah = h_1 + ph_2$ where $h_1 \in \mathbf{Z}[X]$ is monic of degree less than d and $h_2 \in \mathbf{Z}[X]$. Thus $h_1(\alpha) = ah_1(\alpha) - ph_2(\alpha) \in I$. This contradicts the definition of g. In general suppose $\overline{g} \nmid \overline{h}$ and $h(\alpha) = 0$. Then $\overline{h} - \overline{ug}$ is nonzero and has degree less than d for some $u \in \mathbf{Z}[X]$. Then $v\alpha \in I$ where $v = h - ug$ and $\overline{v}$ is nonzero and has degree less than d, which is false. Conversely, if $\overline{g} \mid \overline{h}$ then $h = ug + pv$ with $u, v \in \mathbf{Z}[X]$, and so $h \in I_g \subseteq I$. Hence $I = I_g$. As $h(\alpha) \in I$ then $\overline{g} \mid \overline{h}$.

The p^d numbers $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{d-1}\alpha^{d-1}$ where $0 \leq a_j < p$ form a system of coset representatives for I_g in $\mathcal{O}_K$, since each $h \in \mathbf{F}_p[X]$ is congruent to a unique polynomial of degree less than d modulo $\overline{g}$. Hence

$N(I_g) = p^d$. Since $g_2(\alpha) \in I_{g_1}$ if and only if $\overline{g_1} \mid \overline{g_2}$, it follows that $I_{g_1} \supseteq I_{g_2}$ if and only if $\overline{g_1} \mid \overline{g_2}$. In particular, $I_{g_1} = I_{g_2}$ if and only if $\overline{g_1} \mid \overline{g_2}$ and $\overline{g_2} \mid \overline{g_1}$, that is if and only if $\overline{g_1} = \overline{g_2}$. □

Using the above notation we get that when $g = f$, $I_f = \langle p, 0\rangle = \langle p\rangle$ and when $g = 1$ then $I_1 = \langle p, 1\rangle = \mathcal{O}_K$. Clearly the maximal (prime) ideals containing p correspond to the irreducible factors of $\overline{f}$.

Theorem 4.4 *Let K be a number field of degree n, and suppose that there is $\alpha \in \mathcal{O}_K$ with $\mathcal{O}_K = \mathbf{Z}[\alpha]$. Let f be the minimum polynomial of α, and let p be a prime number. Write*

$$\overline{f} = \overline{g_1}^{a_1}\overline{g_2}^{a_2}\cdots\overline{g_r}^{a_r}$$

where the $\overline{g_j}$ are the distinct monic irreducible factors of $\overline{f}$ in $\mathbf{F}_p[X]$. Then the prime ideal factorization of $\langle p\rangle$ in $\mathcal{O}_K$ is

$$\langle p\rangle = P_1^{a_1}P_2^{a_2}\cdots P_r^{a_r}$$

where

$$P_j = \langle p, g_j(\alpha)\rangle\,.$$

Proof By Proposition 4.6, if Q is an ideal of $\mathcal{O}_K$ and $Q \supseteq P_j$, then $Q = \langle p, h(\alpha)\rangle$ where $\overline{h} \mid \overline{g_j}$. Thus $\overline{h} = 1$ or $\overline{h} = \overline{g_j}$ so that $Q = \mathcal{O}_K$ or $Q = P_j$. Hence P_j is maximal, and so prime.

The norm of the ideal $P_1^{a_1}P_2^{a_2}\cdots P_r^{a_r}$ is

$$N(P_1)^{a_1}N(P_2)^{a_2}\cdots N(P_r)^{a_r} = p^{d_1a_1+d_2a_2+\cdots+d_ra_r}$$

where $d_j = \deg(\overline{g_j})$. Hence

$$N(P_1^{a_1}P_2^{a_2}\cdots P_r^{a_r}) = p^{\deg(\overline{f})} = p^n = N(\langle p\rangle).$$

For any polynomials h_1, $h_2 \in \mathbf{Z}[X]$ we have

$$(\langle p\rangle + \langle h_1(\alpha)\rangle)(\langle p\rangle + \langle h_2(\alpha)\rangle) \subseteq \langle p\rangle + \langle h_1h_2(\alpha)\rangle\,.$$

Iterating this by induction we get

$$P_1^{a_1}P_2^{a_2}\cdots P_r^{a_r} \subseteq \langle p\rangle + \langle g_1^{a_1}g_2^{a_2}\cdots g_r^{a_r}(\alpha)\rangle = \langle p\rangle + \langle f_1(\alpha)\rangle$$

where $f_1 = g_1^{a_1}g_2^{a_2}\cdots g_r^{a_r}$. Then $f_1 - f = pf_2$ where $f_2 \in \mathbf{Z}[\alpha]$. But $f_1(\alpha) = pf_2(\alpha) \in \langle p\rangle$ so that $P_1^{a_1}P_2^{a_2}\cdots P_r^{a_r} \subseteq \langle p\rangle$. But we have seen these ideals have the same norm, so they are equal. □

In fact this result is true even when $\mathcal{O}_K \neq \mathbf{Z}[\alpha]$ as long as $p \nmid |\mathcal{O}_K : \mathbf{Z}[\alpha]|$. We shall not prove this generalization.

Example Let $K = \mathbf{Q}(\sqrt{m})$ be a quadratic field where m is a squarefree integer with $m \not\equiv 1 \pmod 4$. Then $\mathcal{O}_K = \mathbf{Z}[\alpha]$ where $\alpha = \sqrt{m}$ has minimum polynomial $X^2 - m$. To determine the prime ideal factorization of $\langle p \rangle$, where p is a prime number, in $\mathcal{O}_K$, we must factorize $X^2 - m$ in $\mathbf{F}_p[X]$. There are three possibilities:

1. $X^2 - m$ is irreducible over $\mathbf{F}_p$. Then $\langle p \rangle$ is a prime ideal of $\mathcal{O}_K$. This occurs when the congruence $x^2 \equiv m \pmod p$ is insoluble. This can only happen when p is odd. This condition is described by saying that m is a *quadratic nonresidue* of p. In this case we say that p *is inert* in K.

2. $X^2 - m$ splits into two distinct factors over $\mathbf{F}_p$. Then $X^2 - m \equiv (X - a)(X + a) \pmod p$ with $a \not\equiv -a \pmod p$. This means that p is odd, $a^2 \equiv m \pmod p$ and $p \nmid m$. This condition is described by saying that m is a *quadratic residue* of p. In this case $\langle p \rangle = P_1 P_2$ where $P_1 = \langle p, \sqrt{m} + a \rangle$ and $P_2 = \langle p, \sqrt{m} - a \rangle$. Here $P_1 \neq P_2$ and both P_1 and P_2 have norm p. In this case we say that p *splits* in K.

3. $X^2 - m$ splits into two equal factors over $\mathbf{F}_p$. This happens only when $p = 2$ or when $p \mid m$. When $p = 2$ then $X^2 - m \equiv X^2$ or $(X + 1)^2 \pmod 2$ according to the parity of m. When $p \mid m$ then $X^2 - m \equiv X^2 \pmod p$. Then $\langle p \rangle = P^2$ where $P = \langle p, \sqrt{m} \rangle$, unless $p = 2$ and m is odd when $P = \langle 2, \sqrt{m} + 1 \rangle$. In any case P has norm p. In this case we say that p *ramifies* in K.

Note that p ramifies if and only if p divides the discriminant of K. Thus is true for all number fields K, but is too difficult to prove in this course.

It is a good exercise to perform the same calculations when $K = \mathbf{Q}(\sqrt{m})$ has $m \equiv 1 \pmod 4$.

The theory of ideal factorization allows us to prove various results in elementary number theory.

Example Let $K = \mathbf{Q}(i)$. We know that K is norm-Euclidean so that $\mathcal{O}_K = \mathbf{Z}[i]$ is a Euclidean domain. Then each ideal of $\mathbf{Z}[i]$ is principal.

Let p be a prime number. Then p splits in K whenever p is odd and the congruence $a^2 \equiv -1 \pmod p$ is soluble. By elementary number theory this occurs if and only if $p \equiv 1 \pmod 4$. When $p \equiv 1 \pmod 4$ then $\langle p \rangle = P_1 P^2$ where $P_1 = \langle p, a + i \rangle$ and $P_2 = \langle p, a - i \rangle$. Here $a^2 \equiv -1 \pmod p$. These ideals are principal: $P_1 = \langle \beta \rangle$ and as $N(P_1) = p$ then $N(\beta) = p$. Hence

$p = b^2 + c^2$ where $\beta = b + ci$. We have recovered the two-square theorem of elementary number theory: if p is a prime congruent to 1 modulo 4, then p is the sum of two squares of integers.

If for a given p we can find an a with $a^2 \equiv -1 \pmod{p}$ then by applying the Euclidean algorithm for $\mathbf{Z}[i]$ to p and $a+i$ we can obtain $\beta = \gcd(p, a+i)$ and so integers b and c with $p = b^2 + c^2$.

We shall briefly consider ideals in $K = \mathbf{Q}(\zeta)$ where $\zeta = \exp(2\pi i/p)$ and p is an odd prime number. We have seen that the minimum polynomial of ζ is $f(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$ so that K has degree $p-1$. Certainly $\zeta \in \mathcal{O}_K$. Let $\lambda = \zeta - 1$, so that $\mathbf{Z}[\zeta] = \mathbf{Z}[\lambda]$. Then $N(\zeta) = (-1)^{p-1}N(-\zeta) - f(0) = 1$ and $N(\lambda) = (-1)^{p-1}N(1-\zeta) = f(1) = p$. Also $f(\lambda + 1) = 0$ so that the minimum polynomial of λ is

$$g(X) = f(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = X^{p-1} + \sum_{j=1}^{p-1} \binom{p}{j} X^{p-1-j}.$$

Thus

$$\lambda^{p-1} = -\sum_{j=1}^{p-1} \binom{p}{j} \lambda^{p-1-j} = -\sum_{k=0}^{p-2} \binom{p}{k+1} \lambda^k.$$

In particular $\lambda^{p-1} = p\beta$ where $\beta \in \mathcal{O}_K$. Comparing norms gives

$$p^{p-1} = N(\lambda^{p-1}) = p^{p-1}N(\beta).$$

Consequently $N(\beta) = 1$ and $\beta = \lambda^{p-1}/p$ is a unit.

Proposition 4.7 *Let $K = \mathbf{Q}(\zeta)$ where p is an odd prime number and $\zeta = \exp(2\pi i/p)$. Then $\Delta(1, \zeta, \zeta^2, \ldots, \zeta^{p-2}) = (-1)^{(p-1)/2}p^{p-2}$.*

Proof Call this discriminant Δ. Then $\Delta = (-1)^{p(p-1)/2}f'(\zeta)$ where f is the minimum polynomial of ζ. Then $f(X) = (X^p - 1)/(X - 1)$, so

$$f'(X) = \frac{p(X-1)X^{p-2} - (X^p - 1)}{(X-1)^2}$$

and so $f'(\zeta) = p\zeta^{p-2}/(\zeta - 1)$. Hence $N(f'(\zeta)) = N(p)N(\zeta)^{p-1}/N(\zeta - 1) = p^{p-2}$. As p is odd, $(-1)^{p(p-1)/2} = (-1)^{(p-1)/2}$ and the result follows. □

We can now show that the ring of integers of $\mathbf{Q}(\zeta)$ is $\mathbf{Z}[\zeta]$. We have seen $N(\lambda) = p$ and α^{p-1}/p is a unit. Thus $\langle\lambda\rangle$ must be a prime ideal of norm p and $\langle\lambda\rangle^{p-1} = \langle p\rangle$. We thus know the prime factorization of $\langle q\rangle$ when $q = p$.

Theorem 4.5 *Let $K = \mathbf{Q}(\zeta)$ where p is an odd prime number and $\zeta = \exp(2\pi i/p)$. Then $\mathcal{O}_K = \mathbf{Z}[\zeta]$.*

Proof Since the discriminant of $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}$ is, up to sign, a power of p, the index $|\mathcal{O}_K : \mathbf{Z}[\zeta]|$ is a power of p. If $\mathcal{O}_K \neq \mathbf{Z}[\zeta]$ then there is $\beta \in \mathcal{O}_K$ with $\beta \notin \mathbf{Z}[\zeta]$ but $p\beta \in \mathbf{Z}[\zeta]$. Since $\mathbf{Z}[\zeta] = \mathbf{Z}[\lambda]$, where $\lambda = \zeta - 1$ then we can write

$$\beta = \frac{1}{p} \sum_{j=0}^{p-2} b_j \lambda^j$$

where the b_j are integers, not all divisible by p. Choose j to be the smallest number such that $p \nmid b_j$. Then

$$\frac{1}{p} \sum_{k=0}^{j-1} b_k \lambda^k \in \mathcal{O}_K$$

and so

$$\gamma = \beta - \frac{1}{p} \sum_{j=0}^{j-1} b_k \lambda^k = \frac{1}{p} \sum_{k=j}^{p-2} b_k \lambda^k \in \mathcal{O}_K.$$

We infer that

$$\lambda^{p-2-j}\gamma = \frac{1}{p} \sum_{k=j}^{p-2} b_k \lambda^{p-2-j+k} \in \mathcal{O}_K.$$

But we have seen that $\lambda^{p-1}/p \in \mathcal{O}_K$. Then for $k \geq j+1$ we have $\lambda^{p-2+j+k}/p = \lambda^{p-1}\lambda^{k-j-1} \in \mathcal{O}_K$. Hence

$$\frac{b_j \lambda^{p-1}}{p} = \lambda^{p-2-j}\gamma - \frac{1}{p} \sum_{k=j+1}^{p-2} b_k \lambda^{p-2-j+k} \in \mathcal{O}_K.$$

We now consider norms. The norm of $b_j\lambda^{p-2}/p$ is $b_j^{p-1}p^{p-2}/p^{p-1} = b_j^{p-1}/p$. This must be an integer, yet it cannot be as $p \nmid b_j$. This contradiction shows that $\mathcal{O}_k = \mathbf{Z}[\zeta]$. □

Example Let $K = \mathbf{Q}(\zeta)$ where $\zeta = \exp(2\pi i/5)$. Then $\mathcal{O}_K = \mathbf{Z}[\zeta]$ and ζ has minimum polynomial $f(X) = X^4 + X^3 + X^2 + X + 1$. For each prime number q we aim to factorize the ideal $\langle q \rangle$ by factorizing the polynomial f modulo q.

Consider the case $q = 5$. Then

$$(X-1)^4 = X^4 - 4X^3 + 6X^2 - 4X + 1 \equiv X^4 + X^3 + X^2 + X + 1 \pmod 5.$$

It follows that $\langle 5 \rangle = P_5^4$ where $P_5 = \langle 5, \zeta - 1 \rangle$. For $\lambda = \zeta - 1$ we have seen that $\lambda^4 \mid 5$ so that $P_5 = \langle \lambda \rangle$. Hence $\langle 5 \rangle$ is the fourth power of the prime ideal $\langle \zeta - 1 \rangle$.

Now suppose that $q \neq 5$. If f is reducible modulo q, then either it has a linear factor or a quadratic factor. Let us suppose that f has the linear factor $X - a$ modulo q. Then $f(a) \equiv 0 \pmod{q}$ and so as $f(X)(X-1) = X^5 - 1$ then $a^5 \equiv 1 \pmod{q}$. But $a \not\equiv 1 \pmod{q}$ for $f(1) = 5 \not\equiv 0 \pmod{q}$. Thus a has order 5 modulo p. The powers a^2, a^3, a^4 must also be solutions of $f(x) \equiv 0 \pmod{p}$, so we have

$$f(X) \equiv (X-a)(X-a^2)(X-a^3)(X-a^4) \pmod{q}.$$

Such an a exists if and only if $q \equiv 1 \pmod{5}$, and we conclude for these primes that $\langle q \rangle$ is a product of four distinct prime ideals, each of norm q. For instance, take $q = 11$. Then $a = 3$ satisfies $a^5 \equiv 1 \pmod{11}$ and $a^2 \equiv 9$, $a^3 \equiv 5$, and $a^4 \equiv 4 \pmod{11}$. Thus

$$\langle 11 \rangle = \langle 11, \zeta - 3 \rangle \langle 11, \zeta - 4 \rangle \langle 11, \zeta - 5 \rangle \langle 11, \zeta - 9 \rangle .$$

If f has no linear factor modulo q then either f is irreducible or f is the product of two quadratics, each irreducible modulo q. In the latter case then in fact

$$f(X) \equiv (X^2 + aX + 1)(X^2 + bX + 1) \pmod{q} \qquad (*)$$

for some a and b. I shan't prove this; it is easy if one knows some theory of finite fields, otherwise it's a rather messy calculation. Then $(*)$ holds if and only if $a + b \equiv 1$ and $ab \equiv -1 \pmod{q}$, that is that a and b are the roots of $Y^2 - Y - 1 \equiv 0 \pmod{q}$. This equation is soluble modulo q if and only if 5 is a square modulo q; then a and b are congruent to $\frac{1}{2}(1 \pm s)$ modulo q, where $s^2 \equiv 5 \pmod{q}$. By quadratic reciprocity 5 is a square modulo q if and only if $q \equiv \pm 1 \pmod{5}$. We have seen that $q \equiv 1 \pmod{5}$ if and only if $\langle q \rangle$ is the product of four prime ideals of norm q. Thus $\langle q \rangle$ is the product of two prime ideals of norm q^2 if and only if $q \equiv -1 \pmod{5}$. For example, let $q = 19$. Then $9^2 \equiv 5 \pmod{19}$ and so we can take $a = \frac{1}{2}(1+9) = 5$ and $b = \frac{1}{2}(1-9) = -4$. That is

$$f(X) \equiv (X^2 + 5X + 1)(X^2 - 4X + 1) \pmod{19}$$

and both $X^2 + 5X + 1$ and $X^2 - 4X + 1$ are irreducible modulo 19. Thus

$$\langle 19 \rangle = \left\langle 19, \zeta^2 + 5\zeta + 1 \right\rangle \left\langle 19, \zeta^2 - 4\zeta + 1 \right\rangle$$

is the factorization of $\langle 19 \rangle$ into prime ideals.

In all other cases, that is when $q \equiv \pm 2 \pmod{5}$ then f is irreducible modulo q and $\langle q \rangle$ is prime.

5 Ideal classes

The set of fractional ideals of a number field K forms an abelian group under multiplication which we shall call $\mathcal{I}_K$. The set of principal fractional ideals of K is a subgroup of $\mathcal{I}_K$ and we shall denote it by $\mathcal{P}_K$. The quotient group of $\mathcal{I}_K/\mathcal{P}_K$ is called the *class-group* of K and is denoted by Cl_K. Its elements are the cosets of $\mathcal{P}_K$ in $\mathcal{I}_K$ and are called *ideal classes*. An ideal class is an equivalence class of fractional ideals under the equivalence relation $I \sim J$ if $I = \beta J$ for some nonzero $\beta \in K$. The set of principal fractional ideals forms an ideal class, the *principal* ideal class. We denote the ideal class containing the fractional ideal I by $[I]$. We can consider Cl_K as the set of such symbols $[I]$ obeying the rule that $[I] = [J]$ whenever $J = \beta I$, $\beta \in K$ and $\beta \neq 0$ and with the operation $[I][J] = [IJ]$. The identity element of Cl_K is $[\langle 1\rangle] = [\mathcal{O}_K]$. In addition since each fractional ideal I of K has the form βJ where J is an ideal, then $[I] = [J]$ and so each ideal class contains ideals.

Example Let $K = \mathbf{Q}(\sqrt{-6})$ so that $\mathcal{O}_K = \mathbf{Z}[\sqrt{-6}]$. Consider the ideals $I = \langle 2, \sqrt{-6}\rangle$ and $J = \langle 3, \sqrt{-6}\rangle$. We have already seen that I and J are nonprincipal. We can now write this as $[I] \neq [\mathcal{O}_K]$ and $[J] \neq [\mathcal{O}_K]$. But we also have $I^2 = \langle 2\rangle$, $IJ = \langle \sqrt{-6}\rangle$ and $J^2 = \langle 3\rangle$. Thus $[I]^2 = [I][J] = [J]^2 = [\mathcal{O}_K]$ in Cl_K. Thus $[J] = [I]^{-1} = [I]$, that is, the ideals I and J lie in the same ideal class. Indeed $IJ^{-1} = IJJ^{-2} = \langle \sqrt{-6}\rangle \langle 2\rangle^{-1} = \langle \sqrt{-6}/2\rangle$. Hence $J = (\sqrt{-6}/2)I$. We can confirm this by calculating

$$\frac{\sqrt{-6}}{2} I = \frac{\sqrt{-6}}{2} \langle 2, \sqrt{-6}\rangle = \langle \sqrt{-6}, -3\rangle = \langle 3, \sqrt{-6}\rangle = J.$$

So we have at least two elements, $[\mathcal{O}_K]$ and $[I]$, in Cl_K. As $[I]^2 = [\mathcal{O}_K]$ then $[I]$ has order 2 in the class-group. It will turn out that these are the only ideal classes in K so that $|\mathrm{Cl}_K| = 2$.

We now aim to prove that the class-group of each number field is finite. The order of the class-group Cl_K of K is called the *class-number* of K and is denoted by h_K. In particular $h_K = 1$ if and only if every ideal of $\mathcal{O}_K$ is principal. The crucial step in proving the finiteness of the class-group is the following result, which shows that each nonzero ideal of $\mathcal{O}_K$ has an element of approximately the same norm as that of the ideal.

Proposition 5.1 *Let K be a number field. There is a positive number A_K with the following property: each nonzero ideal I of $\mathcal{O}_K$ has a nonzero element β with $|N(\beta)| \leq A_K N(I)$.*

Proof Let $\gamma_1, \ldots, \gamma_n$ form an integral basis of $\mathcal{O}_K$. Let $m = N(I)$ and let r be the integer part of $m^{1/n}$, that is r is an integer and $r \leq m^{1/n} < r + 1$.

Consider the set

$$\mathcal{A} = \{b_1\gamma_1 + b_2\gamma_2 + \cdots + b_n\gamma_n : b_j \in \mathbf{Z}, 0 \leq b_j \leq r\}.$$

Then $\mathcal{A}$ has $(r+1)^n$ elements and so $|\mathcal{A}| > m$. The elements of $\mathcal{A}$ cannot lie in distinct cosets of I in $\mathcal{O}_K$. Hence there are β_1, $\beta_2 \in \mathcal{A}$ with $\beta_1 \neq \beta_2$ but $\beta_1 \equiv \beta_2 \pmod{I}$. Set $\beta = \beta_1 - \beta_2$. Then $\beta \neq 0$ but $\beta \in I$. Also $\beta = \sum_{j=1}^n c_j\beta_j$ where $c_j \in \mathbf{Z}$ and $|c_j| \leq r$.

Now $N(\beta) = \prod_{k=1}^n \sigma_k(\beta)$ and $\sigma_k(\beta) = \sum_{j=1}^n c_j\sigma_k(\beta_j)$. Hence

$$|\sigma_k(\beta)| \leq \sum_{j=1}^n |c_j||\sigma_k(\beta_j)| \leq r\sum_{j=1}^n |\sigma_k(\beta_j)|.$$

Multiplying these inequalities together gives

$$|N(\beta)| \leq r^n \prod_{k=1}^n \sum_{j=1}^n |\sigma_k(\beta_j)| \leq A_K m = A_K N(I)$$

where

$$A_K = \prod_{k=1}^n \sum_{j=1}^n |\sigma_k(\beta_j)|.$$

□

Note here that it is important that A_K only depends on K and not on the ideal I. Also if we know an integral basis we can calculate A_K. However using other methods we can often get smaller constants that this A_K and they will be better in practice.

We now show that each ideal class contains an ideal of small norm.

Proposition 5.2 *Let K be a number field, and suppose that the number A has the property that each nonzero ideal I of $\mathcal{O}_K$ as a nonzero element β with $|N(\beta)| \leq AN(I)$. Then each ideal class of K contains an ideal J with norm $N(J) \leq A$.*

Proof Let $[I]$ be an ideal class with I an ideal of $\mathcal{O}_K$. Let $\beta \in I$ have $\beta \neq 0$ and $|N(\beta)| \leq AN(I)$. Then $I \supseteq \langle\beta\rangle$ and by Proposition 4.4 $\langle\beta\rangle = IJ$ for some ideal J of $\mathcal{O}_K$. Then $[J] = [I]^{-1}$ and by Theorem 4.1 and Proposition 4.5 we have

$$N(J) = \frac{N(\langle\beta\rangle)}{N(I)} = \frac{|N(\beta)|}{N(I)} \leq A.$$

Hence the ideal class $[I]^{-1}$ has an ideal of norm at most A, but if we had started with $[I]^{-1}$ instead of $[I]$ we would have proved that $[I]$ has an ideal of norm at most A. □

The finiteness of the class-group is now easy to see.

Theorem 5.1 *Let K be a number field. Its class-group Cl_K is a finite abelian group.*

Proof Only the finiteness needs to be shown. By Propositions 5.1 and 5.2 there is a positive number A with each class of K containing an ideal of $\mathcal{O}_K$ with norm at most A. By Lemma 4.10, $\mathcal{O}_K$ has only finitely many norms of each given norm, and so only finitely many ideals of norm at most A. Therefore K has only finitely many ideal classes. □

These results give us a method for finding the class-group and so also the class-number. First find a constant A for which Proposition 5.2 is valid, and find all ideals of norm at most A. Determine which of these lie in the same ideal classes. Of course, this is easier said than done, but is is clear that the smaller one can make A, the less work needs to done.

An alternative is to find all prime ideals P of norm at most A. Each ideal of norm at most A is a product of prime ideals of norm at most A. Thus the ideal classes $[P]$ for these prime ideals generate the class-group in the sense that each ideal class is a product of powers of such ideal classes.

Example Let $K = \mathbf{Q}(\sqrt{-6})$. Then $\mathcal{O}_K$ has integral basis 1, $\sqrt{-6}$. Using the proof of proposition 5.1 we can take

$$A = (|\sigma_1(1)| + |\sigma_1(\sqrt{-6})|)(|\sigma_2(1)| + |\sigma_2(\sqrt{-6})|) = (1+\sqrt{6})^2 \approx 11 \cdot 9.$$

We shall find all prime ideals of norm at most 11. We find that 2 and 3 ramify, 5 and 7 and 11 split. In detail $\langle 2\rangle = P_2^2$ where $P_2 = \langle 2, \sqrt{-6}\rangle$, $\langle 3\rangle = P_3^2$ where $P_3 = \langle 3, \sqrt{-6}\rangle$, $\langle 5\rangle = P_5 Q_5$ where $P_5 = \langle 5, \sqrt{-6}+2\rangle$ and $Q_5 = \langle 5, \sqrt{-6}-2\rangle$, $\langle 7\rangle = P_7 Q_7$ where $P_7 = \langle 7, \sqrt{-6}+1\rangle$ and $Q_7 = \langle 7, \sqrt{-6}-1\rangle$, and $\langle 11\rangle = P_{11}Q_{11}$ where $P_{11} = \langle 11, \sqrt{-6}+4\rangle$ and $Q_{11} = \langle 11, \sqrt{-6}-4\rangle$. Thus P_2, P_3, P_5, Q_5, P_7, Q_7, P_{11} and Q_{11} are the prime ideals of norm at most 11, and each ideal class of K is the product of powers of these classes.

To find the relations between these ideal classes we look at the factorization of principal ideals of small norm. We already know that $[P_2]^2 = [\langle 2\rangle] = [\langle 1\rangle]$, $[P_3]^2 = [\langle 3\rangle] = [\langle 1\rangle]$, $[P_5][Q_5] = [\langle 5\rangle] = [\langle 1\rangle]$, $[P_7][Q_7] = [\langle 7\rangle] = [\langle 1\rangle]$ and $[P_{11}][Q_{11}] = [\langle 11\rangle] = [\langle 1\rangle]$. Consider $\langle \sqrt{-6}\rangle$. It has norm 6 so must be the product of prime ideals of norms 2 and 3. Hence $\sqrt{-6} = P_2P_3$ and so $[P_2][P_3] = [\langle 1\rangle]$. As $[P_2]^2 = [\langle 1\rangle]$ then $[P_2] = [P_3]$ (as we have already observed). Next $\langle 1+\sqrt{-6}\rangle$ has norm 7, so this is a prime ideal of norm 7. As $1+\sqrt{-6} \in P_7$ then $P_7 = \langle 1+\sqrt{-6}\rangle$ is principal, and so $[P_7] = [\langle 1\rangle]$ and $[Q_7] = [\langle 1\rangle][P_7]^{-1} = [\langle 1\rangle]$. Next $\langle 2+\sqrt{-6}\rangle$ has norm 10 and so is the product of prime ideals of norms 2 and 5. Hence it is either P_2P_5 or P_2Q_5. But $2+\sqrt{-6} \in P_5$ and so $\langle 2+\sqrt{-6}\rangle \subseteq P_5$. Hence $\langle 2+\sqrt{-6}\rangle = P_2P_5$ and so $[P_5] = [P_2]^{-1} = [P_2]$. Also $[Q_5] = [P_5]^{-1} = [P_2]^{-1} = [P_2]$. Then $\langle 4+\sqrt{-6}\rangle$

has norm 22 and so is the product of prime ideals of norms 2 and 11. It is either P_2P_{11} or P_2Q_{11}, But $4+\sqrt{-6} \in P_{11}$ and so $\langle 4+\sqrt{-6}\rangle \subseteq P_{11}$. Hence $\langle 4+\sqrt{-6}\rangle = P_2P_{11}$ and so $[P_{11}] = [P_2]^{-1} = [P_2]$. Also $[Q_{11}] = [P_{11}]^{-1} = [P_2]^{-1} = [P_2]$. Summarizing, we have $[P_2] = [P_3] = [P_5] = [Q_5] = [P_{11}] = [Q_{11}]$ and $[P_7] = [Q_7] = [\langle 1\rangle]$. We also have $[P_2]^2 = [\langle 1\rangle]$. Hence $\mathrm{Cl}_K = \{[\langle 1\rangle], [P_2]\}$. We have seen that P_2 is nonprincipal so that $[P_2] \neq [\langle 1\rangle]$. Hence the class-group has two elements and $h_K = 2$.

If one knows what the class-number is of a field is, then one can often prove that certain ideals are principal.

Lemma 5.1 *Let K be a number field with class-number h, and let m be an integer with $\gcd(m,h) = 1$. If I is an ideal of $\mathcal{O}_K$ and I^m is principal, then I is principal.*

Proof By assumption we have $[I]^m = [I^m] = [\langle 1\rangle]$ in Cl_K. As h is the order of the group Cl_K then $[I]^h = [\langle 1\rangle]$ also. As $\gcd(m,h) = 1$ there exist integers r and s with $1 = mr + hs$. Then

$$[I] = [I]^{mr+hs} = ([I]^m)^r([I]^h)^s = [\langle 1\rangle]^r[\langle 1\rangle]^s = [\langle 1\rangle].$$

Hence I is principal. □

Another useful lemma really has nothing to do with the class-group and everything to do with unique factorization into prime ideals. We say that two ideals I and J of $\mathcal{O}_K$ are *coprime* if $I + J = \mathcal{O}_K$. Then there is no prime ideal P with $P \supseteq I$ and $P \supseteq J$ (for otherwise $P \supseteq I + J$) and so no prime ideal occurs in both the factorizations of I and J.

Lemma 5.2 *Let K be a number field. Let I_1 and I_2 be coprime ideals of $\mathcal{O}_K$ and suppose that $I_1I_2 = J^m$ for some ideal J and integer m. Then $I_1 = J_1^m$ and $I_2 = J_2^m$ for some ideals J_1 and J_2.*

Proof Let P be a prime ideal occurring in the factorization of I_1. Suppose that P occurs a times in this factorization. Then P does not occur in the prime ideal factorization of I_2, as I_1 and I_2 are coprime. Hence P occurs a times in the prime ideal factorization of $I_1I_2 = J^m$. But if P occurs b times in the prime ideal factorization of J then P occurs mb times in the prime ideal factorization of J^m and so $a = mb$ so that $m \mid a$. As this is true for all prime ideal factors of I_1 then I_1 is the m-th power of an ideal. Similarly I_2 is the m-th power of an ideal. □

Example As an application of these ideas, we investigate the solutions of

$$y^3 = x^2 + 6 \qquad (*)$$

with x, $y \in \mathbf{Z}$. let us work in $K = \mathbf{Q}(\sqrt{-6})$ so that $\mathcal{O}_K = \mathbf{Z}[\sqrt{-6}]$. From $(*)$ we get

$$y^3 = (x + \sqrt{-6})(x - \sqrt{-6})$$

and so in ideal terms

$$\langle y \rangle^3 = \left\langle x + \sqrt{-6} \right\rangle \left\langle x - \sqrt{-6} \right\rangle . \qquad (\dagger)$$

By Lemma 5.2, we can conclude that if the ideals $\left\langle x + \sqrt{-6} \right\rangle$ and $\left\langle x - \sqrt{-6} \right\rangle$ are coprime then each is a cube of an ideal.

Consider then $I = \left\langle x + \sqrt{-6} \right\rangle + \left\langle x - \sqrt{-6} \right\rangle = \left\langle x + \sqrt{-6}, x - \sqrt{-6} \right\rangle$. Then

$$(x + \sqrt{-6}) - (x - \sqrt{-6}) = 2\sqrt{-6} \in I$$

and

$$(x - \sqrt{-6})(x + \sqrt{-6}) = x^2 + 6 \in I.$$

From $2\sqrt{-6} \in I$ we get $\sqrt{-6}(2\sqrt{-6}) = -12 \in I$. If x is not divisible by 2 or 3 then neither is $x^2 + 6$ and so $\gcd(x^2 + 6, -12) = 1$. This implies that $I = \langle 1 \rangle$. Hence as long as x is not divisible by 2 and 3 then $\left\langle x + \sqrt{-6} \right\rangle$ and $\left\langle x - \sqrt{-6} \right\rangle$ are coprime.

If x is even, then by $(*)$ we have $y^3 \equiv 2 \pmod 4$ which is impossible. If $3 \mid x$ then we have $y^3 \equiv 3 \pmod 9$ which is impossible. Hence $\left\langle x + \sqrt{-6} \right\rangle$ and $\left\langle x - \sqrt{-6} \right\rangle$ are coprime and so $\left\langle x + \sqrt{-6} \right\rangle = J^3$ for some ideal J by Lemma 5.2.

The class-number of K is 2, so that by Lemma 5.1, J is a principal ideal. Write $J = \langle \beta \rangle$. Then $\left\langle x + \sqrt{-6} \right\rangle = \langle \beta^3 \rangle$. This means that $x + \sqrt{-6} = \eta\beta^3$ where η is a unit of $\mathcal{O}_K$. But the only units of $\mathcal{O}_K$ are ± 1 so that $x + \sqrt{-6} = \pm\beta^3 = (\pm\beta)^3 = \gamma^3$ where $\gamma = \pm\beta \in \mathcal{O}_K$. Write $\gamma = a + b\sqrt{-6}$ where a, $b \in \mathbf{Z}$. Then

$$x = a^3 - 18ab^2 \qquad \text{and} \qquad 1 = 3a^2b - 6b^3.$$

The latter equation is absurd as it implies that $3 \mid 1$. Hence there are no integers x and y satisfying $(*)$.

6 Geometric methods

We can obtain results such as better bounds in Proposition 5.1, by regarding a number field K of degree n as a subset of $\mathbf{R}^n$. For simplicity's sake, we shall restrict ourselves to quadratic fields here. The general case is no harder in principle, but more complicated in detail. For further details see appropriate

textbooks. Alas, I shall not illustrate the arguments here with diagrams due to my inability to produce then in LaTeX, but the reader should supply her or his own.

Throughout this section, let K be a quadratic field. Then $K = \mathbf{Q}(\sqrt{m})$ for some squarefree integer m. We define a map $\bar{\sigma}$ from K to $\mathbf{R}^2$ or to $\mathbf{C}$ according to whether K is real or imaginary. When K is imaginary we simply take $\bar{\sigma}(\beta) = \beta$. When K is real, let $\bar{\sigma}(a + b\sqrt{m}) = (a + b\sqrt{m}, a - b\sqrt{m})$. Of course we can regard $\mathbf{R}^2$ and $\mathbf{C}$ as being "the same" by letting $(x, y) \in \mathbf{R}^2$ correspond to $x + iy$ in $\mathbf{C}$. Write

$$\tau = \begin{cases} \sqrt{m} & \text{if } m \not\equiv 1 \pmod 4, \\ \frac{1}{2}(1 + \sqrt{m}) & \text{if } m \equiv 1 \pmod 4 \end{cases}$$

so that $\mathcal{O}_K = \mathbf{Z}[\tau]$. The image $\bar{\sigma}(\mathcal{O}_K)$ of $\mathcal{O}_K$ under $\bar{\sigma}$ is now easily seen to equal

$$\{a\mathbf{v}_1 + b\mathbf{v}_2 : a, b \in \mathbf{Z}\}$$

where $\mathbf{v}_1 = \bar{\sigma}(1)$ and $\mathbf{v}_2 = \bar{\sigma}(\tau)$.

Lemma 6.1 *The vectors $\mathbf{v}_1 = \bar{\sigma}(1)$ and $\mathbf{v}_2 = \bar{\sigma}(\tau)$ are linearly independent over $\mathbf{R}$.*

Proof In the case where K is imaginary, $\mathbf{v}_1 = 1 \in \mathbf{C}$ and $\mathbf{v}_2$ has nonzero imaginary part so clear $\mathbf{v}_1$ and $\mathbf{v}_2$ are linearly independent over $\mathbf{R}$.

Suppose that K is real. Then $\mathbf{v}_1 = (1, 1)$ and $\mathbf{v}_2 = (\sqrt{m}, -\sqrt{m})$ or $(\frac{1}{2}(1+\sqrt{m}), \frac{1}{2}(1-\sqrt{m}))$. The matrix with rows $\mathbf{v}_1$ and $\mathbf{v}_2$ is now seen to have nonzero determinant. This means that $\mathbf{v}_1$ and $\mathbf{v}_2$ are linearly independent over $\mathbf{R}$. □

It follows that $\bar{\sigma}(\mathcal{O}_K)$ is a *lattice* in $\mathbf{R}^2$, that is a set of the form

$$\Lambda = \{a\mathbf{u}_1 + b\mathbf{u}_2 : a, b \in \mathbf{Z}\}$$

where $\mathbf{u}_1$ and $\mathbf{u}_2$ are vectors in $\mathbf{R}^2$ which are linearly independent over $\mathbf{R}$. We need some basic results on lattices. We call $\mathbf{u}_1$ and $\mathbf{u}_2$ *generators* of the lattice Λ. The generators $\mathbf{u}_1$ and $\mathbf{u}_2$ determine a *fundamental region*

$$\mathcal{F} = \{r\mathbf{u}_1 + s\mathbf{u}_2 : r, s \in \mathbf{R}, 0 \le r, s < 1\}$$

of Λ. Each element of $\mathbf{R}^2$ is the sum of an element in Λ and in $\mathcal{F}$.

Lemma 6.2 *Let Λ be a lattice in $\mathbf{R}^n$ with generators $\mathbf{u}_1$ and $\mathbf{u}_2$. Let $\mathcal{F}$ be the fundamental region associated to $\mathbf{u}_1$ and $\mathbf{u}_2$. Each $\mathbf{x} \in \mathbf{R}^2$ can be uniquely expressed as $\mathbf{x} = \mathbf{a} + \mathbf{t}$ where $\mathbf{a} \in \Lambda$ and $\mathbf{t} \in \mathcal{F}$.*

Proof The vectors $\mathbf{u}_1$ and $\mathbf{u}_2$ form a basis for $\mathbf{R}^2$. Write $\mathbf{x} = x_1\mathbf{u}_1 + x_2\mathbf{u}_2$ where x_1 and x_2 are uniquely determined. If $\mathbf{a} = a_1\mathbf{u}_1 + a_2\mathbf{u}_2 \in \Lambda$ and $\mathbf{t} = t_1\mathbf{u}_1 + t_2\mathbf{u}_2 \in \mathcal{F}$ then a_1, $a_2 \in \mathbf{Z}$, t_1, $t_2 \in [0, 1)$. Also $\mathbf{x} = \mathbf{a} + \mathbf{t}$ if and only if $x_1 = a_1 + t_1$ and $x_2 = a_2 + t_2$. This can only happen if a_j is the integer part of x_j ($j = 1, 2$) and then $t_j = x_j - a_j$ is its fractional part. Thus the representation $\mathbf{x} = \mathbf{a} + \mathbf{t}$ is uniquely determined. □

Geometrically the fundamental region $\mathcal{F}$ is a parallelogram, and we define the *area* of the lattice Λ as the area of $\mathcal{F}$. We can easily calculate the area of Λ given the generators $\mathbf{u}_1$ and $\mathbf{u}_2$.

Lemma 6.3 *The area of the lattice Λ in $\mathbf{R}^2$ with generators $\mathbf{u}_1$ and $\mathbf{u}_2$ equals $|\det(U)|$, where U is the matrix with rows $\mathbf{u}_1$ and $\mathbf{u}_2$.*

Proof Let

$$U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}$$

be the matrix with rows $\mathbf{u}_1$ and $\mathbf{u}_2$. Consider the map $\psi : \mathbf{R}^2 \to \mathbf{R}^2$ given by $\psi(\mathbf{x}) = \mathbf{x}U$. Then ψ is linear with matrix U and so it multiplies areas by $|\det(U)|$. But $\mathcal{F} = \psi(\mathcal{A})$ where $\mathcal{A} = [0, 1) \times [0, 1)$ is a square of area 1. Hence the area of $\mathcal{F}$ is $|\det(U)|$. □

We aim to show that various regions in the plane contain points of a lattice Λ if their area is big enough. Obviously a very wiggly region might be large but still miss all the points of Λ. We introduce a class of regions which are not too wiggly, namely convex regions. We say that a subset A of $\mathbf{R}^2$ is *convex* if for any points $\mathbf{a}$, $\mathbf{b} \in A$, the line segment joining $\mathbf{a}$ to $\mathbf{b}$ lies in A; more formally if $\mathbf{a}$, $\mathbf{b} \in A$ and $0 < t < 1$ then $t\mathbf{a} + (1 - t)\mathbf{b} \in A$. We aim to show that a sufficiently large and nice enough convex region containing the origin must contain some other point of the lattice Λ. We first need a technical result, an analogue of the pigeonhole principle.

Lemma 6.4 *Let Λ be a lattice in $\mathbf{R}^2$, and let $\mathcal{X}$ be a bounded subset of $\mathbf{R}^2$ whose area is greater than the area of Λ. Then there are points $\mathbf{u}$, $\mathbf{v} \in \mathcal{X}$ with $\mathbf{u} \neq \mathbf{v}$ but $\mathbf{u} - \mathbf{v} \in \Lambda$.*

Proof Let $\mathbf{u}_1$ and $\mathbf{u}_2$ be generators for Λ and consider the fundamental region $\mathcal{F}$ associated to $\mathbf{u}_1$ and $\mathbf{u}_2$. Lemma 6.2 says essentially that the plane is tiled by translates of $\mathcal{F}$ by elements of Λ. More precisely $\mathbf{R}^2$ is the disjoint union of the sets

$$\mathbf{a} + \mathcal{F} = \{\mathbf{a} + \mathbf{t} : \mathbf{t} \in \mathcal{F}\}$$

for $\mathbf{a} \in \Lambda$. The set $\mathcal{X}$ is bounded and so meets only finitely many of these $\mathbf{a} + \mathcal{F}$. Also

$$\mathcal{X} = \bigcup_{\mathbf{a} \in \Lambda} (\mathbf{a} + \mathcal{F}) \cap \mathcal{X}$$

is a disjoint union. Hence

$$\text{area}(\mathcal{X}) = \sum_{\mathbf{a} \in \Lambda} \text{area}((\mathbf{a} + \mathcal{F}) \cap \mathcal{X})$$

where only a finite number of terms in the sum are nonzero. Consider the set $(\mathbf{a} + \mathcal{F}) \cap \mathcal{A}$. Its elements are $\mathbf{a} + \mathbf{t}$ where $\mathbf{t} \in \mathcal{F}$ and $\mathbf{t} \in \{\mathbf{x} - \mathbf{a} : \mathbf{x} \in \mathcal{X}\} = \mathcal{X} - \mathbf{a}$ using the obvious notation. Hence

$$(\mathbf{a} + \mathcal{F}) \cap \mathcal{A} = \mathbf{a} + (\mathcal{F} \cap (\mathcal{X} - \mathbf{a}))$$

and clearly

$$\text{area}((\mathbf{a} + \mathcal{F}) \cap \mathcal{A}) = \text{area}(\mathcal{F} \cap (\mathcal{X} - \mathbf{a})).$$

Thus

$$\text{area}(\mathcal{X}) = \sum_{\mathbf{a} \in \Lambda} \text{area}(\mathcal{F} \cap (\mathcal{X} - \mathbf{a})).$$

As $\text{area}(\mathcal{X}) > \text{area}(\mathcal{F})$ by hypothesis, the sets $\mathcal{F} \cap (\mathcal{X} - \mathbf{a}))$ cannot all be disjoint, for then

$$\sum_{\mathbf{a} \in \Lambda} \text{area}(\mathcal{F} \cap (\mathcal{X} - \mathbf{a})) = \text{area}\left(\bigcup_{\mathbf{a} \in \Lambda} \mathcal{F} \cap (\mathcal{X} - \mathbf{a}) \right) \leq \text{area}(\mathcal{F})$$

as this union is a subset of $\mathcal{F}$. Hence there exist $\mathbf{a}$, $\mathbf{b} \in \Lambda$ with $\mathbf{a} \neq \mathbf{b}$ but $(\mathcal{F} \cap (\mathcal{X} - \mathbf{a})) \cap (\mathcal{F} \cap (\mathcal{X} - \mathbf{b})) \neq \emptyset$. Thus there is $\mathbf{x} \in \mathcal{F}$ with $\mathbf{x} + \mathbf{a} \in \mathcal{X}$ and $\mathbf{x} + \mathbf{b} \in \mathcal{X}$. If we let $\mathbf{u} = \mathbf{x} + \mathbf{a}$ and $\mathbf{v} = \mathbf{x} + \mathbf{b}$ we get $\mathbf{u}$, $\mathbf{v} \in \mathcal{X}$, $\mathbf{u} \neq \mathbf{v}$, and $\mathbf{u} - \mathbf{v} = \mathbf{a} - \mathbf{b} \in \Lambda$. □

We can now prove the the theorem of Minkowski which has a host of applications to algebraic number theory. First one definition: a subset $\mathcal{X}$ of $\mathbf{R}^2$ is *symmetric* if $\mathbf{x} \in \mathcal{X}$ implies $-\mathbf{x} \in \mathcal{X}$.

Theorem 6.1 (Minkowski) *Let Λ be a lattice in $\mathbf{R}^2$ and $\mathcal{X}$ be a bounded convex symmetric subset of $\mathbf{R}^2$. If $\text{area}(\mathcal{X}) > 4\,\text{area}(\Lambda)$ then there exists a nonzero $\mathbf{a} \in \Lambda \cap \mathcal{X}$.*

Proof Consider $\frac{1}{2}\mathcal{X} = \{\frac{1}{2}\mathbf{c} : \mathbf{x} \in \mathcal{X}\}$. Then $\text{area}(\frac{1}{2}\mathcal{X}) = \frac{1}{4}\text{area}(\mathcal{X}) > \text{area}(\Lambda)$ by hypothesis. Also $\frac{1}{2}\mathcal{X}$ is bounded. By Lemma 6.4 there exist $\mathbf{u}$, $\mathbf{v} \in \frac{1}{2}\mathcal{X}$ with $\mathbf{a} = \mathbf{u} - \mathbf{v} \in \Lambda$ and $\mathbf{a} \neq 0$. Now

$$\mathbf{a} = \frac{(2\mathbf{u} + (-2\mathbf{v}))}{2}$$

is the midpoint of the segment joining $2\mathbf{u}$ to $-2\mathbf{v}$. Now $2\mathbf{u}$, $2\mathbf{v} \in \mathcal{X}$ and as $\mathcal{X}$ is symmetric, $-2\mathbf{v} \in \mathcal{X}$. By convexity then $\mathbf{a} \in \mathcal{X}$. As $\mathbf{a} \in \Lambda$ and $\mathbf{a} \neq 0$ the theorem follows. □

We shall apply Minkowski's theorem to $\Lambda = \bar{\sigma}(\mathcal{O}_K)$ for quadratic fields K, and more generally to $\Lambda = \bar{\sigma}(I)$ for ideals I of $\mathcal{O}_K$. We first need to calculate the areas of these lattices. First we calculate $\text{area}(\bar{\sigma}(\mathcal{O}_K))$.

Lemma 6.5 *Let K be a quadratic field of discriminant Δ. Then*

$$\text{area}(\bar{\sigma}(\mathcal{O}_K)) = \begin{cases} \sqrt{\Delta} & \text{if } \Delta > 0, \\ \frac{1}{2}\sqrt{|\Delta|} & \text{if } \Delta < 0. \end{cases}$$

Proof Let $K = \mathbf{Q}(\sqrt{m})$ where m is a squarefree integer. We split into four cases according to the sign of m and whether m is congruent to 1 modulo 4 or not.

Suppose that $m > 0$ and $m \not\equiv 1 \pmod 4$. Then $\Delta = 4m$ and $\mathcal{O}_K = \mathbf{Z}[\sqrt{m}]$. Then $\mathbf{u}_1 = \bar{\sigma}(1) = (1, 1)$ and $\mathbf{u}_2 = \bar{\sigma}(\sqrt{m}) = (\sqrt{m}, -\sqrt{m})$ are generators of $\bar{\sigma}(\mathcal{O}_K)$. Then $\text{area}(\bar{\sigma}(\mathcal{O}_K)) = |\det(U)|$ where U has rows $\mathbf{u}_1$ and $\mathbf{u}_2$. We calculate $\det(U) = -2\sqrt{m}$ and so $\text{area}(\bar{\sigma}(\mathcal{O}_K)) = 2\sqrt{m} = \sqrt{\Delta}$.

Now suppose that $m > 0$ and $m \equiv 1 \pmod 4$. Then $\Delta = m$ and $\mathcal{O}_K = \mathbf{Z}[\frac{1}{2}(1 + \sqrt{m})]$. Then we can take $\mathbf{u}_1 = \bar{\sigma}(1) = (1, 1)$ and $\mathbf{u}_2 = \bar{\sigma}(\sqrt{m}) = (\frac{1}{2}(1+\sqrt{m}), \frac{1}{2}(1-\sqrt{m}))$, and we find that $\det(U) = -\sqrt{m}$. Hence again $\text{area}(\bar{\sigma}(\mathcal{O}_K)) = \sqrt{m} = \sqrt{\Delta}$.

Now consider the case where $m < 0$ and $m \not\equiv 1 \pmod 4$. Then $|\Delta| = 4|m|$ and $\mathcal{O}_K = \mathbf{Z}[\sqrt{m}]$. Here we need to identify $\mathbf{C}$ with $\mathbf{R}^2$ by identifying $x + iy$ with (x, y). Then $\mathbf{u}_1 = \bar{\sigma}(1) = 1 = (1, 0)$ and $\mathbf{u}_2 = \bar{\sigma}(\sqrt{m}) = i\sqrt{|m|} = (0, \sqrt{|m|})$ are generators of $\bar{\sigma}(\mathcal{O}_K)$. It is immediate that $\det(U) = \sqrt{|m|}$ and so so $\text{area}(\bar{\sigma}(\mathcal{O}_K)) = \sqrt{m} = \frac{1}{2}\sqrt{\Delta}$.

Finally suppose that $m < 0$ and $m \equiv 1 \pmod 4$. Then $|\Delta| = |m|$ and $\mathcal{O}_K = \mathbf{Z}[\frac{1}{2}(1+\sqrt{m})]$. Then $\mathbf{u}_1 = \bar{\sigma}(1) = 1 = (1, 0)$ and $\mathbf{u}_2 = \bar{\sigma}(\frac{1}{2}(1+\sqrt{m})) = \frac{1}{2}(1+i\sqrt{|m|}) = (\frac{1}{2}, \frac{1}{2}\sqrt{|m|})$ are generators of $\bar{\sigma}(\mathcal{O}_K)$. Then $\det(U) = \frac{1}{2}\sqrt{|m|}$ and so so $\text{area}(\bar{\sigma}(\mathcal{O}_K)) = \frac{1}{2}\sqrt{m} = \frac{1}{2}\sqrt{\Delta}$. □

Now we calculate $\text{area}(\bar{\sigma}(I))$.

Lemma 6.6 *Let K be a quadratic field and I a nonzero ideal of $\mathcal{O}_K$. Then* $\text{area}(\bar{\sigma}(I)) = N(I)\text{area}(\bar{\sigma}(\mathcal{O}_K))$.

Proof Let β_1, β_2 form an integral basis of $\mathcal{O}_K$ and let γ_1, γ_2 form an integral basis of I. Then $\gamma_j = a_{j1}\beta_1 + a_{j2}\beta_2$ where the $a_{jk} \in \mathbf{Z}$. Then $N(I) = |\mathcal{O}_K : I| = |\det(A)|$ where A is the 2-by-2 matrix with entries a_{jk} by Proposition A.4. Let $\mathbf{u}_j = \bar{\sigma}(\beta_j)$ and $\mathbf{v}_j = \bar{\sigma}(\gamma_j)$ $(j = 1, 2)$. Let $\mathcal{F}$ and

$\mathcal{F}'$ be the fundamental regions of $\bar{\sigma}(\mathcal{O}_K)$ and $\bar{\sigma}(I)$ respectively corresponding to these generators. Then $\mathcal{F}' = \phi(\mathcal{F})$ where ϕ is the linear transformation with matrix A. Hence $\text{area}(\mathcal{F}') = |\det(A)|\text{area}(\mathcal{F})$ which gives $\text{area}(\bar{\sigma}(I)) = N(I)\text{area}(\bar{\sigma}(\mathcal{O}_K))$. □

We now apply this to prove a major theorem of Minkowski. We define the *Minkowski bound* M_K of a number field as follows. Write $K = \mathbf{Q}(\alpha)$ where α has degree n. Consider the conjugates $\alpha_1, \ldots, \alpha_n$ of α. Let s denote the number of α_j which are real. Since $\overline{\alpha}_j$ is also a conjugate of α for each j, the nonreal conjugates come in pairs. Hence there are $2t$ nonreal conjugates of α and $s + 2t = n$. The Minkowski bound of K is

$$M_K = \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta_K|}$$

where Δ_K denotes the discriminant of K. In particular when K is real quadratic then $M_K = \frac{1}{2}\sqrt{\Delta_K}$ and when K is imaginary quadratic then $M_K = \frac{2}{\pi}\sqrt{|\Delta_K|}$.

The following theorem is valid for all number fields, but we state and prove it only for quadratic fields.

Theorem 6.2 (Minkowski) *Let K be a quadratic field. Each ideal class of K contains an ideal I of $\mathcal{O}_K$ with $N(I) \leq M_K$.*

Proof First take any nonzero ideal J of $\mathcal{O}_K$. Let $\Lambda = \bar{\sigma}(J)$. We shall apply Minkowski's theorem 6.1 to Λ and a suitable region $\mathcal{X}$. To define $\mathcal{X}$ we split into the cases of K real and K imaginary.

First suppose that K is imaginary. Let c be any positive number, and let $\mathcal{X}$ be the interior of the circle radius c centred at the origin. Note that the interior of a circle is convex; also $\mathcal{X}$ is symmetric. By Lemmas 6.5 and 6.6, $\text{area}(\Lambda) = \frac{1}{2}N(J)\sqrt{|\Delta_K|}$. The area of $\mathcal{X}$ is πc^2. If $\text{area}(\mathcal{X}) > 4\,\text{area}(\Lambda)$, that is, if $\pi c^2 > 2N(J)\sqrt{|\Delta_K|}$ then there is a nonzero $\mathbf{a} \in \Lambda \cap \mathcal{X}$ by Theorem 6.1. Then $\mathbf{a} = \bar{\sigma}(\beta)$ with $\beta \in J$ and $|\beta| < c$. Hence $0 < N(\beta) < c^2$. Hence if $c^2 > \frac{2}{\pi}N(J)\sqrt{|\Delta_K|} = M_K N(J)$ then there exists a nonzero $\beta \in J$ with $N(\beta) < c^2$. If γ is a nonzero element of J with $N(\gamma)$ as small as possible, then $N(\gamma) < c^2$ for all $c^2 > M_K N(J)$. Hence $N(\gamma) \leq M_K N(J)$. Now by Proposition 5.2 each ideal class of K contains an ideal I with $N(I) \leq M_K$.

The argument when K is real is similar. Again let c be any positive number. Then let

$$\mathcal{X} = \{(x, y) : |x| + |y| < c\}.$$

Then $\mathcal{X}$ is the interior of a square with vertices $(\pm c, 0)$ and $(0, \pm c)$. Again, note that the interior of a square is convex; also $\mathcal{X}$ is symmetric. This time,

by Lemmas 6.5 and 6.6, $\text{area}(\Lambda) = N(J)\sqrt{|\Delta_K|}$. The area of $\mathcal{X}$ is $2c^2$ as the side of the square has length $\sqrt{2}c$. If $\text{area}(\mathcal{X}) > 4\,\text{area}(\Lambda)$, that is, if $2c^2 > 4N(J)\sqrt{|\Delta_K|}$ then there is a nonzero $\mathbf{a} \in \Lambda \cap \mathcal{X}$ by Theorem 6.1. Then $\mathbf{a} = \bar{\sigma}(\beta) = (\beta, \sigma_2(\beta))$ with $\beta \in J$. Now

$$|\beta| + |\sigma_2(\beta)| < c$$

and $|N(\beta)| = |\beta||\sigma_2(\beta)|$. By the inequality of the arithmetic and geometric means,

$$\frac{|\beta| + |\sigma_2(\beta)|}{2} \geq \sqrt{|\beta||\sigma_2(\beta)|}$$

and so

$$\sqrt{|N(\beta)|} < c/2.$$

Hence $0 < |N(\beta)| < c^2/4$. Hence if $c^2 > 2\pi N(J)\sqrt{|\Delta_K|} = 4M_K N(J)$ then there exists a nonzero $\beta \in J$ with $N(\beta) < c^2/4$. If γ is a nonzero element of J with $|N(\gamma)|$ as small as possible, then $|N(\gamma)| < c^2/4$ for all $c^2/4 > M_K N(J)$. Hence $|N(\gamma)| \leq M_K N(J)$. Again by Proposition 5.2 each ideal class of K contains an ideal I with $N(I) \leq M_K$. □

We can now compute class-groups more efficiently.

Example Let $K = \mathbf{Q}(\sqrt{-6})$. Then $\Delta_K = \frac{2}{\pi}\sqrt{24} \approx 3 \cdot 1$ so that Cl_K is generated by the prime ideals of norm at most 3. We have seen that the only such ideals are $P_2 = \left\langle 2, \sqrt{-6}\right\rangle$ and $P_3 = \left\langle 3, \sqrt{-6}\right\rangle$, that P_2 is not principal, but that P_2^2, P_2P_3 and P_3^2 all are. Then it is easy to see that the class-number is 2. This took a great deal less effort than our previous computation!

Example Let $K = \mathbf{Q}(\sqrt{-47})$. Then $\Delta_K = -47$ and $\mathcal{O}_K = \mathbf{Z}[\tau]$ where $\tau = \frac{1}{2}(1 + \sqrt{-47})$ and τ has minimum polynomial $f(X) = X^2 - X + 12$. We have $M_K = \frac{2}{\pi}\sqrt{47} \approx 4 \cdot 4$ so that the class-group is generated by the prime ideals of norm at most 4. We now need to find the prime ideal factors of $\langle 2\rangle$ and $\langle 3\rangle$. As

$$f(X) \equiv X^2 - X = X(X-1) \pmod 2$$

and

$$f(X) \equiv X^2 - X = X(X-1) \pmod 3$$

then $\langle 2\rangle = P_2Q_2$ and $\langle 3\rangle = P_3Q_3$ where $P_2 = \langle 2, \tau\rangle$, $Q_2 = \langle 2, \tau - 1\rangle$, $P_3 = \langle 3, \tau\rangle$ and $Q_3 = \langle 3, \tau - 1\rangle$. Naturally $[Q_2] = [P_2]^{-1}$ and $[Q_3] = [P_3]^{-1}$, and we attempt to find relations between $[P_2]$ and $[P_3]$ by considering principal ideals of small norm. First of all $N(\tau) = 12$. Also $\tau \in P_2$ and $\tau \in P_3$ so that $P_2P_3 \supseteq \langle\tau\rangle$. Hence either $\langle\tau\rangle = P_2^2P_3$ or $P_2Q_2P_3$ but the latter is impossible as $\langle 2\rangle = P_2Q_2 \supseteq P_2Q_2P_3$ but $2 \nmid \tau$. Hence $\langle\tau\rangle = P_2^2P_3$ and so $[P_3] = [P_2]^{-2}$. It follows that Cl_K is generated by $[P_2]$. If we try $\tau + 1 = \frac{1}{2}(3 + \sqrt{-47})$

then $N(\tau+1)=14$ so $\langle\tau+1\rangle$ has a prime ideal factor of norm 7, which we haven't considered. We get better luck with $\tau+2=\frac{1}{2}(5+\sqrt{-47})$. This time $N(\tau+2)=18$. Also $\tau+2\in P_2$ and $\tau+2=(\tau-1)+3\in Q_3$ and so $\langle\tau+2\rangle=P_2P_3Q_3$ or $P_2Q_3^2$. The former is impossible as $P_3Q_3=\langle 3\rangle$ does not divide $\langle\tau+2\rangle$. Hence $\langle\tau+2\rangle=P_2Q_3^2$ and

$$[P_2]=[Q_3]^{-2}=[P_3]^2=[P_2]^{-4}$$

so that $[P_2]^5=[\langle 1\rangle]$.

We have not determined whether P_2 is principal or not. If P_2 is principal—$P_2=\langle\gamma\rangle$ where $\gamma=\frac{1}{2}(b+c\sqrt{-47})$ with $b,\,c\in\mathbf{Z}$—then $N(\gamma)=2$. Hence $b^2+47c^2=8$ and it is apparent that there are no solutions in integers to this equation. Hence $[P_2]=[\langle 1\rangle]$ and so $[P_2]$ has order 5 in the class-group. The class-number of K is 5.

It is an instructive exercise to find generators for the principal ideals P_2^5, Q_2^5, P_3^5 and Q_3^5.

We finish this section by showing that $U(\mathcal{O}_K)$ is an infinite group whenever K is a real quadratic field. We first show that there are arbitrarily large numbers in $\mathcal{O}_K$ with small norm.

Lemma 6.7 *Let K be a real quadratic field with discriminant Δ. Let A be any positive number with $A>\sqrt{|\Delta|}$. Then for each positive number M, there exists $\beta\in\mathcal{O}_K$ with $\beta>M$ and $|N(\beta)|<A$.*

Proof Apply Minkowski's theorem 6.1 to the following set

$$\mathcal{X}=\{(x,y):|x|<AM,|y|<1/M\}.$$

Then $\mathcal{X}$ is a convex symmetric set (the interior of a rectangle centred at the origin) with area $4A$. But $\bar{\sigma}(\mathcal{O}_K)$ has area $\sqrt{\Delta}$ by Lemma 6.5. Thus $\text{area}(\mathcal{X})>4\,\text{area}(\bar{\sigma}(\mathcal{O}_K))$ and so by Theorem 6.1 there exists a nonzero $\beta\in\mathcal{O}_K$ with $\bar{\sigma}(\beta)\in\mathcal{X}$. By replacing β by $-\beta$ if necessary, we may assume that $\beta>0$. Now $\bar{\sigma}(\beta)=(\beta,\sigma_2(\beta))$ and $N(\beta)=\beta\sigma_2(\beta)$. As $|\sigma_2(\beta)|<1/M$ and $|N(\beta)|\geq 1$ then $|\beta|>M$. □

We can now show that $\mathcal{O}_K$ has a unit $\xi>1$.

Proposition 6.1 *Let K be a real quadratic field. There exists $\xi\in U(\mathcal{O}_K)$ with $\xi>1$.*

Proof Let A be any number satisfying the conditions of Lemma 6.7. Define a sequence $\beta_0,\beta_1,\beta_2,\ldots$ of elements of $\mathcal{O}_K$ as follows. Let $\beta_0=1$. Suppose that β_n has been defined. Then choose β_{n+1} to be some number in $\mathcal{O}_K$

with $\beta_{n+1} > \beta_n$ and $|N(\beta_{n+1})| < A$. Consider the ideals $\langle\beta_0\rangle, \langle\beta_1\rangle, \langle\beta_2\rangle, \ldots$. Each of these ideals has norm less than A, and so by Lemma 4.10 only a finite number of different ideals can occur. Hence there exist $j < k$ with $\langle\beta_j\rangle = \langle\beta_k\rangle$. Thus $\beta_k = \xi\beta_j$ where $\xi \in U(\mathcal{O}_K)$, and $\xi > 1$ as $\beta_k > \beta_j$. □

In fact the structure of the unit group of $\mathcal{O}_K$ is easy to determine.

Theorem 6.3 *Let K be a real quadratic field. There exists $\eta \in \mathcal{O}_K$ such that $\eta > 1$ and such that every unit in $\mathcal{O}_K$ has the form $\pm\eta^j$ where $j \in \mathbf{Z}$.*

Proof By Proposition 6.1 there exists $\xi \in U(\mathcal{O}_K)$ with $\xi > 1$. I claim that there are only finitely many units ε in $\mathcal{O}_K$ with $1 < \varepsilon \leq \xi$. For such an ε, $1/\varepsilon \in \mathcal{O}_K$. Let $\varepsilon = \frac{1}{2}(a+b\sqrt{m})$ where a, b, $m \in \mathbf{Z}$, then $1/\varepsilon = \pm\frac{1}{2}(a-b\sqrt{m})$. Consequently $a = \varepsilon \pm 1/\varepsilon$. As $0 < 1/\varepsilon < 1$ then $0 < a < \xi + 1$. There are only a finite number of possibilities for a, and as a determines b up to sign, only finitely many possibilities for ε.

We let η be the smallest unit with $1 < \eta \leq \xi$; this exists as there is at least one such unit, namely ξ, and there are only finitely many such units. Then there are no units ε with $1 < \varepsilon < \eta$. Let δ be any unit. Consider $\log|\delta|$. There exists an integer j such that

$$j\log\eta \leq \log|\delta| < (j+1)\log\eta$$

and so

$$0 \leq \log|\delta|\eta^{-j} < \log\eta.$$

Now $|\delta|\eta^{-j}$ is a unit and $1 \leq |\delta|\eta^{-j} < \eta$. Thus $|\delta|\eta^{-j} = 1$ and so $\delta = \pm\eta^j$. □

It is easily seen that the unit η in this theorem is uniquely determined by the field K, as it is called the *fundamental unit* of K.

Example Let $K = \mathbf{Q}(\sqrt{2})$. Then $\eta = 1+\sqrt{2}$ is a unit in $\mathcal{O}_K$, and obviously $\eta > 1$. I claim that it is the fundamental unit. If it were not, then there would be a unit $\xi = a + b\sqrt{2}$ of $\mathcal{O}_K$ with $1 < \xi < \eta$. Now $1/\xi = \pm(a - b\sqrt{2})$ and so $2a = \xi \pm 1/\xi$. As $0 < 1/\xi < 1$ then $0 < 2a < \eta + 1 = 2 + \sqrt{2} < 5$. Thus $a = 1$ or 2. Of course $a = 1$ gives $b = \pm 1$ and for $\xi > 1$ we need $b = 1$, that is $\xi = \eta$ which is false. But $a = 2$ gives $4 - 2b^2 = \pm 1$ which is impossible. Thus η is the fundamental unit.

We shall not give details on how to find the fundamental unit. If $\xi = a + b\sqrt{m}$ with a, $b \in \mathbf{Z}$ then ξ is a unit if and only if

$$a^2 - mb^2 = 1. \qquad (*)$$

The equation $(*)$ is called *Pell's equation* and methods for finding its solution using continued fractions can be found in texts on elementary number theory.

Of course, not all units are of this form, but for any given unit ξ, ξ^6 does have this form and so these methods can be used to determine the fundamental unit of a given real quadratic field.

Example The method of solving Pell's equation shows that the first non-trivial solution of

$$a^2 - 61b^2 = 1$$

is

$$a = 1766319049, \quad b = 226153980.$$

Thus the smallest unit of the form $\xi = a + b\sqrt{61}$ with a, $b \in \mathbf{Z}$ $\xi > 1$ and $N(\xi) = 1$ is

$$1766319049 + 226153980\sqrt{61}.$$

However, this is not the fundamental unit of $\mathbf{Q}(\sqrt{61})$, since we find

$$\xi^{1/2} = 29718 + 3805\sqrt{61}$$

which is a unit of norm -1. Again, this is still not the fundamental unit. Since $61 \equiv 1 \pmod 4$ the ring of integers of $\mathbf{Q}(\sqrt{61})$ is $\mathbf{Z}[\frac{1}{2}(1 + \sqrt{61})]$ and there may be units of $\sqrt{61}$ of the form $\frac{1}{2}(c+d\sqrt{61})$ with c and d odd integers. Indeed we find that

$$\eta = \xi^{1/6} = (\xi^{1/2})^{1/3} = \frac{39 + 5\sqrt{61}}{2}.$$

Now it is not hard to check that η really is the fundamental unit of this quadratic field.

In general given $K = \mathbf{Q}(\sqrt{m})$ with m positive and squarefree, the size of the fundamental unit varies very irregularly with m; some fields have small fundamental units, while others have astronomical fundamental units.

A Appendix

A.1 Polynomials

If R is a (commutative) ring then $R[X]$ denotes the ring of polynomials in the variable X with coefficients in R. If $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ with $a_n \neq 0$ then n is the *degree* of f, a_n is the *leading coefficient* of f and a_nX^n is the *leading term* of f. The degree of f is denoted $\deg(f)$. These concepts are not defined for the zero polynomial. A *monic* polynomial is one whose leading coefficient is 1.

If R is an integral domain, then $\deg(fg) = \deg(f) + \deg(g)$ whenever f and g are nonzero elements of $R[X]$. In particular $fg \neq 0$ and so $R[X]$ is also an integral domain.

Proposition A.1 (The division algorithm) *Let K be a field, and let f, $g \in K[X]$ with $g \neq 0$. There exist unique q, $r \in K[X]$ with*

- *$f = gq + r$, and*
- *either $r = 0$ or $\deg(r) < \deg(g)$.* □

Let f, $g \in K[X]$. We say that *f divides g* (or *g is divisible by f*) if $g = fh$ for some $h \in K[X]$.

Proposition A.2 (Greatest common divisors) *Let K be a field, and let f and g be nonzero elements of $K[X]$. There is a unique monic polynomial h such that*

- *$h \mid f$ and $h \mid g$*
- *if $q \in K[X]$ and $q \mid f$ and $q \mid g$ then $q \mid h$.*

In addition there exist u, $v \in K[X]$ with $h = uf + vg$. □

Let K be a field and $f \in K[X]$ have positive degree. We say that f is *irreducible* over K if there are no g, $h \in K[X]$ with $f = gh$ and $\deg(g)$, $\deg(h) < \deg(f)$.

Theorem A.1 (Unique factorization) *Let K be a field and let $f \in K[X]$ be a monic polynomial of positive degree. Then there are monic polynomials $p_1, p_2, \ldots, p_k \in K[X]$, each irreducible over K, such that $f = p_1p_2 \cdots p_k$. Furthermore the p_j are determined, up to order, uniquely by f.* □

A.2 Symmetric polynomials

Let R be a ring. Then $R[T_1, \ldots, T_k]$ denotes the ring of polynomials in the n indeterminates $T_1, \ldots, T_k$ with coefficients in R. (In our applications R will usually be $\mathbf{Z}$ or $\mathbf{Q}$ so you may think of R as being one of these rings if you prefer). A polynomial $f \in R[T_1, \ldots, T_n]$ is *symmetric* if it is left invariant under any permutation of the indeterminates. More precisely f is symmetric if

$$f(T_1, T_2, \ldots, T_n) = f(T_{\sigma(1)}, T_{\sigma(2)}, \ldots, T_{\sigma(n)})$$

for all permutations σ in the symmetric group S_n.

For example when $n = 3$,

$$f_1(T_1, T_2, T_3) = T_1^2T_2 + T_1^2T_3 + T_2^2T_1 + T_2^2T_3 + T_3^2T_1 + T_3^2T_2$$

is symmetric since

$$\begin{aligned} & f_1(T_1, T_2, T_3) = f_1(T_1, T_3, T_2) = f_1(T_2, T_1, T_3) \\ = \; & f_1(T_2, T_3, T_1) = f_1(T_3, T_1, T_2) = f_1(T_3, T_2, T_1) \end{aligned}$$

but

$$f_2(T_1, T_2, T_3) = T_1^2T_2 + T_2^2T_3 + T_3^2T_1$$

is not symmetric, as although $f_2(T_1, T_2, T_3) = f_2(T_2, T_3, T_1) = f_2(T_3, T_1, T_2)$ we have

$$f_2(T_1, T_3, T_2) = T_1^2T_3 + T_2^2T_1 + T_3^2T_2 \neq f_2(T_1, T_2, T_3).$$

The *elementary symmetric functions* are defined as follows. Write

$$(X + T_1)(X + T_2) \cdots (X + T_n) = X^n + \sum_{r=1}^{n} e_r(T_1, T_2, \ldots, T_n)X^{n-r}.$$

Then

$$e_r(T_1, T_2, \ldots, T_n) = \sum_{1 \leq j_1 < j_2 < \cdots < j_r \leq n} T_{j_1}T_{j_2} \cdots T_{j_r}$$

is the sum of the $\binom{n}{r}$ products of r distinct T_j. For instance

$$e_1(T_1, T_2, \ldots, T_n) = T_1 + T_2 + \cdots + T_n,$$

$$e_2(T_1, T_2, \ldots, T_n) = T_1T_2 + T_1T_3 + \cdots + T_1T_n + T_2T_3 + \cdots + T_{n-1}T_n$$

and

$$e_n(T_1, T_2, \ldots, T_n) = T_1T_2 \cdots T_n.$$

Each symmetric function can be expressed in terms of elementary symmetric polynomials.

Theorem A.2 (Newton) *Let R be a ring, and let $f \in R[T_1, \ldots, T_n]$ be a symmetric polynomial. Then there is a polynomial $g \in R[X_1, \ldots, X_n]$ with the property that*

$$f(T_1, \ldots, T_n) = g(E_1, \ldots, E_n)$$

where E_r denotes $e_r(T_1, \ldots, T_n)$.

Proof (outline) Order the terms of f "lexicographically", that is write the term $aT_1^{i_1} \cdots T_n^{i_n}$ ahead of $bT_1^{j_1} \cdots T_n^{j_n}$ when $i_k > j_k$ for the least k where $i_k \neq j_k$. Let $aT_1^{i_1} \cdots T_n^{i_n}$ be the first term of f in lexicographic ordering. Then since $aT_{\sigma(1)}^{i_1} \cdots T_{\sigma(n)}^{i_n}$ is also a term in f, as f is symmetric, we have $i_1 \geq i_2 \geq \cdots \geq i_n$. But also $aT_1^{i_1} \cdots T_n^{i_n}$ is the first term of $h_1 = aE_1^{i_1 - i_2} E_2^{i_2 - i_3} \cdots E_{n-1}^{i_{n-1} - i_n} E_n^{i_n}$ in lexicographical order. Then either $f - h_1$ is zero, or its first term is later than $aT_1^{i_1} \cdots T_n^{i_n}$ in lexicographical ordering. Repeating this argument for $h - h_1$ then yields h_2, a monomial expression in the E_j, with either $f - h_1 - h_2 = 0$ or $f - h_1 - h_2 = 0$ having first term even later in the lexicographical ordering. Eventually we get $f = h_1 + h_2 + \cdots + h_k$ where each h_i is a monomial in the E_j. □

Example The method of proof gives an algorithm that computes g given f. For instance let

$$f(T_1, T_2, T_3) = T_1^3 T_2 + T_1^3 T_3 + T_1 T_2^3 + T_1 T_3^3 + T_2^3 T_3 + T_2 T_3^3.$$

These terms have been written in lexicographic order. The first term $T_1^3 T_2$ is also the first term in

$$\begin{aligned} E_1^2 E_2 &= (T_1 + T_2 + T_3)^2 (T_1 T_2 + T_1 T_3 + T_2 T_3) \\ &= T_1^3 T_2 + T_1^3 T_3 + 2T_1^2 T_2^2 + 5T_1^2 T_2 T_3 + 2T_1^2 T_3^2 + T_1 T_2^3 \\ &\quad + 5T_1 T_2^2 T_3 + 5T_1 T_2 T_3^2 + T_1 T_3^3 + T_2^3 T_3 + 2T_2^2 T_3^2 + T_2 T_3^3. \end{aligned}$$

Then

$$f - E_1^2 E_2 = -2T_1^2 T_2^2 - 5T_1^2 T_2 T_3 - 2T_1^2 T_3^2 - 5T_1 T_2^2 T_3 - 5T_1 T_2 T_3^2 - 2T_2^2 T_3^2.$$

The first term of this is $-2T_1^2 T_2^2$ which is the same as that of

$$-2E_2^2 = -2T_1^2 T_2^2 - 4T_1^2 T_2 T_3 - 2T_1^2 T_3^2 - 4T_1 T_2^2 T_3 - 4T_1 T_2 T_3^2 - 2T_2^2 T_3^2.$$

Then

$$f - E_1^2 E_2 + 2E_2^2 = -T_1^2 T_2 T_3 - T_1 T_2^2 T_3 - T_1 T_2 T_3^2.$$

The first term of this expression agrees with that of

$$f - E_1 E_3 = -T_1^2 T_2 T_3 - T_1 T_2^2 T_3 - T_1 T_2 T_3^2$$

and so $f = E_1^2 E_2 - 2E_2^2 - E_1 E_3$.

A.3 Free abelian groups

In this section all groups are written with addition as the operation. Naturally, the identity element of each of our groups will be denoted as 0 and the inverse of an element u as $-u$.

The set $\mathbf{Z}^n$ of all n-tuples of integers will be our main example. Its elements are row vectors of integers and it forms a group under vector addition. A group G is called a *free abelian group of rank* n if it is isomorphic to $\mathbf{Z}^n$. This means that G has an *integral basis* or $\mathbf{Z}$*-basis*: there is a sequence $u_1, \ldots, u_n$ of elements of G such that each element of G can be **uniquely** expressed in the form $a_1u_1 + \cdots + a_nu_n$ with $a_1, \ldots, a_n \in \mathbf{Z}$.

The rank of a free abelian group is uniquely determined. Each abelian group G has a subgroup $2G = \{u + u : u \in G\}$ and when G is free abelian of rank n, then the index $|G : 2G| = 2^n$.

We wish to show that each subgroup of a free abelian group G is also a free abelian group. It suffices to prove this for $G = \mathbf{Z}^n$. To warm up, consider the case where $n = 1$. If H is a subgroup of $\mathbf{Z}$ then either $H = \{0\}$ or H contains some positive number. The group $\{0\}$ is free abelian of rank 0, but if $H \neq \{0\}$ let b be the smallest positive integer in H. Then b (on its own) forms an integral basis of H. For if $c \in H$ there is $a \in \mathbf{Z}$ with $0 \leq c - ab < b$. Then as $c - ab \in H$ we must have $c - ab = 0$. Thus $c = ab$ and $a = c/b$ is uniquely determined. We now consider the general result.

Proposition A.3 *Let G be a free abelian group of rank n, and let H be a subgroup of G. Then H is free abelian of rank m where $m \leq n$.*

Proof We may assume that $G = \mathbf{Z}^n$. We begin by defining various subgroups $H_1, \ldots, H_n$ of H. We let $H_1 = H$ and for $j > 1$ let

$$H_j = \{(0, 0, \ldots, 0, c_j, c_{j+1}, \ldots, c_n) : c_j, c_{j+1}, \ldots, c_n \in \mathbf{Z}\} \cap H.$$

That is H_j is the set of all vectors in H where the first $j - 1$ entries vanish. We also let

$$K_j = \{c_j : (0, 0, \ldots, 0, c_j, c_{j+1}, \ldots, c_n) \in H_j\}$$

for each j. That is, K_j is the set of j-th entries of vectors in H_j. It is easy to see that H_j is a subgroup of H (and so of $\mathbf{Z}^n$) and consequently that K_j is a subgroup of $\mathbf{Z}$. Then $J_j = \mathbf{Z}b_j = \{ab_j : a \in \mathbf{Z}\}$ for some integer b_j. Define vectors $u_1, \ldots, u_n \in H$ as follows. If $b_j = 0$ let u_j be the zero vector, otherwise let u_j be any vector in H_j whose j-th entry is b_j. We claim that those u_j which are nonzero form an integral basis of H. Given this claim, it is immediate that H is free abelian of rank m, where m is the number of nonzero u_j, and so $m \leq n$.

We first show that each element of H has the form $\sum_{j=1}^{n} a_j u_j$ with $u_j \in \mathbf{Z}$. To do this note that if $v = (0, \ldots, 0, c_j, \ldots, c_n) \in H_j$ then $c_j = a_j b_j$ with $a_j \in \mathbf{Z}$ and so $v - a_j u_j \in H_{j+1}$ if $j < n$ and $v - a_j u_j = 0$ if $j = n$. Start with any $v \in H = H_1$. Then there exists $a_1 \in \mathbf{Z}$ with $v - a_1 u_1 \in H_2$. Then there exists $a_2 \in \mathbf{Z}$ with $v - a_1 u_1 - a_2 u_2 \in H_3$ etc. Eventually we find $a_1, \ldots, a_n \in \mathbf{Z}$ with $v - a_1 u_1 - a_2 u_2 - \cdots - a_n u_n = 0$ so that $v = \sum_{j=1}^{n} a_j u_j$. In this sum we may discard the u_j which vanish, so each $v \in H$ is a linear combination, with integer coefficients, of the nonzero u_j.

We now show uniqueness. Define an n-by-n matrix U with the j-th row being u_j. Let u_{jk} denote the typical entry. Then U is upper-triangular: $u_{jk} = 0$ when $k < j$. Also $u_{jj} = b_j$ and the j-th row of U is zero whenever $u_{jj} = 0$. To show that H is free abelian we need to show that $v = \sum_{j=1}^{n} a_j u_j$ uniquely determine the a_j for the j where u_j is nonzero. We proceed by induction on j; suppose that a_k for the $k < j$ with $u_k \neq 0$ are uniquely determined by v. Then v uniquely determines $\sum_{k=1}^{j-1} a_k u_k$ and so also $v - \sum_{k=1}^{j-1} a_k u_k = a_j v_j + \sum_{r=j+1}^{n} a_j v_j$. But the j-th entry of this vector is $a_j b_j$, and as long as $b_j = 0$ this determines a_j uniquely. □

Example Let $n = 3$ and

$$H = \{(r, s, t) \in \mathbf{Z}^3 : 3r + 5s + 7t = 0 \text{ and } s \text{ is even}\}.$$

It is swiftly verified that H is a subgroup of $\mathbf{Z}^3$. Of course $H_1 = H$ and we find that $(1, -2, 1) \in H_1$. It follows that $K_1 = \mathbf{Z}$ and we may take $b_1 = 1$ and $u_1 = (1, -2, 1)$. Now

$$H_1 = \{(0, s, t) \in \mathbf{Z}^3 : 5s + 7t = 0 \text{ and } s \text{ is even}\}.$$

If $(0, s, t) \in H_2$ then s is even and $5s = -7t \equiv 0 \pmod 7$. It follows that $s \equiv 0 \pmod 7$ and so s is divisible by 14. Hence $K_2 \subseteq 14\mathbf{Z}$. But as $(0, 14, -10) \in H_2$, then $K_2 = 14\mathbf{Z}$ and we may take $b_2 = 14$ and $u_2 = (0, 14, -10)$. Finally

$$H_3 = \{(0, 0, t) \in \mathbf{Z}^3 : 7t = 0\} = \{(0, 0, 0)\}$$

so that $b_3 = 0$ and $u_3 = (0, 0, 0)$. It follows that H has rank 2 and that each element of H can be written uniquely as $a_1 u_1 + a_2 u_2$ for $a_1, a_2 \in \mathbf{Z}$.

For example $v = (19, 4, -11) \in H$. To have $v = a u_1 + v u_2$ we must have, on comparing the first coordinate, $19 = a_1$ so that $a_2 u_2 = v - 19 a_1 = (0, 42, -30)$. Thus $a_2 = 3$ so that $v = 19 u_1 + 3 u_2$.

In general given an integral basis $u_1, \ldots, u_m$ of a subgroup H of $\mathbf{Z}^n$, we define an m-by-n matrix U having the u_j as rows. We call U a *generator matrix* of H. In the language of matrix theory, this means that the elements

of H are the vectors $v = aU$ where $a \in \mathbf{Z}^m$, and that each $v \in H$ determines the vector a uniquely.

A square matrix is called *unimodular* if it has integer entries and determinant ± 1. Equivalently a matrix A is unimodular if it is nonsingular and both A and A^{-1} have integer entries.

Lemma A.1 *Let H be a subgroup of $\mathbf{Z}^n$ of rank m with generator matrix U. The m-by-n matrix V is also a generator matrix of M if and only if $V = AU$ where A is an m-by-m unimodular matrix.*

Proof Let V be a generator matrix of H. Let its rows be $v_1, \ldots, v_m$ while let the rows of U be $u_1, \ldots, u_m$. There are integers a_{jk} with $v_j = \sum_{k=1}^m a_{jk} u_k$. It follows that $V = AU$ where A is the matrix with entries a_{jk}. Similarly $U = BV$ where B is also a matrix with integer entries. Hence $U = BAU = CU$ where $C = BA$ has integer entries. We get $u_j = \sum_{k=1}^m c_{jk} u_k$ so that by uniqueness, $c_{jj} = 1$ and $c_{jk} = 0$ for $j \neq k$. Hence $C = BA = I$ and so A is unimodular.

Now let A be unimodular with inverse B, so that B also has integer entries. Let $V = AU$. Let $H' = \{wV : w \in \mathbf{Z}^m\}$ be the subgroup of $\mathbf{Z}^n$ generated by the rows of V. Then $wV = wAU \in H$ so that $H' \subseteq H$. Similarly if $w'U \in H$, then $w'U = w'BAUV = w'BV \in H'$ so that $H' = H$. If the rows of V did not form an integral basis then $wV = 0$ for some nonzero $w \in \mathbf{Z}^m$. Then $0 = wABV = wAU$ so that $wA = 0$. Consequently $w = wAB = 0$, a contradiction. □

In the case where $m = n$ the matrix U is square, and so has a determinant. This determinant has a group-theoretical interpretation.

Proposition A.4 *Let U be an n-by-n matrix with integer entries. The rows of U form an integral basis of a subgroup H of $\mathbf{Z}^n$ if and only if* $\det(U) \neq 0$. *In this case H has rank n and $|\mathbf{Z}^n : H| = |\det(U)|$.*

Proof If the matrix U is singular, then $xU = 0$ for some nonzero $x \in \mathbf{Q}^n$. By multiplying the vector x by the product of the denominators of its entries, we get a nonzero $y \in \mathbf{Z}^n$ with $yU = 0$. Then the rows of U cannot form an integral basis for any subgroup of $\mathbf{Z}^n$.

Suppose that U is nonsingular and let $H = \{xU : x \in \mathbf{Z}^n\}$. Then H is a subgroup of $\mathbf{Z}^n$ and the rows of u form an integral basis of H since $xU = 0$ implies $x = 0$ due to U's nonsingularity. Hence H is free abelian of rank n.

Now assume that U is nonsingular. Then H has a generating matrix V which is upper triangular by the proof of Proposition A.3. By Lemma A.1,

$V = AU$ with A unimodular, so that $\det(V) = \det(A)\det(U) = \pm\det(U)$. Let V have diagonal entries $b_1, \ldots, b_n$. Then I claim that the set of vectors

$$\mathcal{A} = \{(a_1, \ldots, a_n) : 0 \le a_j < |b_j|, \text{ for each } j\}$$

is a set of coset representatives for H in $\mathbf{Z}^n$. To prove this we need to show that each $x \in \mathbf{Z}^n$ is congruent modulo H to a unique $a \in \mathcal{A}$. Given such an x consider the first entry of $x - tv_1$ for $t \in \mathbf{Z}$. This entry equals $x_1 - tb_1$. There is a unique $t = t_1 \in \mathbf{Z}$ with $0 \le a_1 = x_1 - tb_1 < |b_1|$. Now consider $x - t_1v_1 - tv_2$. The first entry is still a_1, and there is a unique $t = t_2$ making the second entry a_2 satisfy $0 \le a_2 < b_2$. Proceeding in this manner we get unique $t_1, t_2, \ldots, t_n$ such that $a = x - \sum_{k=1}^{n} t_j v_j$ satisfy $0 \le a_j < |b_j|$ for each j. □

Example Suppose that $n = 3$ and H has the generator matrix

$$\begin{pmatrix} 3 & -2 & 1 \\ 0 & 4 & -3 \\ 0 & 0 & 5 \end{pmatrix}.$$

Let $x = (17, -11, 13)$. We wish to find integers t_1, t_2 and t_3 with $x - t_1v_1 - t_2v_2 - t_3v_3 = (a_1, a_2, a_3)$ and $0 \le a_1 < 3$, $0 \le a_2 < 4$ and $0 \le a_3 < 5$. Then $a_1 = 17 - 3t_1$ so that we must have $t_1 = 5$ and $a_1 = 2$. Then $x - t_1v_1 = (2, -1, 8)$. Then $a_2 = -1 - 4t_2$ so that we must have $t_2 = -1$ and $a_2 = 3$. Then $x - t_1v_1 - t_2v_2 = (2, 3, 5)$. Then $a_3 = 5 - 5t_3$ so that we must have $t_3 = 1$ and $a_3 = 0$. Thus $x - 5v_1 + v_2 - v_2 = (2, 3, 0) \in \mathcal{A}$, and these coefficients are uniquely determined.

Proposition A.4 implies that each rank n subgroup of $\mathbf{Z}^n$ has finite index. In fact the converse is true: each finite index subgroup of $\mathbf{Z}^n$ has rank n. Equivalently each subgroup of $\mathbf{Z}^n$ of rank less than n has infinite index.

Lemma A.2 *Let H be a rank m subgroup of $\mathbf{Z}^n$ with $m < n$. Then H has infinite index in $\mathbf{Z}^n$.*

Proof Take a generator matrix U for H. As it has m rows and $m < n$ its rows fail to span the $\mathbf{Q}$-vector space $\mathbf{Q}^n$. There must be some vector $e_j = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$ (with the unique 1 in the j-th position) not in the span of the rows. Hence $ke_j \notin H$ for any nonzero integer k. It follows that the image of e_j in the quotient group $\mathbf{Z}^n/H$ has infinite order. Hence $\mathbf{Z}^n/H$ has infinite order. □

A.4 The Vandermonde determinant

For variables $X_1, X_2, \ldots, X_n$ the Vandermonde determinant is defined as

$$V(X_1, X_2, \ldots, X_n) = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ X_1 & X_2 & X_3 & \cdots & X_n \\ X_1^2 & X_2^2 & X_3^2 & \cdots & X_n^2 \\ X_1^3 & X_2^3 & X_3^3 & \cdots & X_n^3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ X_1^{n-1} & X_2^{n-1} & X_3^{n-1} & \cdots & X_n^{n-1} \end{vmatrix}.$$

Proposition A.5 *For variables $X_1, X_2, \ldots, X_n$ we have*

$$V(X_1, X_2, \ldots, X_n) = \prod_{1 \le j < k \le n} (X_k - X_j).$$

Proof We use elementary row operations on the determinant. Starting at the bottom row and continuing upwards until one reaches the second row, subtract X_1 times the preceding row from each row. This does not alter the determinant so that

$$\begin{aligned} & V(X_1, X_2, \ldots, X_n) \\ = & \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & X_2 - X_1 & X_3 - X_1 & \cdots & X_n - X_1 \\ 0 & X_2(X_2 - X_1) & X_3(X_3 - X_1) & \cdots & X_n(X_n - X_1) \\ 0 & X_2^2(X_2 - X_1) & X_3^2(X_3 - X_1) & \cdots & X_n^2(X_n - X_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & X_2^{n-2}(X_2 - X_1) & X_3^{n-2}(X_3 - X_1) & \cdots & X_n^{n-2}(X_n - X_1) \end{vmatrix} \\ = & \begin{vmatrix} X_2 - X_1 & X_3 - X_1 & \cdots & X_n - X_1 \\ X_2(X_2 - X_1) & X_3(X_3 - X_1) & \cdots & X_n(X_n - X_1) \\ X_2^2(X_2 - X_1) & X_3^2(X_3 - X_1) & \cdots & X_n^2(X_n - X_1) \\ \vdots & \vdots & \ddots & \vdots \\ X_2^{n-2}(X_2 - X_1) & X_3^{n-2}(X_3 - X_1) & \cdots & X_n^{n-2}(X_n - X_1) \end{vmatrix}. \end{aligned}$$

Taking out the common factors from each column we get

$$V(X_1, X_2, \ldots, X_n) = V(X_2, X_3, \ldots, X_n) \prod_{k=2}^{n} (X_k - X_1)$$

from which the stated formula follows by induction. □

A.5 Euclidean domains

Recall that an *integral domain* is a (commutative) ring in which the product of two nonzero elements is always nonzero. Let R be an integral domain. Recall that we write $a \mid b$ for $a, b \in R$ if $b = ac$ for some $c \in R$.

A *Euclidean function* ϕ on an integral domain R is a function $\phi : R\backslash\{0\} \to \mathbf{Z}$ with the properties

- $\phi(a) \geq 0$ for all $a \in R$, $a \neq 0$, and
- if a, $b \in R$ with $a \neq 0$ then either $a \mid b$ or there is $c \in \mathbf{R}$ with $\phi(b - ac) < \phi(a)$.

An integral domain R is a *Euclidean domain* if there is a Euclidean function on R.

Proposition A.6 *Let R be a Euclidean domain. Each ideal in R is principal.*

Proof Let ϕ be a Euclidean function on R. Suppose that I is a nonzero ideal of R. Let a be a nonzero element of I with $\phi(a)$ minimal. Clearly $\langle a \rangle \subseteq I$. If equality did not hold there would be $b \in I$ with $a \nmid b$. By the Euclidean property there is $c \in R$ with $\phi(b - ac) < \phi(a)$. But $b - ac \in I$ so this contradicts the choice of a as minimizing $\phi(a)$. Hence $I = \langle a \rangle$ is principal. □