Chapter 1

Algebraic numbers and algebraic integers

1.1 Algebraic numbers

Definition 1.1. *The number $\alpha \in \mathbb{C}$ is said to be* algebraic *if it satisfies a polynomial equation*

$$x^n + a_1 x^{n-1} + \cdots + a_n$$

with rational coefficients $a_i \in \mathbb{Q}$.

We denote the set of algebraic numbers by $\bar{\mathbb{Q}}$.

Examples:

1. $\alpha = \frac{1}{2}\sqrt{2}$ is algebraic, since it satisfies the equation

$$x^2 - \frac{1}{2} = 0.$$

2. $\alpha = \sqrt[3]{2} + 1$ is algebraic, since it satisfies the equation

$$(x-1)^3 = 2,$$

ie

$$x^3 - 3x^2 + 3x - 3 = 0.$$

Proposition 1.1. $\mathbb{Q} \subset \bar{\mathbb{Q}}$.

Proof ▶. This is trivial; $r \in \mathbb{Q}$ satisfies the equation $x - r = 0$. ◀

Theorem 1.1. *$\bar{\mathbb{Q}}$ is a subfield of $\mathbb{C}$.*

Proof ▶. We have to show that

$$\alpha, \beta \in \bar{\mathbb{Q}} \implies \alpha + \beta, \alpha\beta \in \bar{\mathbb{Q}},$$

and that

$$\alpha \in \bar{\mathbb{Q}}, \alpha \neq 0 \implies 1/\alpha \in \bar{\mathbb{Q}}.$$

The last result is easy to prove; if α satisfies the equation

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

then $1/\alpha$ satisfies

$$x^n f(1/x) = \mathfrak{a}_n x^n + \cdots + a_1 x + a_0 = 0.$$

For the first part, we introduce an alternative description of algebraic numbers.

Lemma 1. *The number $\alpha \in C$ is algebraic if and only if the vector space over $\mathbb{Q}$*

$$V = \langle 1, \alpha, \alpha^2, \dots \rangle$$

is finite-dimensional.

Proof ▶ Suppose $\dim_{\mathbb{Q}} V = d$. Then the $d+1$ elements

$$1, \alpha, \dots, \alpha^d$$

are linearly dependent over $\mathbb{Q}$, ie α satisfies an equation of degree $\leq d$.

Conversely, if

$$\alpha^n + a_1 \alpha^{n-1} + \cdots + a_n = 0$$

then

$$\alpha^n = -a_1 \alpha^{n-1} - \cdots - a_n \in \langle 1, \alpha, \dots, \alpha^{n-1} \rangle.$$

Now

$$\alpha^{n+1} = -a_1 \alpha^n - \cdots - a_n \alpha \in \langle 1, \alpha, \dots, \alpha^{n-1} \rangle;$$

and so successively

$$\alpha^{n+2}, \alpha^{n+3}, \cdots \in \langle 1, \alpha, \dots, \alpha^{n-1} \rangle.$$

Thus

$$V = \langle 1, \alpha, \dots, \alpha^{n-1} \rangle$$

is finitely-generated. ◀

Now suppose $\alpha, \beta \in \bar{\mathbb{Q}}$. Let

$$U = \langle 1, \alpha, \alpha^2, \dots \rangle, \quad V = \langle 1, \beta, \beta^2, \dots \rangle.$$

By the Lemma above, U, V are finite dimensional vector spaces over $\mathbb{Q}$; and

$$\alpha U \subset U, \ \beta V \subset V.$$

Let

$$UV = \langle uv : u \in U, v \in V \rangle$$

be the vector space spanned by the elements uv. (Thus the general element of UV is of the form $u_1v_1 + \cdots u_rv_r$.)

Then UV is finite-dimensional; for if U, V are spanned by $u_1, \dots, u_m, \ v_1, \dots, v_n$, respectively, then UV is spanned by the mn elements u_iv_j.

Furthermore,

$$(\alpha + \beta)UV \subset UV, \quad (\alpha\beta)UV \subset UV.$$

Hence

$$\alpha + \beta, \alpha\beta \in \bar{\mathbb{Q}},$$

by the Lemma. ◀

A slight variant of the Lemma is sometimes useful.

Proposition 1.2. *The number $\alpha \in \mathbb{C}$ is algebraic if and only if there exists a finite-dimensional (but non-zero) vector space*

$$V \subset \mathbb{C}$$

such that

$$\alpha V \subset V.$$

Proof ▶. If α is algebraic then we can take

$$V = \langle 1, \alpha, \alpha^2, \dots \rangle$$

by the previous Lemma.

Conversely, suppose $\dim_{\mathbb{Q}} V = d$. Choose $v \in V, v \neq 0$. Then the $d + 1$ elements

$$v, \alpha v, \dots, \alpha^d v$$

are linearly dependent, and so (as before) α satisfies an equation of degree $\leq d$. ◀

Theorem 1.2. $\bar{\mathbb{Q}}$ *is* algebraically closed*, ie if* $\alpha \in \mathbb{C}$ *satisfies an equation*

$$x^n + c_1 x^{n-1} + \cdots + c_n = 0$$

with $c_i \in \bar{\mathbb{Q}}$ *then* $\alpha \in \bar{\mathbb{Q}}$.

Proof ▶. For $i = 1, \ldots, n$ let V_i be a finite-dimensional (but non-zero) vector space such that

$$c_i V_i \subset V_i;$$

and let

$$V_0 = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle.$$

Set

$$V = V_0 V_1 \cdots V_{n-1},$$

ie the vector space spanned by the products

$$\alpha^i v_1 \cdots v_{n-1},$$

with $v_i \in V_i$.

Then

$$\alpha V \subset V.$$

It is sufficient for this to show that

$$\alpha^{i+1} v_1 \cdots v_{n-1} \in V.$$

This is immediate unless $i = n - 1$, in which case

$$\alpha^n v_1 \cdots v_n = -\sum_{0 \le i < n} \alpha^i v_1 \cdots v_{i-1} (c_i v_i) v_{i+1} \cdots v_{n-1}.$$

But $c_i v_i \in V_i$. Hence

$$\alpha^n v_1 \cdots v_n \in V,$$

and so

$$\alpha V \subset V.$$

Since V is finite-dimensional, it follows from Proposition 1.2 above that

$$\alpha \in \bar{\mathbb{Q}}.$$

◀

1.2 The minimal polynomial of an algebraic number

Recall that a polynomial $f(x) \in k[x]$ is said to be *monic* if its leading coefficient is 1:

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n.$$

Proposition 1.3. *An algebraic number $\alpha \in \bar{\mathbb{Q}}$ satisfies a unique monic polynomial $m(x) \in \mathbb{Q}[x]$ of minimal degree; and if $f(x) \in \mathbb{Q}[x]$ then*

$$f(\alpha) = 0 \iff m(x) \mid f(x).$$

Proof ►. If α satisfies two monic polynomials $m_1(x), m_2(x)$ of the same degree, then it satisfies the polynomial $m_1(x) - m_2(x)$ of lower degree.

If $f(\alpha) = 0$, divide $f(x)$ by $m(x)$, say

$$f(x) = m(x)q(x) + r(x),$$

where $\deg r(x) < \deg m(x)$. Then

$$r(\alpha) = f(\alpha) - m(\alpha)q(\alpha) = 0,$$

contradicting the minimality of $m(x)$ unless $r(x) = 0$, ie $m(x) \mid f(x)$. ◄

Definition 1.2. *The polynomial $m(x)$ is called the* minimal polynomial *of α; and if $\deg m(x) = d$ then α is said to be an algebraic number* of degree d.

1.3 Algebraic integers

Definition 1.3. *The number $\alpha \in \mathbb{C}$ is said to be an* algebraic integer *if it satisfies a polynomial equation*

$$x^n + a_1 x^{n-1} + \cdots + a_n$$

with integer coefficients $a_i \in \mathbb{Z}$.

We denote the set of algebraic integers by $\bar{\mathbb{Z}}$.

Remark. In algebraic number theory, an algebraic integer is often just called an *integer*, while the ordinary integers (the elements of $\mathbb{Z}$) are called *rational integers*.

Examples:

1. We have
$$\alpha = 3\sqrt{2} + 1 \in \bar{\mathbb{Z}},$$
since α satisfies
$$(x-1)^2 = 18,$$
ie
$$x^2 - 2x - 17 = 0.$$

2. Again,
$$\alpha = \sqrt{2} + \sqrt{3} \in \bar{\mathbb{Z}},$$
since α satisfies
$$(x - \sqrt{3})^2 = (x - 2\sqrt{3} + 3 = 2,$$
ie
$$x^2 - 2\sqrt{3}x + 1 = 0.$$
Hence
$$(x^2+1)^2 = 12x^2,$$
ie
$$x^4 - 10x^2 + 1 = 0.$$

Proposition 1.4. *1. $\mathbb{Z} \subset \bar{\mathbb{Z}}$;*

2. $\bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$ ie if an algebraic integer is rational then it is a rational integer.

Proof ▶. The first part is trivial: $n \in \mathbb{Z}$ satisfies the equation $z - n = 0$.
For the second part, suppose
$$\alpha = \frac{r}{s},$$
with $r, s \in \mathbb{Z}$, $\gcd(r,s) = 1$, satisfies
$$x^n + a_1 x^{n-1} + \cdots + a_n$$

with $a_i \in \mathbb{Z}$.

Then

$$r^n + a_1 r^{n-1} s + \cdots + a_n s^n = 0.$$

Hence

$$s \mid r^n.$$

Since $\gcd(r, s) = 1$, this is only possible if $s = \pm 1$, ie $\alpha \in \mathbb{Z}$. ◀

Proposition 1.5. *If $\alpha \in \bar{\mathbb{Q}}$ then*

$$n\alpha \in \bar{\mathbb{Z}}$$

for some non-zero $n \in \mathbb{Z}$.

Proof ▶. We may take the equation satisfied by α in the form

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_n = 0.$$

But then $\beta = a_0\alpha$ satisfies

$$x^n + a_0 a_1 x^{n-1} + \cdots + a_0^n a_n = 0,$$

and so

$$a_0\alpha \in \mathbb{Z}.$$

◀

Thus each algebraic number α can be written in the form

$$\alpha = \frac{\beta}{n}$$

where β is an algebraic integer and n is a rational integer.

Theorem 1.3. *$\bar{\mathbb{Z}}$ is a subring of $\mathbb{C}$.*

Proof ▶. We have to show that

$$\alpha, \beta \in \bar{\mathbb{Z}} \implies \alpha + \beta, \alpha\beta \in \bar{\mathbb{Z}}.$$

We follow an argument very similar to the proof that $\bar{\mathbb{Q}}$ is a field (Proposition 1.1). except that we use abelian groups (which we can think of as modules over $\mathbb{Z}$) in place of vector spaces over $\mathbb{Q}$.

We start by introducing an alternative description of algebraic integers.

Lemma 2. *The number $\alpha \in C$ is an algebraic integer if and only if the abelian group*

$$B = \langle 1, \alpha, \alpha^2, \dots \rangle \subset \mathbb{C}$$

is finitely-generated.

Proof ▶ This abelian group is torsion-free. It follows from the Structure Theory for Finitely-Generated Abelian Groups (which we shall abbreviate to FGAG) that a torsion-free abelian group B is finitely-generated if and only if it is free, ie

$$B \cong \mathbb{Z}^r$$

for some r. We say in this case that B has *rank* r; and it follows from the theory that every subgroup $C \subset B$ has rank $s \leq r$:

$$C = \mathbb{Z}^s \quad (s \leq r).$$

Suppose B has rank r. Let $b_1, \dots, b_r$ be a basis for B, ie each element $b \in B$ is a linear combination

$$b = z_1 b_1 + \cdots + z_r b_r$$

with integer coefficients $z_i \in \mathbb{Z}$.

Each of the b_i's can be expressed as a linear combination of a finite number of powers α^i. Taken together, these expressions for $b_1, \dots, b_r$ involve only a finite number of powers of α, say a subset of $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$.

Then

$$\alpha^n \in \langle b_1, \dots, b_r \rangle \subset \langle 1, \alpha, \dots, \alpha^{n-1} \rangle.$$

Thus α^n is a linear combination (with integer coefficients) of $1, \alpha, \dots, \alpha^{n-1}$, say

$$\alpha^n = z_0 + z_1 \alpha + \cdots + z_{n-1} \alpha^{n-1}.$$

In other words, α satisfies an equation

$$x^n - z_{n-1} x^{n-1} - \cdots - z_0 = 0.$$

Hence

$$\alpha \in \bar{\mathbb{Z}}.$$

On the other hand, suppose α satisfies an equation

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

with $a_i \in \mathbb{Z}$. Let

$$C = \langle 1, \alpha, \dots, \alpha^{n-1} \rangle.$$

Then

$$\alpha^n = -a_1\alpha^{n-1} - \cdots - a_n \in C,$$

and

$$\alpha^{n+1} = -a_1\alpha^n - \cdots - a_n\alpha \in \langle \alpha, \alpha^2, \ldots, \alpha^n \rangle \subset C,$$

since $\alpha^n \in C$. Continuing in this way,

$$\alpha^{n+i} \in C$$

for all i. Hence

$$B = C$$

is finitely-generated. ◀

Now suppose $\alpha, \beta \in \bar{\mathbb{Z}}$. Let

$$B = \langle 1, \alpha, \alpha^2, \ldots \rangle, \quad C = \langle 1, \beta, \beta^2, \ldots \rangle$$

Then B, C are finitely-generated, by the Lemma.

Let

$$BC = \langle bc : b \in B, c \in C \rangle$$

be the abelian group spanned by the elements bc. (Thus the general element of BC is of the form $b_1c_1 + \cdots b_rc_r$.)

Then BC is finitely-generated; if B, C is generated by $b_1, \ldots, b_m,\ c_1, \ldots, c_n$, respectively, then BC is generated by the mn elements b_ic_j.

Furthermore,

$$(\alpha + \beta)BC \subset BC, \quad (\alpha\beta)BC \subset BC.$$

Hence

$$\alpha + \beta, \alpha\beta \in \bar{\mathbb{Z}},$$

by the Lemma ◀

A variant of this Lemma, analagous to Proposition 1 for algebraic numbers, is often useful.

Proposition 1.6. *The number $\alpha \in \mathbb{C}$ is an algebraic integer if and only if there exists a finitely-generated (but non-zero) abelian group*

$$B \subset \mathbb{C}$$

such that

$$\alpha B \subset B.$$

Proof ▶. If α is an algebraic integer then we can take

$$B = \langle 1, \alpha, \alpha^2, \dots \rangle$$

by the previous Lemma.

Conversely, suppose B has rank r, so that

$$B \cong \mathbb{Z}^r.$$

Choose $v \in V, v \neq 0$. Then the $d+1$ elements

$$v, \alpha v, \dots, \alpha^d v$$

are linearly dependent, and so (as before) α satisfies an equation of degree $\leq d$. ◀

Theorem 1.4. $\bar{\mathbb{Z}}$ *is* integrally closed*, ie if* $\alpha \in \mathbb{C}$ *satisfies an equation*

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

with $a_i \in \bar{\mathbb{Z}}$ *then* $\alpha \in \bar{\mathbb{Z}}$*.*

Proof ▶. For $i = 1, \dots, n$ let B_i be a finitely-generated (but non-zero) abelian groups such that

$$a_i B_i \subset B_i;$$

and let

$$B_0 = \langle 1, \alpha, \dots, \alpha^{n-1} \rangle.$$

Set

$$B = B_0 B_1 \cdots B_{n-1},$$

ie the abelian group spanned by the products

$$\alpha^i b_1 \cdots b_{n-1},$$

with $b_i \in B_i$.

Then it follows exactly as in the proof of Proposition 1.2 that

$$\alpha B \subset B,$$

and so

$$\alpha \in \bar{\mathbb{Z}}$$

by Proposition 1.6. ◀

Chapter 2

Number fields and number rings

2.1 Number fields

Suppose k is a subfield of $\mathbb{C}$. Then $1 \in k$, from which it follows that k contains all rational numbers:

$$\mathbb{Q} \subset k \subset \mathbb{C}.$$

We can consider k as a vector space over $\mathbb{Q}$. In effect we 'forget' about the product $\alpha\beta$ unless $\alpha \in \mathbb{Q}$.

Definition 2.1. *An* algebraic number field *(or just* number field*) is a subfield $k \subset \mathbb{C}$ which is of finite dimension as a vector space over $\mathbb{Q}$.*

This dimension is called the degree *of the number field:*

$$\deg k = \dim_{\mathbb{Q}} k.$$

Proposition 2.1. *If k is a number field then each $\alpha \in k$ is an algebraic number of degree $\leq \deg k$.*

Proof ▶. Consider the $d+1$ elements

$$1, \alpha, \ldots, \alpha^d.$$

where $d = \deg k$. These elements must be linearly dependent over $\mathbb{Q}$, say

$$a_0 + a_1\alpha + \cdots + a_d\alpha^d = 0,$$

with $a_i \in \mathbb{Q}$. Thus α satisfies an equation of degree $\leq d$ over $\mathbb{Q}$. ◀

It follows that any number field k is sandwiched between $\mathbb{Q}$ and $\bar{\mathbb{Q}}$:

$$\mathbb{Q} \subset k \subset \bar{\mathbb{Q}}.$$

Proposition 2.2. *Suppose α is an algebraic number of degree d. Then the elements*

$$\beta = f(\alpha),$$

where $f(x) \in \mathbb{Q}[x]$, form a number field k of degree d, with basis

$$1, \alpha, \ldots, \alpha^{d-1}.$$

Proof ▶. It is clear that k is closed under addition and multiplication.

To see that it is closed under inversion, suppose $\beta \in k,\ \beta \neq 0$. Consider the map

$$\theta : \gamma \mapsto \beta\gamma : k \to k.$$

This is a linear map over $\mathbb{Q}$. Moreover it is injective since

$$\theta(\gamma) = 0 \implies \beta\gamma = 0 \implies \gamma = 0.$$

But a linear transformation $\phi : V \to V$ of a finite-dimensional vector space V is surjective if and only if it is injective. Thus $\theta : k \to k$ is surjective; and in particular

$$\beta\gamma = 1$$

for some $\gamma \in k$, ie

$$\beta^{-1} \in k.$$

Suppose $\beta = f(\alpha)$, where $f(x) \in \mathbb{Q}[x]$. Divide $f(x)$ by the minimal polynomial $m(x)$ of α, say

$$f(x) = m(x)q(x) + r(x),$$

where

$$\deg r(x) \leq d = \deg m(x).$$

Then

$$\beta = f(\alpha) = r(\alpha)$$

Thus

$$\beta = c_0 + c_1\alpha + \cdots + c_{d-1}\alpha^{d-1}.$$

Hence the d elements $1, \alpha, \ldots, \alpha^{d-1}$ span k; and they are linearly independent since otherwise α would satisfy an equation of degree $< d$. So these elements form a basis for k; and consequently $\deg k = d$. ◀

It is evident that this is the smallest number field containing α, since such a field must contain all numbers of the form $f(\alpha)$.

Definition 2.2. *We say that the field k is* generated *by α, and denote it by* $\mathbb{Q}(\alpha)$.

A number field of the form $k = \mathbb{Q}(\alpha)$ is sometimes said to be *simple*, although the Theorem below makes this definition somewhat superfluous.

But first we note that the notion of extending $\mathbb{Q}$ to the number field $\mathbb{Q}(\alpha)$ applies equally with any number field k in place of $\mathbb{Q}$.

Proposition 2.3. *Suppose k is a number field of degree d; and suppose $\beta \in \bar{\mathbb{Q}}$. Then β satisfies an equation $m(x) \in k[x]$ of minimal degree e, and the numbers $\gamma = f(\beta)$, with $f(x) \in k[x]$, form a number field K of degree*

$$\deg K = de.$$

Proof ▶. The only part that is any different from the case $k = \mathbb{Q}$ is the last statement, that $\deg K = de$.

Lemma 3. *Suppose $k = \mathbb{Q}(\alpha)$. Then the de elements*

$$\alpha^i \beta^j \quad (0 \le i < d,\ 0 \le j < e)$$

form a basis for K over $\mathbb{Q}$.

Proof ▶ Each element $\gamma \in K$ is uniquely expressible in the form

$$\gamma = \alpha_0 + \alpha_1 \beta + \cdots + \alpha_{e-1} \beta^{e-1},$$

with $\alpha_i \in k = \mathbb{Q}(\alpha)$.

But each α_i is uniquely expressible as a polynomial $f_i(\alpha)$, where $f_i(x) \in \mathbb{Q}[x]$ is of degree $< d$. It follows that γ is uniquely expressible as a linear combination of the de elements $\alpha^i \beta^j$. ◀

◀

Corollary 2.1. *If $k \subset K$ is a subfield of the number field K, then k is a number field, and*

$$\deg k \mid \deg K.$$

Theorem 2.1. *Every number field k is simple, ie*

$$k = \mathbb{Q}(\alpha)$$

for some $\alpha \in k$.

Proof ▶. This is a little tricky.

First of all, we can certainly obtain K by adjoining a finite number of elements, say

$$K = \mathbb{Q}(\alpha_1, \ldots, \alpha_r),$$

since each adjunction (assuming $\alpha_{i+1} \notin \mathbb{Q}(\alpha_1, \ldots, \alpha_i)$) wll increase the degree.

It is sufficient therefore to show that

$$\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta).$$

Suppose the minimal polynomials of α, β are $f(x), g(x)$; and suppose the roots of $f(x), g(x)$ are

$$\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d \text{ and } \beta = \beta_1, \beta_2, \ldots, \beta_e,$$

respectively. Note that the α_i are distinct, as are the β_j, since $f(x), g(x)$ are irreducible.

Let

$$\theta = c\alpha + \beta,$$

where $c \in \mathbb{Q}$ is chosen so that the de elements

$$c\alpha_i + \beta_j$$

are distinct. This is certainly possible, since we only have to avoid a finite number of values of c.

Now α satisfies the polynomial equations

$$f(x) = 0, \quad g(\theta - cx) = 0,$$

where the second equation is over the field $K = \mathbb{Q}(\theta)$

But α is the only common root (in $\mathbb{C}$) of these two polynomials. For any root of the first equation is α_i, for some i; and if this is a root of the second polynomial then

$$\beta_j = \theta - c\alpha_i,$$

so that

$$\theta = c\alpha_i + \beta_j = c\alpha + \beta.$$

But from our choice of c, this is only possible if $i = j = 1$.

It follows that

$$\gcd(f(x), g(\theta - cx)) = x - \alpha,$$

where the gcd is computed over $K = \mathbb{Q}(\theta)$.

But we know that when we compute a gcd, eg with the Euclidean algorithm, we end up with a polynomial in the field we started in.

We conclude that

$$\alpha \in K = \mathbb{Q}(\theta).$$

It follows that

$$\beta = \theta - c\alpha \in K$$

also.

Hence

$$\alpha, \beta \in K,$$

and so

$$\mathbb{Q}(\alpha, \beta) \subset K.$$

On the other hand

$$\theta = c\alpha + \beta \in \mathbb{Q}(\alpha, \beta)$$

and so

$$K \subset \mathbb{Q}(\alpha, \beta).$$

We conclude that

$$\mathbb{Q}(\alpha, \beta) = K = \mathbb{Q}(\theta).$$

◀

2.2 Number rings

Definition 2.3. *To each number field $k = \mathbb{Q}(\alpha)$ we associate the ring*

$$A = k \cap \bar{\mathbb{Z}},$$

ie A consists of the algebraic integers in k.

We say that A is a number ring of degree *d, where $d = \deg \mathbb{Q}(\alpha)$.*

Given a ring $A \subset \mathbb{C}$ we can form the *field of fractions* k of A, consisting of the numbers of the form

$$c = \frac{a}{b},$$

where $a, b \in A$ with $b \neq 0$.

Proposition 2.4. *If A is the number ring associated to the number field k,*

$$A = k \cap \bar{\mathbb{Z}},$$

then k is the field of fractions of A.

Proof ►. This is almost trivial. If $\alpha \in k$ then

$$\beta = n\alpha \in \bar{\mathbb{Z}}$$

for some $n \in \mathbb{N},\ n > 0$. Hence

$$\alpha = \frac{\beta}{n}$$

is in the field of fractions of A. ◄

2.3 Conjugates, norms and spurs

We suppose in this Section that k is a number field.

Suppose $\beta \in k$. Let μ_β denote the map

$$\gamma \mapsto \beta\gamma : k \to k.$$

This is a linear map over $\mathbb{Q}$.

Definition 2.4. *We set*

$$S(\beta) = \operatorname{tr} \mu_\beta,$$
$$\mathcal{N}(\beta) = \det \mu_\beta.$$

We call $S(\beta)$, $\mathcal{N}(\beta)$ the spur *and* norm *of $\beta \in k$.*

Evidently,

$$S(\beta),\ \mathcal{N}(\beta) \in \mathbb{Q}.$$

The following results are immediate.

Proposition 2.5. *1. $S(\beta + \gamma) = S(\beta) + S(\gamma)$;*

2. $\mathcal{N}(\beta\gamma) = \mathcal{N}(\beta)\mathcal{N}(\gamma)$;

3. if $c \in k$ then $S(c) = dc$, $\mathcal{N}(c) = c^d$.

There is an alternative way of looking at the spur and norm, in terms of *conjugates*.

If k, K are two fields then any ring homomorphism

$$\theta : k \to K$$

is necessarily injective; for if $c \in k$ is non-zero then

$$\begin{aligned} c \in \ker\theta &\implies f(c) = 0 \\ &\implies f(1) = f(cc^{-1}) = f(c)f(c^{-1}) = 0, \end{aligned}$$

while $f(1) = 1$ by definition.

Suppose k is a number field, and $K = \mathbb{C}$. We may say that θ defines an *embedding* of k in $\mathbb{C}$. We want to see in how many ways the number field $k = \mathbb{Q}(\alpha)$ can be embedded in $\mathbb{C}$.

Suppose $m(x)$ is the minimal polynomial of α. Let the roots of $m(x)$ be $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$, so that

$$m(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Note that the roots are distinct, since $m(x)$ is irreducible. For if there was a multiple root it would also be a root of $m'(x)$, and then

$$f(x) = \gcd(m(x), m'(x))$$

would be a non-trivial factor of $m(x)$.

Proposition 2.6. *Suppose $k = \mathbb{Q}(\alpha)$ is a number field of degree d, Then there are just d ring homomorphisms*

$$\sigma_i : k \to \mathbb{C},$$

given by

$$\sigma_i : f(\alpha) \mapsto f(\alpha_i) \quad (f(x) \in \mathbb{Q}[x])$$

for $i = 1, \ldots, d$.

Proof ▶. If $\alpha \mapsto \alpha'$ then

$$m(\alpha) = 0 \implies m(\alpha') = 0.$$

Hence

$$\alpha' = \alpha_i$$

for some i; and so

$$f(\alpha) \mapsto f(\alpha_i).$$

This map is well-defined, since

$$\begin{aligned} f(\alpha) = g(\alpha) &\implies m(x) \mid f(x) - g(x) \\ &\implies f(\alpha_i) = g(\alpha_i); \end{aligned}$$

and it is evident that it is a ring-homomorphism. ◀

In other words, there are just $d = \deg k$ embeddings of the number field k in $\mathbb{C}$.

Note that this result is independent of the choice of generator α; it is a property of the field k itself.

Definition 2.5. *If*

$$\sigma_1, \ldots, \sigma_d : k \to \mathbb{C}$$

are the d embeddings of k in $\mathbb{C}$ then the conjugates *of $\beta \in k$ are the d elements*

$$\sigma_i(\beta) \quad (1 \leq i \leq d).$$

The following result follows at once from our concrete construction of the embeddings of $k = \mathbb{Q}(\alpha)$ above.

Proposition 2.7. *The d conjugates of $\beta = f(\alpha)$ are the elements*

$$\sigma_i(\beta) = f(\alpha_i) \quad (1 \leq i \leq d).$$

Theorem 2.2. *We have*

1. $S(\beta) = \beta_1 + \cdots + \beta_d$;
2. $\mathcal{N}(\beta) = \beta_1 \cdots \beta_d$.

Proof ▶. This is a little tricky.

First consider the case of α. The matrix of the linear map

$$\mu_\alpha : k \to k$$

with respect to the basis $1, \alpha, \ldots, \alpha^{d-1}$ is

$$M = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_d \\ 1 & 0 & \cdots & 0 & -a_{d-1} \\ \vdots & \vdots & & \vdots & \\ 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}.$$

Thus

$$S(\alpha) = \operatorname{tr} M = -a_1,$$
$$\mathcal{N}(\alpha) = \det M = a_d.$$

On the other hand, the characteristic polynomial of M is

$$\chi_M(x) = \det(xI - M) = x^n + a_1 x^{d-1} + \cdots + a_d,$$

ie

$$\chi_M(x) = m(x),$$

the minimal polynomial — as we might have expected, since it is clear that M satisfies $m(M) = 0$, and we know that M satisfies its characteristic polynomial. Since $m(x)$ is irreducible, it follows that the two must be the same.

But the roots of $m(x)$ are the conjugates $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$.

It follows that these are the eigenvectors of M; and so

$$\begin{aligned} S(\alpha) &= \operatorname{tr} M = \alpha_1 + \cdots + \alpha_d, \\ \mathcal{N}(\alpha) &= \det M = \alpha_1 \cdots \alpha_d. \end{aligned}$$

Now consider a general element $\beta = f(\alpha)$ of k. The matrix of the linear map $\mu_\beta : k \to k$ with respect to the same basis $1, \alpha, \ldots, \alpha^{d-1}$ is just $p(M)$; and we know that the eigenvalues of $p(M)$ are $p(\alpha_i)$. It follows that

$$\begin{aligned} S(\beta) &= \operatorname{tr} \mu_\beta \\ &= \operatorname{tr} p(M) \\ &= p(\alpha_1) + \cdots + p(\alpha_d) \\ &= \beta_1 + \cdots + \beta_d; \end{aligned}$$

and similarly

$$\begin{aligned} \mathcal{N}(\beta) &= \det \mu_\beta \\ &= \det p(M) \\ &= p(\alpha_1) \cdots p(\alpha_d) \\ &= \beta_1 \cdots \beta_d. \end{aligned}$$

◀

2.4 The discriminant

Recall that the disciminant of a monic polynomial

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_1),$$

with roots $\alpha_1, \ldots, \alpha_n$, is defined by

$$\begin{aligned} D(f) &= \prod_{i<j} (\alpha_i - \alpha_j)^2 \\ &= \pm \prod_{i \neq j} (\alpha_i - \alpha_j), \end{aligned}$$

where the sign (which doesn't really concern us) is

$$(-1)^{(n-1)+(n-2)+\cdots+1} = (-1)^{n(n-1)/2} = \begin{cases} +1 \text{ if } n \equiv 0, 1 \bmod 4 \\ -1 \text{ if } n \equiv 2, 3 \bmod 4. \end{cases}$$

Evidently the discriminant $D = 0$ if and only if $f(x)$ has a double root, ie $\alpha_i = \alpha_j$ for some $i \neq j$.

The formula for the discriminant can be re-written in several ways. First note that

$$f'(\alpha_i) = (\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1})(\alpha_i - \alpha_n),$$

and so

$$\begin{aligned} D &= \pm f'(\alpha_1) \cdots f'(\alpha_n) \\ &= \pm \mathcal{N} f'(\alpha) \end{aligned}$$

(with the same sign as before), where we have written $\alpha = \alpha_1$.

Secondly, recall that the Vandermonde matrix

$$X = \begin{pmatrix} \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \\ \alpha_1^{n-2} & \alpha_2^{n-2} & \cdots & \alpha_n^{n-2} \\ \vdots & \vdots & & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}$$

has determinant

$$\det X = \prod_{i<j} (\alpha_i - \alpha_j).$$

Hence

$$\begin{aligned} D(f) &= (\det X)^2 \\ &= \det X'X \\ &= \det Y, \end{aligned}$$

where

$$\begin{aligned} Y_{ij} &= \alpha_1^i \alpha_1^j + \cdots + \alpha_n^i \alpha_n^j \\ &= S(\alpha^{i+j}). \end{aligned}$$

Now suppose we have a number field

$$k = \mathbb{Q}(\alpha),$$

where α has minimal polynomial $m(x)$ of degree d. Then $1, \alpha, \ldots, \alpha^{d-1}$ forms a basis for the vector space $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. This suggests the following definition.

Definition 2.6. *Suppose $\beta_1, \ldots, \beta_d$ is a basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Then we define the* discriminant *of the extension with respect to this basis to be*

$$D(\beta_1, \ldots, \beta_d) = \det X,$$

where

$$X_{ij} = S(\beta_i \beta_j).$$

If we choose another basis $\gamma_1, \ldots, \gamma_d$ then

$$\gamma_i = \sum_j T_{ij} \beta_j,$$

where T is an invertible $d \times d$ matrix; and it follows that

$$D(\gamma_1, \ldots, \gamma_d) = (\det T)^2 D(\beta_1, \ldots, \beta_d).$$

Thus the discriminant is defined up to a square factor ρ^2 where $\rho \in \mathbb{Q}^\times$).

In particular, since

$$D(\beta_1, \ldots, \beta_d) = \rho^2 D(1, \alpha, \ldots, \alpha^{d-1}) = \pm D(m(x)),$$

and $m(x)$ is *separable*, ie does not have repeated roots, the discriminant of a number field (with respect to any basis) is non-zero.

Now consider the number ring

$$A = \mathbb{Q}(\alpha) \cap \bar{\mathbb{Z}}.$$

Proposition 2.8. *If $\beta_1, \ldots, \beta_n \in A$ then*

$$D(\beta_1, \ldots, \beta_n) \in \mathbb{Z}.$$

Proof ▶. This follows at once from the fact that

$$S(\beta_i \beta_j) \in \mathbb{Z}.$$

◀

Theorem 2.3. *If $k = \mathbb{Q}(\alpha)$ is a number field of degree d then the number ring $A = k \cap \bar{\mathbb{Z}}$ is a free abelian group of rank d:*

$$A \cong \mathbb{Z}^d.$$

Proof ▶. Let $\beta_1, \ldots, \beta_d \in A$ be a basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. (We can certainly find such a basis, since given $\beta \in k$ we can always find non-zero $n \in \mathbb{Z}$ such that $n\beta \in A$.) Let

$$D = D(\beta_1, \ldots, \beta_d).$$

Lemma 4. *If $\alpha \in A$ then*

$$\alpha = \frac{z_1\beta_1 + \cdots + z_d\beta_d}{D},$$

where $z_1, \ldots, z_d \in \mathbb{Z}$.

Proof ▶ Let

$$\sigma_i : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha_i) \quad (1 \le i \le d)$$

denote the d injective isomorphisms (or *embeddings*) $\mathbb{Q}(\alpha) \to \mathbb{C}$, given by

$$\sigma_i(f(\alpha)) = f(\alpha_i) \quad (f(x) \in \mathbb{Q}[x]).$$

Suppose $\gamma \in A$. Then

$$\gamma = \mathfrak{c}_1\beta_1 + \cdots + c_d\beta_d,$$

with $c_i \in \mathbb{Q}$. Hence

$$S(\gamma\beta_i) = S(\beta_1\beta_i)c_1 + \cdots + S(\beta_d\beta_i)x_d$$

for $i = 1, \ldots, d$.

We can regard these as d linear equations for $c_1, \ldots, c_d$. The matrix of the equations is

$$D_{ij} = S(\beta_i\beta_j)$$

with determinant

$$D = D(\beta_1, \ldots, \beta_d).$$

Moreover all the traces (or spurs) $S(\cdot)$ are in $\mathbb{Z}$. It follows (eg from Cramer's rule for solving linear equations) that the c_i are all of the form

$$c_i = \frac{z_i}{D}$$

with $z_i \in \mathbb{Z}$. ◀

It follows from the Lemma that the abelian group A is sandwiched between two free abelian groups of rank d:

$$\langle \beta_1, \ldots, \beta_d \rangle \subset A \subset \langle \beta_1/D \ldots, \beta_d/D \rangle.$$

But this implies, from the Structure Theory of Finitely-Generated Abelian Groups, that A itself is also a free abelian group of rank d. ◀

Proposition 2.9. *Any two bases $\alpha_1, \ldots, \alpha_d$, $\beta_1, \ldots, \beta_d$ of a number ring have the same disciminant:*

$$D(\alpha_1, \ldots, \alpha_d) = D(\beta_1, \ldots, \beta_d).$$

Proof ▶. Since the elements of each basis can be expressed in terms of the other, there are $d \times d$ matrices T, U such that

$$\alpha_i = \sum_j T_{ij}\beta_j, \quad \beta_i = \sum_i U_{ij}\alpha_j.$$

It follows that

$$\begin{aligned} TU = I &\implies \det T \det U = 1 \\ &\implies \det T = \det U = \pm 1. \end{aligned}$$

The result follows, since

$$D(\alpha_1, \ldots, \alpha_d) = \det(T)^2 D(\beta_1, \ldots, \beta_d).$$

◀

Definition 2.7. *The discriminant $D = D(A)$ of a number ring is the discriminant of a basis for A (as an abelian group).*

The discriminant $D(A)$ is an important invariant of A.

Examples:

1. Consider the quadratic field $\mathbb{Q}(\sqrt{m})$, where $m \in \mathbb{Z}$ is square-free.

   Suppose first that $m \not\equiv 1 \bmod 4$. Then

   $$A = \mathbb{Z}[\sqrt{m}].$$

   The numbers $1, \sqrt{m}$ form a basis for A. Hence

   $$\begin{aligned} D(A) &= \begin{pmatrix} S(1) & S(\sqrt{m} \\ S(\sqrt{m} & S(m) \end{pmatrix} \\ &= \begin{pmatrix} 2 & 0 \\ 0 & 2m \end{pmatrix} \\ &= 4m. \end{aligned}$$

2. Now suppose $m \equiv 1 \bmod 4$. In that case the integers are the numbers

$$a + b\,\frac{1+\sqrt{m}}{2} \quad (a, b \in \mathbb{Z}).$$

Thus

$$\begin{aligned} D(A) &= \begin{pmatrix} S(1) & S((1+\sqrt{m})/2) \\ S((1+\sqrt{m})/2) & S((m+1)/4 + \sqrt{m}/2) \end{pmatrix} \\ &= \begin{pmatrix} 2 & 1 \\ 1 & (m+1)/2 \end{pmatrix} \\ &= m. \end{aligned}$$

Chapter 3

Quadratic number fields

Chapter 4

Ideal Theory

4.1 Ideals

We shall assume throughout this Chapter that A is a *commutative ring with 1.*

Definition 4.1. *An* ideal *in A is a non-empty subset $\mathfrak{a} \subset A$ such that*

1. $a, b \in \mathfrak{a} \implies a + b \in \mathfrak{a}$;
2. $a \in A,\ b \in \mathfrak{a} \implies ab \in \mathfrak{a}$.

There is an intimate connection between ideals and quotient-rings. In fact the two concepts are more or less interchangeable.

Note that a ring A has an underlying structure as an additive group, if we 'forget' about multiplication; and if $\mathfrak{a} \subset A$ is an ideal, then $\mathfrak{a}$ is a subgroup of A. We assume that the notion of a quotient-group is familiar. The following result is readily verified.

Proposition 4.1. *Suppose $\mathfrak{a} \subset A$ is an ideal. Then there is a natural ring-structure on the quotient-group $A/\mathfrak{a}$, with*

$$\overline{ab} = \bar{a}\bar{b}.$$

Thus we may speak of the *quotient-ring* $A/\mathfrak{a}$.

Recall that a ring-homomorphism

$$f : A \to B$$

is a map such that

1. $f(a + b) = f(a) + f(b)$;

2. $f(ab) = f(a)f(b)$;

3. $f(1) = 1$.

Proposition 4.2. *Suppose*

$$f : A \to B$$

is a ring-homomrphism. Then

$$\ker f = \{a \in A; f(a) = 0\}$$

is an ideal in A; and

$$\operatorname{im} f \cong A/\ker f.$$

Conversely, if $\mathfrak{a} \subset A$ is an ideal, then the map $a \mapsto \bar{a}$ defines a surjective homomorphism

$$A \to A/\mathfrak{a},$$

with kernel $\mathfrak{a}$.

Proof ▶. The First Isomorphism Theorem for groups establishes an isomorphism

$$\operatorname{im} f \cong A/\ker f$$

of additive groups; and it is a straightforward matter to verify that this isomorphism preserves multiplication. ◀

Proposition 4.3. *If $\mathfrak{a}, \mathfrak{b} \subset A$ are ideals then so are*

1. $\mathfrak{a} \cup \mathfrak{b}$;

2. $\mathfrak{a} + \mathfrak{b} = \{a + b,\ a \in \mathfrak{a}, b \in \mathfrak{b}\}$;

3. $\mathfrak{ab} = \{a_1b_1 + \cdots a_rb_r,\ a_1 \ldots, a_r \in \mathfrak{a},\ b_1 \ldots, b_r \in \mathfrak{b}\}$;

4. $(\mathfrak{a} : \mathfrak{b}) = \{a \in A : a\mathfrak{b} \subset \mathfrak{a}\}$.

These are all immediate. Note that we must allow sums in the definition of the product; an element of $\mathfrak{ab}$ is not necessarily of the form ab.

4.2 Principal ideals

Definition 4.2. *We denote the ideal generated by $a_1, \ldots, a_r \in A$ by*

$$(a_1, \ldots, a_r) = \{a_1u_1 + \cdots + a_ru_r : u_1, \ldots, u_r \in A\}.$$

An ideal (a) generated by a single element is said to be principal.

Remark. Observe that

$$(0) = \{0\},\ (1) = A.$$

Proposition 4.4. *If $a, b \in A$ then*

$$(a) = (b) \iff b = \epsilon a$$

for some unit $\epsilon \in A$.

Definition 4.3. *We say that A is a* principal ideal domain *if every ideal $\mathfrak{a} \in A$ is principal.*

The abbreviation PID is often used for 'principal ideal domain'.

Proposition 4.5. *$\mathbb{Z}$ is a principal ideal domain.*

Proof ▶. Suppose $\mathfrak{a} \subset \mathbb{Z}$ is an ideal. If $\mathfrak{a} = (0)$ the result is immediate.

If not, suppose $n \in \mathfrak{a},\ n \neq 0$. We may suppose that $n > 0$, since

$$n \in \mathfrak{a} \implies -n = (-1)n \in \mathfrak{a}.$$

Let d be the smallest integer > 0 in $\mathfrak{a}$. Then

$$\mathfrak{a} = (d).$$

For suppose $n \in \mathfrak{a}$. Divide n by d, say

$$n = dq + r,$$

where $0 \leq r < d$. Then

$$r = n + (-q)d \in \mathfrak{a}$$

since $n, d \in \mathfrak{a}$. Hence $r = 0$, by the minimality of d. Thus

$$n = dq \in (d),$$

and so

$$\mathfrak{a} = (d).$$

◀

Proposition 4.6. *If k is a field, then the ring $k[x]$ (of polynomials in one variable over k) is a principal ideal domain.*

Proof ▶. The proof is almost identical to that for $\mathbb{Z}$.

Suppose $\mathfrak{a} \subset k[x]$ is an ideal. If $\mathfrak{a} = (0)$ the result is immediate. Otherwise, let $m(x)$ be the monic polynomial of lowest degree in $\mathfrak{a}$. Then

$$\mathfrak{a} = (m(x)).$$

For suppose $f(x) \in k[x]$. Divide $f(x)$ by $m(x)$, say

$$f(x) = m(x)q(x) + r(x),$$

where $0 \leq \deg r(x) < \deg m(x)$. Then

$$r(x) = f(x) - q(x)m(x) \in \mathfrak{a}.$$

Hence $r(x) = 0$, by the minimality of $m(x)$. Thus

$$f(x) = m(x)q(x) \in (m(x)),$$

and so

$$\mathfrak{a} = (m(x)).$$

◀

4.3 Prime ideals

Definition 4.4. *The ideal $\mathfrak{p} \subset A$ is said to be* prime *if $\mathfrak{p} \neq (1)$ and*

$$ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}.$$

Proposition 4.7. *The principal ideal (a) is prime if and only if the element a is prime.*

Proof ▶. Suppose (a) is a prime ideal, Then

$$\begin{aligned} a \mid bc &\implies bc \in (a) \\ &\implies b \in (a) \text{ or } c \in (a) \\ &\implies a \mid b \text{ or } a \mid c. \end{aligned}$$

Conversely, if the element a is prime then

$$\begin{aligned} bc \in (a) &\implies a \mid bc \\ &\implies a \mid b \text{ or } a \mid c \\ &\implies b \in (a) \text{ or } c \in (a). \end{aligned}$$

◀

Proposition 4.8. *The ideal $\mathfrak{p} \in A$ is prime if and only if the quotient-ring $A/\mathfrak{p}$ is an integral domain.*

Proof ▶. Let $\bar{a}$ denote the image of $a \in A$ in $A/\mathfrak{p}$. Then

$$\begin{aligned} \bar{a}\,\bar{b} = 0 &\iff \overline{ab} = 0 \\ &\iff ab \in \mathfrak{p} \\ &\iff a \in \mathfrak{p} \text{ or } b \in \mathfrak{p} \\ &\iff \bar{a} = 0 \text{ or } \bar{b} = 0. \end{aligned}$$

◀

There is one very important case in which we know an ideal is prime.

Definition 4.5. *The ideal $\mathfrak{m} \in A$ is said to be* maximal *if $\mathfrak{m} \neq A$ and*

$$\mathfrak{m} \subset \mathfrak{a} \subset A \implies \mathfrak{a} = \mathfrak{m} \text{ or } \mathfrak{a} = A$$

for any ideal $\mathfrak{a}$.

Proposition 4.9. *An ideal $\mathfrak{m} \subset A$ is maximal if and only if the quotient-ring $A/\mathfrak{m}$ is a field.*

Proof ▶. A ring A is a field if and only if the only ideals in A are (0) and (1).

The ideals in $A/\mathfrak{m}$ are in one-one correspondence with the ideals $\mathfrak{a} \supset \mathfrak{m}$ in A.

Thus $A/\mathfrak{m}$ is a field if and only if the only ideals $\mathfrak{a}$ such that

$$\mathfrak{m} \subset \mathfrak{a} \subset A$$

are $\mathfrak{m}$ and A itself, ie if $\mathfrak{m}$ is maximal. ◀

Corollary 4.1. *A maximal ideal is necessarily prime.*

This follows at once from the Proposition; but it is easy to see directly. Suppose $\mathfrak{m}$ is maximal, and suppose $ab \in \mathfrak{m}$ but $a \notin \mathfrak{m}$. Then

$$(\mathfrak{m}, a) = A = (1).$$

Thus we can find $m \in \mathfrak{m},\ c \in A$ such that

$$m + ac = 1.$$

But now, multiplying by b,

$$b = mb + (ab)c \in \mathfrak{p},$$

showing that $\mathfrak{m}$ is prime.

We shall see that in the case of a number ring A: *every prime ideal except* (0) *is maximal.*

And our main aim. of course, is to prove Dedekind's Theorem, that *every non-zero ideal* $\mathfrak{a}$ *in a number ring* A *is uniquely expressible as a product of prime ideals*

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r.$$

4.4 Co-prime ideals

Definition 4.6. *The ideals* $\mathfrak{a}, \mathfrak{b} \subset A$ *are said to be* co-prime *if*

$$\mathfrak{a} + \mathfrak{b} = (1) = A.$$

Proposition 4.10. *If the ideals* $\mathfrak{a}, \mathfrak{b} \subset A$ *are co-prime then*

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}.$$

Proof ▶. It is evident that

$$\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b};$$

that is true for any two ideals.

By definition, there are elements $a \in \mathfrak{a},\ b \in \mathfrak{b}$ such that

$$a + b = 1.$$

Suppose

$$x \in \mathfrak{a} \cap \mathfrak{b}.$$

Then

$$x = x(a + b) = xa + xb \in \mathfrak{a}\mathfrak{b};$$

for $xa \in \mathfrak{a}\mathfrak{b}$ since $a \in \mathfrak{a}, x \in \mathfrak{b}$, and similarly $xb \in \mathfrak{a}\mathfrak{b}$. ◀

Proposition 4.11. *1. if* $\mathfrak{a}$ *is coprime to* $\mathfrak{b}$ *then* $\mathfrak{a}^e$ *is coprime to* $\mathfrak{b}^f$ *for any* $e, f \in \mathbb{N}$*;*

2. If $\mathfrak{a}$ *is coprime to* $\mathfrak{b}_1, \dots, \mathfrak{b}_r$ *then it is coprime to* $\mathfrak{b}_1 \cdots \mathfrak{b}_r$.

Proof ▶. 1. Suppose

$$a + b = 1.$$

Then

$$(a + b)^{e+f} = 1.$$

The terms in the binomial expansion all lie either in $\mathfrak{a}^e$ or in $\mathfrak{b}^f$.

2. Suppose

$$a_i + b_i = 1,$$

with $a_1, \ldots, a_r \in \mathfrak{a},\ b_i \in \mathfrak{b}_i$. Multiplying these equations together we obtain 2^r terms, all of which lie in $\mathfrak{a}$ except for $b_1 \cdots b_r \in \mathfrak{b}_1 \cdots \mathfrak{b}_r$.

◀

Corollary 4.2. *Suppose the ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ are mutually co-prime. Then*

$$\mathfrak{a}_1^{e_1} \cap \mathfrak{a}_2^{e_1} \cap \cdots \cap \mathfrak{a}_r^{e_r} = \mathfrak{a}_1^{e_1} \mathfrak{a}_2^{e_1} \cdots \mathfrak{a}_r^{e_r},$$

for any exponents $e_1, e_2, \ldots, e_r \in \mathbb{N}$.

Note that distinct maximal ideals $\mathfrak{p}, \mathfrak{q}$ are necessarily co-prime. Thus if $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are maximal then

$$\mathfrak{p}_1^{e_1} \cap \mathfrak{p}_2^{e_1} \cap \cdots \cap \mathfrak{p}_r^{e_r} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

The following result might be called the Chinese Remainder Theorem for ideals.

Theorem 4.1. *Suppose $\mathfrak{a}, \mathfrak{b} \subset A$ are co-prime ideals; and suppose $r, s \in A$. Then there exists $a \in A$ such that*

$$a \equiv r \bmod \mathfrak{a}$$
$$a \equiv s \bmod \mathfrak{b}.$$

Moreover, $b \in A$ is a second solution to these two congruences if and only if

$$a \equiv b \bmod \mathfrak{ab}.$$

Proof ▶. Since $\mathfrak{a} + \mathfrak{b} = (1)$ we can find $u \in A,\ v \in B$ such that

$$u + v = 1.$$

Note that

$$v \begin{cases} \equiv 0 \bmod \mathfrak{a}, \\ \equiv 1 \bmod \mathfrak{b}, \end{cases} \qquad u \begin{cases} \equiv 1 \bmod \mathfrak{a}, \\ \equiv 0 \bmod \mathfrak{b}. \end{cases}$$

It follows that

$$rv + su \begin{cases} \equiv r \bmod \mathfrak{a}, \\ \equiv s \bmod \mathfrak{b}. \end{cases}$$

Conversely, suppose a, b are two solutions to the two congruences, Then

$$a - b \in \mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab},$$

ie

$$a \equiv b \bmod \mathfrak{ab}.$$

◀

The result can be expressed equivalently in terms of quotient-rings, as follows.

Suppose $\mathfrak{a}, \mathfrak{b} \subset A$ are two ideals (not necessarily co-prime). Then the homomorphisms

$$A \to A/\mathfrak{a}, \quad A \to A/\mathfrak{b}$$

combine in a homomorphism

$$\Theta : A \to A/\mathfrak{a} \times A/\mathfrak{b}.$$

Since

$$\ker \Theta = \mathfrak{a} \cap \mathfrak{b},$$

this gives an injective homomorphism

$$\Phi : A/(\mathfrak{a} \cap \mathfrak{b}) \to A/\mathfrak{a} \times A/\mathfrak{b}.$$

Now suppose $\mathfrak{a}, \mathfrak{b}$ are co-prime. Then $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$; and by Theorem 4.1, Θ and so Φ are surjective.

Hence Φ is bijective, ie an isomorphism:

$$A/(\mathfrak{ab}) \cong A/\mathfrak{a} \times A/\mathfrak{b}.$$

4.5 Noetherian rings

Definition 4.7. *The ring A is said to be* noetherian *if every ideal $\mathfrak{a} \in A$ is finitely-generated.*

All the commutative rings we meet will be noetherian. In fact, virtually all commutative rings one is likely to meet in mathematics are noetherian. (There is perhaps an analogy with locally compact spaces in topology.)

There is an alternative way of defining the property of noetherian-ness.

Proposition 4.12. *The ring A is noetherian if and only if its ideals satisfy the* increasing chain condition*, ie every increasing sequence of ideals*

$$\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$$

is stationary*, that is*

$$\mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \cdots$$

for some n.

Proof ▶. It is easy to see that the union

$$\mathfrak{a} = \bigcup_i \mathfrak{a}_i$$

of an increasing sequence of ideals is itself an ideal.

Suppose A is noetherian. Then this ideal is finitely-generated, say by $a_1, \ldots, a_r$. Each of these elements lies in one of the $\mathfrak{a}_i$. Hence all of them lie in $\mathfrak{a}_n$ for some n; and then

$$\mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \cdots$$

Conversely, suppose the ideals in A satisfy the increasing chain condition; and suppose $\mathfrak{a} \in A$ is an ideal. Choose any element $a_1 \in \mathfrak{a}$. If $\mathfrak{a} = (a_1)$ we are done; if not choose an element $a_2 \in \mathfrak{a} \setminus (a_1)$. If $\mathfrak{a} = (a_1, a_2)$ we are done; if not choose an element $a_3 \in \mathfrak{a} \setminus (a_1, a_2)$.

Continuing in this way, we obtain an increasing sequence of ideals

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots .$$

By the increasing chain condition, this process must stop, ie

$$\mathfrak{a} = (a_1, \ldots, a_r)$$

at some stage. ◀

Proposition 4.13. *Every number ring*

$$A = \mathbb{Q}[\alpha] \cap \bar{\mathbb{Z}}$$

is noetherian.

Proof ▶. By Proposition /refD3,

$$A \cong \mathbb{Z}^d$$

as an additive group, where

$$d = \deg \mathbb{Q}(\alpha) = \dim_{\mathbb{Q}} \mathbb{Q}[\alpha].$$

But from the Structure Theory of Finitely Generated Abelian Groups, every subgroup of a finitely-generated abelian group of rank r is also finitely-generated, of rank $\leq r$.

It follows that every ideal $\mathfrak{a} \in A$ is finitely-generated *as an abelian group* by $\leq d$ elements. A fortiori it is generated by $\leq d$ elements *as an ideal*. ◀

We shall see later that in fact each ideal in a number-ring A is generated by at most 2 elements.

Theorem 4.2. *Suppose A is a noetherian integral domain. Then A is a Unique Factorisation Domain if and only if it is a Principal Ideal Domain.*

Proof ▶.

Lemma 5. *Each element $a \in A$ is expressible as a product of irreducibles*

$$a = p_1 p_2 \cdots p_r.$$

Proof ▶ If a is not irreducible, then it factorises

$$a = a_1 a_2,$$

where neither a_1 nor a_2 are units. Note that

$$(a) \subset (a_1),\ (a) \subset (a_2),$$

with both inclusions proper; for if $(a) = (a_1)$, say, then $a = \epsilon a_1$ where ϵ is a unit, and then it follows (since A is an integral domain) that $a_2 = \epsilon$.

If now a_1, a_2 are both irreducible then we are done. If not then one, say a_1 factorises:

$$a_1 = a_{11} a_{11}.$$

Continuing in this way, if all the factorisations end then we are done.

If not, then one (at least) of a_1, a_2 must factorise indefinitely. Suppose it is a_1. Then one of the factors a_{11}, a_{12} must factorise indefinitely. Suppose it is a_{11}.

If this continues indefinitely then we obtain a strictly increasing sequence of ideals

$$(a_1) \subset (a_{11}) \subset \cdots,$$

contrary to the supposition that A is noetherian.

Hence the factorisation must end, giving an expression for a as a product of irreducibles. ◀

Now suppose A is a UFD. We have to show that every ideal $\mathfrak{a} \subset A$ is principal. It is sufficient to prove this for ideals (a, b) generated by two elements; for every ideal is finitely generated, and this will allow us to repeatedly reduce the number of generators by one:

$$\mathfrak{a} = (a_1, \ldots, a_r) = (b, a_3, \ldots, a_r) = (c, a_4, \ldots, a_r) = \cdots .$$

Express a, b as products of irreducibles, say

$$a = \epsilon \prod p_i^{e_i}, \quad b = \eta \prod p_i^{f_i},$$

where we include all inequivalent irreducibles p_i, with $e_i, f_i = 0$ for all but a finite number of i.

Let

$$d = \prod p_i^{\min(e_i, f_i)}.$$

Then

$$d \mid a, b;$$

and

$$e \mid a, b \implies e \mid d,$$

as one may see on expressing e as a product of irreducibles.

It follows that

$$(a, b) = (d);$$

for if

$$c = ua + vb \in (a, b)$$

then

$$p_i^{\min(e_i, f_i)} \mid c,$$

and so $d \mid c$, ie

$$c \in (d).$$

Conversely, suppose A is a PID. If p is irreducible, then p is prime. For suppose

$$p \mid ab.$$

Let

$$(p, a) = (d).$$

Then

$$p = cd.$$

Since p is irreducible, either c or d is a unit.

If c is a unit then $d \sim p$, and so

$$p \mid a.$$

If d is a unit, then

$$(p, a) = (1),$$

ie there exists u, v such that

$$up + va = 1.$$

Multiplying by b,

$$b = (ub)p + v(ab).$$

Since $p \mid ab$ it follows that

$$p \mid b.$$

Now the uniqueness of factorisation follows in the usual way, eg by induction on the minimal number, r say, of irreducibles in an expression for $a \in A$. Thus if

$$a = \epsilon p_1 \dots p_r = \eta q_1 \dots q_s.$$

then $p_1 \mid q_i$ for some i, and so

$$p_1 \sim q_i,$$

since q_i is irreducible. Now, on dividing both sides by p_1, the problem is reduced to a number expressible as a product of $< r$ irreducibles. ◀

4.6 Fractional ideals

It is convenient, and satisfying, to extend the notion of ideals from a number ring A to the corresponding number field $\mathbb{Q}(\alpha)$, ie the field of fractions of A.

We suppose in this Section that A is an integral domain with field of fractions k.

Definition 4.8. *A non-empty subset $\mathfrak{c} \subset k$ is said to be a* fractional ideal *if*

$$\mathfrak{c} = c\mathfrak{a}$$

for some ideal $a \subset A$, and some $c \in k^\times$.

Evidently a non-zero ideal $\mathfrak{a} \subset A$ is a fractional ideal; the notion *extends* the concept of an ideal.

Most of our results on fractional ideals follow immediately from the corresponding result for ordinary ideals, and will be given without proof.

Proposition 4.14. *If $\mathfrak{c}, \mathfrak{d} \subset k$ are fractional ideals then so is*

$$\mathfrak{cd} = \{c_1 d_1 + \cdots + c_r d_r : c_1, \ldots, c_r \in \mathfrak{c},\ d_1, \ldots, d_r \in \mathfrak{d}\}.$$

Definition 4.9. *If $\mathfrak{c} \subset k$ is a fractional ideal then we set*

$$\mathfrak{c}^{-1} = \{c \in k^\times : c\mathfrak{c} \subset \mathfrak{a}\}.$$

Proposition 4.15. *If $\mathfrak{c}$ is a fractional ideal then so is $\mathfrak{c}^{-1}$.*

If $\mathfrak{c}$ is a fractional ideal then by definition

$$\mathfrak{c}\ \mathfrak{c}^{-1} \subset A.$$

Definition 4.10. *The fractional ideal $\mathfrak{c} \subset k$ is said to be* invertible *if*

$$\mathfrak{c}\ \mathfrak{c}^{-1} = A.$$

Proposition 4.16. *The invertible fractional ideals in k form a group.*

Proposition 4.17. *If the fractional ideal $\mathfrak{c}$ is invertible then so is $c\mathfrak{c}$ for any $c \in k^\times$.*

Proposition 4.18. *The fractional ideal $\mathfrak{c}$ is invertible if and only if there is a fractional ideal $\mathfrak{d}$ such that*

$$\mathfrak{cd} = (c) = cA$$

for some $c \in k^\times$.

Remark. The notation (c) for cA is somewhat ambiguous, but unlikely to cause confusion in this context.

Proposition 4.19. *If A is a number-ring, then every fractional ideal is invertible.*

Proof ▶. It is sufficient to show that every non-zero ideal $\mathfrak{a} \in A$ is invertible.

Lemma 6. *If $\mathfrak{a} \subset A$ is a proper ideal (ie $\mathfrak{a} \neq (0), (1)$) then*

$$\mathfrak{a}^{-1} \not\subset A.$$

Proof ▶ Since $\mathfrak{a} \subset \mathfrak{p}$ for some maximal ideal $\mathfrak{p}$, and

$$\mathfrak{p}^{-1} \subset \mathfrak{a}^{-1},$$

it is sufficient to prove the result for a maximal ideal $\mathfrak{p}$.

Choose $a \in \mathfrak{p},\ a \neq 0$. By Proposition **??**, we can find maximal ideals $\mathfrak{p} = \mathfrak{p}_1, \mathfrak{p}_2, \ldots, p_r$ such that

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \subset (a).$$

Let us suppose that this is a minimal expression of this form, ie with minimal $e_1 + \cdots + e_r$. Since $a \in \mathfrak{p}$, $\mathfrak{p}$ must be among the primes on the left, say $\mathfrak{p} = \mathfrak{p}_1$.

But now

$$\mathfrak{p}_1^{e_1 - 1} \cdots \mathfrak{p}_r^{e_r} \not\subset (a).$$

◀

◀

Chapter 5

Dedekind's Theorem

We suppose throughout this Chapter that A is an integral domain, with field of fractions k. Of course we are interested primarily in the case of a number-ring A and its field of fractions $k = \mathbb{Q}(\alpha)$.

Definition 5.1. *A integral domain A is said to be a* Dedekind domain *if every non-zero ideal $\mathfrak{a} \in A$ is expressible as a product of prime ideals:*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

5.1 Fractional ideals

Definition 5.2. *A subset $\mathfrak{a} \in k$ is said to be a* fractional ideal *if $c\mathfrak{a}$ is an ideal in A for $c \in k^\times$.*

Proposition 5.1. *If $\mathfrak{a}, \mathfrak{b} \in k$ are fractional ideals then so is*

$$\mathfrak{ab} = \{a_1b_1 + \cdots a_rb_r : a_1, \ldots, a_r \in \mathfrak{a},\ b_1, \ldots, b_r \in \mathfrak{b}\}.$$

Proof ▶. If $a\mathfrak{a}, b\mathfrak{b}$ are ideals in A, then so is

$$(ab)(\mathfrak{ab}).$$

◀

Proposition 5.2. *If $c \in k^\times$ then*

$$(c) = cA$$

is a fractional ideal.

Proof ▶. This follows at once, since

$$c^{-1}(c) = A.$$

◀

Definition 5.3. *The fractional ideal* $\mathfrak{a}$ *is said to be* invertible *if there is a fractional ideal* $\mathfrak{b}$ *such that*

$$\mathfrak{ab} = (1) = A.$$

Proposition 5.3. *If the fractional ideal* $\mathfrak{a}$ *is invertible if and only if*

$$\mathfrak{ab} = (c)$$

for some fractional ideal $\mathfrak{b}$ *and some* $c \in k^\times$.

Proof ▶. If $\mathfrak{a}$ is invertible then

$$\mathfrak{ab} = (1)$$

for some fractional ideal $\mathfrak{b}$.

Conversely, if

$$\mathfrak{ab} = (c)$$

then

$$\mathfrak{a}(c^{-1}\mathfrak{b}) = (1).$$

◀

Proposition 5.4. *If the fractional ideal* $\mathfrak{a}$ *is invertible then it is finitely-generated.*

Proof ▶. Suppose

$$\mathfrak{ab} = (1).$$

Then

$$a_1b_1 + \cdots + a_rb_r = 1$$

for some elements $a_1, \ldots, a_r \in A,\ b_1, \ldots, b_r \in B$.

If follows that $a_1, \ldots, a_r$ generate $\mathfrak{a}$:

$$\mathfrak{a} = a_1A + \cdots + a_rA.$$

For suppose $a \in \mathfrak{a}$. Then

$$\begin{aligned} a &= a(a_1b_1 + \cdots + a_rb_r) \\ &= (ab_1)a_1 + \cdots + (ab_r)a_r. \end{aligned}$$

Since $ab_i \in A$ this establishes the result. ◀

Definition 5.4. *If $\mathfrak{a} \subset k$ is a fractional ideal we set*

$$\mathfrak{a}^{-1} = \{x \in k : x\mathfrak{a} \subset A\}.$$

Proposition 5.5. *If $\mathfrak{a} \subset k$ is a non-zero fractional ideal then so is $\mathfrak{a}^{-1}$.*

Proof ▶. Suppose $c \in \mathfrak{a},\ c \neq 0$. Then

$$x\mathfrak{a} \subset A \implies xc \in A.$$

with $d \in A$.

$$c\mathfrak{a}^{-1} \subset A.$$

It is readily verified that

$$c, d \in \mathfrak{a}^{-1} \implies c + d \in \mathfrak{a}^{-1},$$
$$a \in A, c \in \mathfrak{a}^{-1} \implies ac \in \mathfrak{a}^{-1}.$$

If follows that $c\mathfrak{a}^{-1}$ is an ideal in A, and so $\mathfrak{a}^{-1}$ is a fractional ideal. ◀

Proposition 5.6. *The non-zero fractional ideal $\mathfrak{a} \subset k$ is invertible if and only if*

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

Proof ▶. Suppose

$$\mathfrak{a}\mathfrak{b} = A.$$

Then

$$\mathfrak{b} \subset \mathfrak{a}^{-1}$$

from the definition of $\mathfrak{a}^{-1}$.

Hence

$$\mathfrak{a}\mathfrak{a}^{-1} \supset \mathfrak{a}\mathfrak{b} = A.$$

But

$$\mathfrak{a}\mathfrak{a}^{-1} \subset A,$$

again from the definition of $\mathfrak{a}^{-1}$. Hence

$$\mathfrak{a}\mathfrak{a}^{-1} = A.$$

◀

Proposition 5.7. *The integral domain A is a Dedekind domain if and only if every non-zero fractional ideal is invertible.*

Proof ▶. Suppose first that A is a Dedekind domain. It is sufficient to show that any non-zero ideal $\mathfrak{a} \subset A$ is invertible; for then

$$(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1}.$$

Choose any $a \in \mathfrak{a},\ a \neq 0$. Then

$$(a) \subset \mathfrak{a}.$$

It follows on expressing both (a) and $\mathfrak{a}$ as products of prime ideals that

$$(a) = \mathfrak{a}\mathfrak{b},$$

where $\mathfrak{b} \subset A$ is an ideal. Hence $\mathfrak{a}$ is invertible, by Proposition 5.3.

Conversely, suppose every non-zero fractional ideal is invertible. Then every ideal is finitely-generated by Proposition 5.4. Hence A is a noetherian ring.

Now suppose $\mathfrak{a} \subset A$ is an ideal. We show first that $\mathfrak{a}$ is a product of prime ideals.

If $\mathfrak{a}$ is prime there is nothing to prove. Otherwise, by Proposition **??**, we can find a maximal (and therefore prime) ideal $\mathfrak{p}_1$ such that

$$\mathfrak{a} \subset \mathfrak{p}_1.$$

Then

$$\mathfrak{a} \subset \mathfrak{p}_1^{-1}\mathfrak{a}.$$

Moreover, this inclusion is strict; for otherwise, on multiplying each side by $\mathfrak{a}^{-1}$,

$$A = \mathfrak{p}_1^{-1},$$

so that

$$\mathfrak{p}_1^{-1}\mathfrak{p}_1 = \mathfrak{p}_1,$$

contradicting the invertibility of $\mathfrak{p}_1$.

If $p_1^{-1}\mathfrak{a}$ is prime, say

$$\mathfrak{p}_1^{-1}\mathfrak{a} = \mathfrak{p}_2,$$

then

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2,$$

on multiplying each side by $\mathfrak{p}_1$.

If not, we can find a maximal (and therefore prime) ideal $\mathfrak{p}_2$ such that

$$\mathfrak{p}_1^{-1}\mathfrak{a} \subset \mathfrak{p}_2.$$

Again,

$$\mathfrak{p}_1^{-1}\mathfrak{a} \subset \mathfrak{p}_2^{-1}p_1^{-1}\mathfrak{a},$$

with strict inclusion.

If the ideal on the right is prime, say

$$\mathfrak{p}_2^{-1}\mathfrak{p}_1^{-1}\mathfrak{a} = \mathfrak{p}_3,$$

then

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3.$$

If not, then we continue as before.

Since A is noetherian, this process must end, yielding an expression

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

Finally, to prove uniqueness we argue by induction on the minimal number r of primes in an expression

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

Suppose we have a second expression

$$\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

where $s \geq r$. Then

$$q_1 \cdots \mathfrak{q}_s \subset \mathfrak{p}_1,$$

and so

$$\mathfrak{q}_i \subset \mathfrak{p}_1$$

for some i.

But then

$$\mathfrak{p}_1^{-1}\mathfrak{q}_i \subset \mathfrak{p}_1^{-1}\mathfrak{p}_1 = A,$$

ie

$$\mathfrak{b} = \mathfrak{p}_1^{-1}\mathfrak{q}_i$$

is either the whole of A, or an ideal in A, which can be expressed as a product of prime ideals, say

$$\mathfrak{b} = \mathfrak{q}_1' \cdots \mathfrak{q}_t'$$

(where the product will be empty if $\mathfrak{b} = A$).

Thus

$$p_1^{-1}\mathfrak{a} = \mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_{i-1}\mathfrak{q}_{i+1} \cdots \mathfrak{q}_s\mathfrak{q}_1' \cdots \mathfrak{q}_t'.$$

But now, applying the inductive hypothesis, we must have $t = 0$, and the $\mathfrak{q}_j$ (for $j \neq i$) must be $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$ in some order. On multiplying by $\mathfrak{p}_1$ we deduce that the expression for $\mathfrak{a}$ is unique (up to order). ◀

In the course of this proof we have established two further results.

Proposition 5.8. *Every Dedekind domain is noetherian.*

Proposition 5.9. *In a Dedekind domain, every non-zero prime ideal is maximal.*

Proof ▶. This follows because we obtained an expression for $\mathfrak{a}$ as a product of maximal ideals. ◀

Theorem 5.1. *Each number ring A is a Dedekind domain.*

Proof ▶. ◀

Chapter 6

Dedekind's Theorem

6.1 Dedekind domains

Our aim in this Chapter is to show that *every number ring is a Dedekind domain*, according to the following definition.

Definition 6.1. *The integral domain A is said to be a* Dedekind domain *if every non-zero ideal $\mathfrak{a} \subset A$ is uniquely expressible (up to order) as a product of prime ideals:*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

6.2 Ideals in number rings

We suppose in the rest of this Chapter that A is a number ring, ie

$$A = \mathbb{Q}(\alpha) \cap \bar{Z}$$

where $\mathbb{Q}(\alpha)$ is a finite extension of $\mathbb{Q}$.

Proposition 6.1. *Every non-zero ideal $\mathfrak{a} \subset A$ contains a rational integer $n > 0$.*

Proof ▶. Take any non-zero element $\alpha \in \mathfrak{a}$. Since $\alpha \in \bar{\mathbb{Z}}$, it satisfies a minimal equation of the form

$$\alpha^d + a_1\alpha^{d-1} + \cdots + a_d = 0,$$

with $a_i \in \mathbb{Z}$. Then

$$a_d = -\alpha(\alpha^{d-1} + \cdots a_{d-1}) \in \mathfrak{a};$$

and $a_d \neq 0$, since otherwise α would satisfy an equation of lower degree. ◀

Proposition 6.2. *If $\mathfrak{a} \subset A$ is a non-zero ideal in the number ring A then the quotient-ring $A/\mathfrak{a}$ is finite.*

Proof ▶. We have to show that there are only a finite number of residue classes modulo $\mathfrak{a}$.

We know that, as an abelian group,

$$A \cong \mathbb{Z}^d,$$

where

$$d = \deg \mathbb{Q}(\alpha).$$

Let $e_1, \ldots, e_d$ be a basis for this abelian group, ie each element $a \in A$ is uniquely expressible in the form

$$a = z_1 e_1 + \cdots + z_d e_d,$$

with $z_i \in \mathbb{Z}$. By the last Proposition, there is a natural integer $n > 0$ in $\mathfrak{a}$. Let $r_i \in \{0, 1, \ldots, n-1\}$ be the remainder when z_i is divided by n, say

$$z_i = nq_i + r_i.$$

Then

$$\begin{aligned} a &= n(q_1 e_1 + \cdots + q_d e_d) + (r_1 e_1 + \cdots + r_d e_d) \\ &\equiv r_1 e_1 + \cdots + r_d e_d \bmod \mathfrak{a} \end{aligned}$$

since $n \in \mathfrak{a}$.

Thus each $a \in A$ is congruent $\bmod \mathfrak{a}$ to at least one of the n^d elements

$$r_1 e_1 + \cdots + r_d e_d \quad (0 \le r_i < n);$$

and so

$$\#(A/\mathfrak{a}) \le n^d.$$

◀

Definition 6.2. *We call*

$$\mathcal{N}(\mathfrak{a}) = \#(A/\mathfrak{a})$$

the norm *of the ideal $\mathfrak{a}$. By convention we also set*

$$\mathcal{N}((0)) = 0.$$

Proposition 6.3. *If $\mathfrak{a}, \mathfrak{b} \subset A$ are ideals with $\mathfrak{a} \subset \mathfrak{b}$ then*

$$\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{b}) \iff \mathfrak{a} = \mathfrak{b}.$$

Proof ►. This is trivial. If $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(b)$ then

$$x \equiv y \bmod \mathfrak{b} \implies x \equiv y \bmod \mathfrak{a}.$$

Thus

$$\begin{aligned} b \in \mathfrak{b} &\implies b \equiv 0 \bmod \mathfrak{b} \\ &\implies b \equiv 0 \bmod \mathfrak{a} \\ &\implies b \in \mathfrak{a}. \end{aligned}$$

◄

Corollary 6.1. *If* $\mathfrak{a} \neq (0)$ *then* $\mathcal{N}(\mathfrak{a}) \geq 1$*; and*

$$\mathcal{N}(\mathfrak{a}) = 1 \iff \mathfrak{a} = (1) = A.$$

6.3 Dedekind's Theorem

Proposition 6.4. *Every non-zero prime ideal* $\mathfrak{p}$ *in a number ring* A *is maximal.*

Proof ►. If $\mathfrak{p}$ is prime then $A/\mathfrak{p}$ is an integral domain, by Proposition **??**. Also $A/\mathfrak{p}$ is finite, by Proposition **??**.

Lemma 7. *A finite integral domain* A *is a field.*

Proof ► Suppose $a \in A,\ a \neq 0$. Consider the sequence

$$a, a^2, a^3, \cdots .$$

There must be a repeat (since A is finite), say

$$a^{n+r} = a^n,$$

where $r > 0$. Then

$$a^n(a^r - 1) = 0.$$

Hence

$$a^r = 1,$$

since $a^n = 0 \implies a = 0$. Thus a has an inverse

$$a^{-1} = a^{r-1}.$$

Hence A is a field. ◄

It follows from the Lemma that $A/\mathfrak{p}$ is field, and so $\mathfrak{p}$ is maximal, by Proposition **??**. ◀

Theorem 6.1. *Every number ring A is a Dedekind domain, ie each non-zero ideal $\mathfrak{a} \subset A$ is uniquely expressible (up to order) as a product of prime ideals:*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

Proof ▶. Suppose $\mathfrak{a} \neq (0)$.

Lemma 8. *There are only a finite number of ideals $\mathfrak{b} \supset \mathfrak{a}$; and in particular there are only a finite number of maximal ideals*

$$\mathfrak{p}_1, \ldots, \mathfrak{p}_r \supset \mathfrak{a}.$$

Proof ▶ There is a one-one correspondence between ideals $\mathfrak{b} \supset \mathfrak{a}$ and ideals in the quotient-ring $A/\mathfrak{a}$. But this ring is finite; so it only has a finite number of subsets, let alone ideals. ◀

Lemma 9. *We can find a product of maximal ideals*

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{a}.$$

Proof ▶ We argue by induction on $\mathcal{N}(\mathfrak{a})$.

If $\mathfrak{a}$ is prime then it is maximal by Proposition 6.4 and there is nothing to prove.

If $\mathfrak{a}$ is not prime then by definition there exist $u, v \in A$ such that

$$uv \in \mathfrak{a} \text{ but } u, v \notin \mathfrak{a}.$$

Thus

$$\mathfrak{a} = (\mathfrak{a} + (u))\,(\mathfrak{a} + (v))\,.$$

with both $\mathfrak{a} + (u)$, $\mathfrak{a} + (b)$ strictly larger than $\mathfrak{a}$.

By the inductive hypothesis we can find prime ideals

$$\mathfrak{p}_1 \ldots \mathfrak{p}_r \subset \mathfrak{a} + (u),\ \mathfrak{q}_1 \ldots \mathfrak{q}_s \subset \mathfrak{a} + (v),$$

and then

$$\mathfrak{p}_1 \ldots \mathfrak{p}_r \mathfrak{q}_1 \ldots \mathfrak{q}_s \subset \mathfrak{a}.$$

◀

Recall that if $\mathfrak{a} \subset A$ is a non-zero ideal then

$$\mathfrak{a}^{-1} = \{c \in k : c\,\mathfrak{a} \subset A\} \supset A.$$

Lemma 10. *If $\mathfrak{p} \subset A$ is a prime ideal then*

$$\mathfrak{p}^{-1} \neq A,$$

ie $\mathfrak{p}^{-1}$ is strictly greater than A.

Proof ▶ Choose $a \in \mathfrak{p}$, $a \neq 0$. By Lemma 9 we can find a product of maximal ideals

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (a) \subset \mathfrak{p},$$

where we may assume that r is minimal.

Then some

$$\mathfrak{p}_i \subset \mathfrak{p},$$

by Proposition **??**. Thus

$$\mathfrak{p} = \mathfrak{p}_i,$$

since $\mathfrak{p}_i$ is maximal. Let us re-order the $\mathfrak{p}_i$ (if necessary) so that $\mathfrak{p} = \mathfrak{p}_1$.

Choose

$$b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r, \quad b \notin \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = (a).$$

(This is possible, since $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subset (a)$ by the minimality of r.)

Then

$$b\,\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset (a).$$

Thus

$$\frac{b}{a}\,\mathfrak{p} \subset A,$$

and so

$$c = \frac{b}{a} \in \mathfrak{p}^{-1},$$

while

$$c \notin A$$

since $b \notin (a)$. ◀

Lemma 11. *Every maximal ideal $\mathfrak{p} \subset A$ is invertible:*

$$\mathfrak{p}^{-1}\mathfrak{p} = A.$$

Proof ▶ Since $A \subset \mathfrak{p}^{-1}$,

$$\mathfrak{p} \subset \mathfrak{p}^{-1}\mathfrak{p} \subset A.$$

Since $\mathfrak{p}$ is maximal, it follows that

$$\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p} \text{ or } A.$$

In the latter case $\mathfrak{p}$ is invertible.

If not then

$$\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}.$$

Suppose $c \in \mathfrak{p}^{-1}$. Then

$$c\,\mathfrak{p} = \mathfrak{p}.$$

But as an abelian group, $\mathfrak{p}$ is a finitely-generated subgroup of $\mathbb{C}$. It follows therefore from our criterion for an algebraic integer (Proposition **??**) that

$$c \in \bar{\mathbb{Z}},$$

ie

$$c \in \mathbb{Q}(\alpha) \cap \bar{\mathbb{Z}} = A.$$

Since this is true for all $c \in \mathfrak{p}^{-1}$,

$$\mathfrak{p}^{-1} \subset A,$$

contrary to the last Lemma.

We conclude that $\mathfrak{p}$ must be invertible. ◀

Lemma 12. *Every non-zero ideal $\mathfrak{a} \subset A$ is expressible as a product of prime ideals:*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

Proof ▶ We argue by induction on $\mathcal{N}(\mathfrak{a})$.

We know by Lemma 9 that we can find prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{a},$$

where we may assume that r is minimal.

Multiplying by $\mathfrak{p}_1^{-1}$ (and using the fact that $\mathfrak{p}_1$ is invertible),

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset \mathfrak{p}^{-1}\mathfrak{a}.$$

But $p^{-1}\mathfrak{a}$ is strictly larger than $\mathfrak{a}$, by the minimality of r.

Thus by our inductive hypothesis,

$$\mathfrak{p}_1^{-1}\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

where the $\mathfrak{q}_j$ are prime. Hence

$$\mathfrak{a} = \mathfrak{p}_1(\mathfrak{p}_1^{-1}\mathfrak{a}) = \mathfrak{p}_1\mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

◀

Lemma 13. *The expression of a non-zero ideal*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

as a product of prime ideals is unique up to order.

Proof ▶ We argue by induction on the minimal r in such an expression.
Suppose

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Then

$$\mathfrak{q}_1 \cdots \mathfrak{q}_s \subset \mathfrak{p}_1 \implies \mathfrak{q}_j \subset \mathfrak{p}_1$$

for some j.
Since $\mathfrak{q}_j$ is maximal (by Proposition 6.4) it follows that

$$\mathfrak{q}_j = \mathfrak{p}_1.$$

We may assume, on re-ordering the $\mathfrak{q}_j$ if necessary, that

$$\mathfrak{q}_1 = \mathfrak{p}_1.$$

But now

$$\mathfrak{p}_1^{-1}\mathfrak{a} = \mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s,$$

and the result follows from the inductive hypothesis. ◀

That concludes the proof of Dedekind's Theorem; we have shown that each non-zero ideal is uniquely expressible (up to order) as a product of prime ideals:

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

◀

6.4 First consequences

We continue to assume that A is a number ring, with field of fractions k.

Proposition 6.5. *Suppose $\mathfrak{a}, \mathfrak{b} \subset A$ are ideals. Then*

$$\mathfrak{a} \subset \mathfrak{b} \iff \mathfrak{a} = \mathfrak{b}\mathfrak{c}$$

for some ideal $\mathfrak{c} \subset A$.

Proof ▶. It is clear that

$$\mathfrak{bc} \subset \mathfrak{b}.$$

Conversely, suppose

$$\mathfrak{b} = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

We argue by induction on r

The result is trivial if $r = 0$, ie $\mathfrak{a} = A$.

If $r \geq 1$ then on multiplying by $\mathfrak{p}_1^{-1}$,

$$\mathfrak{p}_1^{-1}\mathfrak{a} \subset \mathfrak{p}_1^{-1}\mathfrak{b} = \mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

Hence, by the inductive hypothesis,

$$\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{p}^{-1}\mathfrak{bc}$$

for some ideal c, and so, on multiplying by $\mathfrak{p}_1$,

$$\mathfrak{a} = \mathfrak{bc}.$$

◀

We may say that $\mathfrak{b}$ *divides* a if $\mathfrak{a} \subset \mathfrak{b}$, and write

$$\mathfrak{b} \mid \mathfrak{a} \iff \mathfrak{a} \subset \mathfrak{b}.$$

Similarly, we can extend the notation $p^e \mid\mid n$ for exact division by a rational prime p, by writing (for a non-zero prime ideal $\mathfrak{p}$)

$$\mathfrak{p}^e \mid\mid \mathfrak{a} \text{ if } \mathfrak{p}^e \mid \mathfrak{a} \text{ but } \mathfrak{p}^{e+1} \nmid \mathfrak{a}.$$

We can express any non-zero ideal in the form

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{e_i},$$

where the product extends over all non-zero prime ideals $\mathfrak{p}_i$, with the understanding that $e_i \in \mathbb{N}$, with $e_i = 0$ for all but a finite number of e_i. (We may say that e_i is *almost always* 0.)

Proposition 6.6. *Suppose* $\mathfrak{a}, \mathfrak{b} \subset A$ *are non-zero ideals, with*

$$\mathfrak{a} = \prod \mathfrak{p}_i^{e_i}, \quad \mathfrak{b} = \prod \mathfrak{p}_i^{f_i}.$$

Then

$$\mathfrak{a} + \mathfrak{b} = \prod \mathfrak{p}_i^{\min(e_i, f_i)}.$$

Proof ▶. Suppose

$$\mathfrak{a} + \mathfrak{b} = \prod \mathfrak{p}_i^{g_i}.$$

Then

$$\mathfrak{a}, \mathfrak{b} \subset \mathfrak{a} + \mathfrak{b} \implies g_i \leq e_i, f_i \implies g_i \leq \min(e_i, f_i).$$

On the other hand, suppose $e_i \leq f_i$. We can find

$$a \in \mathfrak{a} \setminus \mathfrak{a}\mathfrak{p}_i.$$

Then

$$\mathfrak{p}_i^{e_i} \mid\mid (a).$$

Since $a \in \mathfrak{a} + \mathfrak{b}$, it follows that

$$\mathfrak{p}_i^{e_i} \mid\mid \mathfrak{a} + \mathfrak{b}.$$

Thus

$$g_i = e_i = \min(e_i, f_i).$$

◀

In view of this result, it is natural to write

$$\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}.$$

Proposition 6.7. *Every ideal $\mathfrak{a} \subset A$ is generated by at most 2 elements:*

$$\mathfrak{a} = (a, b).$$

Proof ▶. If $\mathfrak{a} = (0)$ the result is trivial. Otherwise choose any non-zero $a \in \mathfrak{a}$.

By Proposition 6.5, $\mathfrak{a} \mid (a)$; say

$$\mathfrak{a} = (a)\ \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are distinct prime ideals.

We only have to choose b to "avoid" this finite set of ideals.

Lemma 14. *We can find $b \in \mathfrak{a}$ such that*

$$\mathfrak{b} = (a)\ \mathfrak{q}_1^{f_1} \cdots \mathfrak{q}_s^{f_s},$$

where none of the q_j's is equal to any of the $\mathfrak{p}_i$'s.

Proof ▶ For each i, choose

$$b_i \in \mathfrak{a}\mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \cdots \mathfrak{p}_r \setminus \mathfrak{a}\mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

(This is possible, by the uniqueness part of Dedekind's Theorem.) Thus

$$b_j \in \mathfrak{a}\mathfrak{p}_i \iff j \neq i.$$

Set

$$b = b_1 + \cdots + b_r.$$

Since all the b_j except b_i are in $\mathfrak{a}\mathfrak{p}_i$, while b_i is not, it follows that

$$b \notin \mathfrak{a}\mathfrak{p}_i$$

for each i.

Thus (b) is of the form specified in the Lemma; no additional powers of the $\mathfrak{p}_i$'s occur in it apart from those in $\mathfrak{a}$. ◀

Let b be as in the Lemma. Suppose $\mathfrak{p}$ is a non-zero prime ideal, and suppose

$$\mathfrak{p}^e \mid\mid \mathfrak{a},\ \mathfrak{p}^f \mid\mid (a),\ \mathfrak{p}^g \mid\mid (b).$$

Then $f, g \geq e$, and we have chosen b so that if $f > e$ then $g = e$. Thus

$$e = \min(f, g).$$

Since this is true for all $\mathfrak{p}$,

$$(a, b) = (a) + (b) = \gcd\left((a), (b)\right) = \mathfrak{a}.$$

◀

Dedekind's Theorem extends at once to fractional ideals.

Proposition 6.8. *Every non-zero fractional ideal $\mathfrak{a} \subset k$ can be expressed uniquely in the form*

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{e_i},$$

where $e_i \in \mathbb{Z}$, with $e_i = 0$ for all but a finite number of e_i.

Proof ▶. By definition,

$$\mathfrak{a} = \frac{a}{b}\,\mathfrak{b}$$

where $a.b \in A$ and $\mathfrak{b} \subset A$ is an 'ordinary' ideal.

Lemma 15. *Every non-zero ideal $\mathfrak{a} \subset A$ is invertible; if*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

then

$$\mathfrak{a}^{-1} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}.$$

Proof ▶ This follows at once from the fact that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \; \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1} = (1).$$

◀

The result follows from the Lemma, since

$$\begin{aligned} \mathfrak{a} &= \frac{r}{s}\mathfrak{b} \\ &= (s)^{-1}(r\mathfrak{b}). \end{aligned}$$

(We leave the uniqueness of the expression as a — very simple — exercise.)

◀

6.5 Prime ideals and rational primes

Proposition 6.9. *Each non-zero prime ideal $\mathfrak{p}$ contains exactly one rational prime p.*

Proof ▶. We know that there is a non-zero rational integer $n \in \mathfrak{p}$, by Proposition DT?. We may assume that $n > 0$ since $n \in \mathfrak{p} \implies -n \in \mathfrak{p}$. By the Fundamental Theorem of Arithmetic,

$$n = p_1^{e_1} \cdots p_r^{e_r},$$

where $p_1, \ldots, p_r$ are rational primes Hence

$$p_i \in \mathfrak{p}$$

by the definition of a prime ideal.

Suppose there are two distinct rational primes

$$p, q \in \mathfrak{p}.$$

Then $\gcd(p, q) = 1$, and so we can find $u, v \in \mathbb{Z}$ such that

$$up + vq = 1.$$

But then

$$p, q \in \mathfrak{p} \implies 1 \in \mathfrak{p},$$

contrary to the definition of a prime ideal. ◀

We may say that the prime ideal $\mathfrak{p}$ *belongs to* p.

Appendix A

Continued fractions

A.1 Finite continued fractions

Definition A.1. *We write*

$$[a_0, a_1, \ldots, a_N]$$

for the finite continued fraction

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_N}}}}$$

We call a_n *the* nth quotient *of* α*, and we call*

$$x_n = [a_0, a_1, \ldots, a_n]$$

the nth convergent *to* α *(for* $0 \leq n \leq N$*). Finally, for* $0 \leq n, N$ *we call*

$$\alpha_n = [a_n, \ldots, a_N]$$

the nth remainder *for* α

Example. The continued fraction

$$[2, 1, 3, 2] = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2}}}$$

represents the rational number

$$2 + \cfrac{1}{1 + \cfrac{2}{7}} = 2 + \frac{7}{9} = \frac{25}{9}.$$

Although we are mainly interested in the case where

$$a_i \in \mathbb{Z},\ a_1, a_2, \ldots, a_n \geq 1$$

(when we shall speak of α as a *simple finite continued fraction*), we also need to consider α as a rational function of $a_0, a_1, \ldots, a_n$. Thus

$$[a_0] = a_0,$$
$$[a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1},$$

etc.

Proposition A.1. *For* $0 \leq n < N$,

$$[a_0, \ldots, a_N] = [a_0, \ldots, a_{n-1}, \alpha_n].$$

Proof ▶. This is what we get if we end the computation at

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{\alpha_n}}}}$$

◀

Proposition A.2. *The nth convergent*

$$x_n = \frac{p_n}{q_n},$$

where p_n, q_n *are defined by the recursion relations*

$$p_n = a_n p_{n-1} + p_{n-2},$$
$$q_n = a_n q_{n-1} + q_{n-2},$$

with the initial conditions

$$p_0 = a_0,\ q_0 = 1$$
$$p_1 = a_0 a_1 + 1,\ q_1 = a_1.$$

Proof ▶. We argue by induction on n. We have

$$\begin{aligned} x_{n+1} &= [a_0, \ldots, a_n, a_{n+1}] \\ &= \left[a_0, \ldots, a_n + \frac{1}{a_{n+1}}\right] \\ &= \frac{(a_n + \frac{1}{a_{n+1}})p_{n-1} + p_{n-2}}{(a_n + \frac{1}{a_{n+1}})q_{n-1} + q_{n-2}} \\ &= \frac{(a_n a_{n+1} + 1)p_{n-1} + a_{n+1}p_{n-2}}{(a_n a_{n+1} + 1)q_{n-1} + a_{n+1}q_{n-2}} \\ &= \frac{a_{n+1}(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1}(a_n q_{n-1} + q_{n-2}) + q_{n-1}} \\ &= \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}}. \end{aligned}$$

◀

Proposition A.3. *For $n \geq 0$,*

$$p_{n+1}q_n - q_{n+1}p_n = (-1)^n,$$

ie

$$x_{n+1} - x_n = \frac{(-1)^n}{q_{n+1}q_n}.$$

Proof ▶. Substituting for p_{n+1}, q_{n+1},

$$\begin{aligned} p_{n+1}q_n - q_{n+1}p_n &= (a_{n+1}p_n + p_{n-1})q_n - (a_{n+1}q_n + q_{n-1})p_n \\ &= p_{n-1}q_n - q_{n-1}p_n \\ &= -(p_n q_{n-1} - q_n p_{n-1}). \end{aligned}$$

Thus by repetition (or induction on n),

$$\begin{aligned} p_{n+1}q_n - q_{n+1}p_n &= (-1)^n(p_1 q_0 - q_1 p_0) \\ &= (-1)^n((a_1 a_0 + 1) - a_1 a_0) \\ &= (-1)^n. \end{aligned}$$

◀

Corollary A.1. *If α is a simple continued fraction, ie $a_i \in \mathbb{Z}$ with $a_1, \ldots, a_N \geq 1$, then $p_n, q_n \in \mathbb{Z}$ and*

$$\gcd(p_n, q_n) = 1$$

with $q_n \geq 1$; in other words, the fraction

$$x_n = \frac{p_n}{q_n}$$

is in its lowest terms.

Proof ▶. Since

$$p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1},$$

any common factor of p_n, q_n would also divide $(-1)^{n-1}$; while it follows by induction from

$$q_{n+1} = a_{n+1} q_n + q_{n-1}$$

that $q_n \geq 1$. ◀

Example. Continuing the previous example, the successive convergents to $[2, 1, 3, 2]$ are

$$\begin{aligned} 2 &= \frac{2}{1}, \\ [2, 1] &= \frac{3}{1}, \\ [2, 1, 3] &= \frac{11}{4}. \\ [2, 1, 3, 2] &= \frac{25}{9}. \end{aligned}$$

Thus

$$(p_0, q_0) = (2, 1),\ (p_1, q_1) = (3, 1),\ (p_2, q_2) = (11, 4),\ (p_3, q_3) = (25, 9).$$

There is an intimate relation between the continued fraction for $x = \frac{p}{q}$ and the Euclidean Algorithm for the numbers p, q. In fact the successive quotients in the algorithm are precisely the numbers a_i in the continued fraction.

Example. Suppose $x = \frac{23}{17}$. Then the Euclidean Algorithm for the numbers $23, 17$ runs as follows:

$$\begin{aligned} 23 &= 1 \cdot 17 + 6, \\ 17 &= 2 \cdot 6 + 5, \\ 6 &= 1 \cdot 5 + 1, \\ 5 &= 5 \cdot 1. \end{aligned}$$

This corresponds to the continued fraction expression

$$\frac{23}{17} = [1,2,1,5] = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{5}}}.$$

Proposition A.4. *Each rational number*

$$x = \frac{p}{q} \in \mathbb{Q}$$

can be expressed in just two ways as a continued fraction

$$x = [a_0, a_1, \ldots, a_n] \qquad (a_0 \in \mathbb{Z},\ a_1, \ldots, a_n \in \mathbb{N} \setminus \{0\}),$$

one with last quotient $a_n = 1$, and one with last quotient $a_n > 1$. as a finite continued fraction

Proof ▶. Note that if $a_n > 1$ then

$$[a_0, \ldots, a_{n-1}, a_n] = [a_0, \ldots, a_{n-1}, a_n - 1, 1].$$

As we have just seen, the euclidean algorithm yields a continued fraction for p/q, with final convergent $a_n > 1$ (unless $\mathfrak{p}/q \in \mathbb{Z}$).

It remains to show that there is just one continued fraction for p/q with final quotient $a_n > 1$. We argue by induction on the length $n + 1$ of the shortest continued fraction for x.

Suppose

$$x = [a_0, \ldots, a_n] = [a'_0, \ldots, a'_{n'}].$$

Since

$$a_0 \leq [a_0, a_1, \ldots, a_n] < a_0 + 1,$$

we must have

$$a_0 = [x] = a'_0.$$

Thus

$$x = a_0 + \frac{1}{\alpha_1} = a_0 + \frac{1}{\alpha'_1},$$

where

$$\alpha = [a_1, \ldots, a_n], \quad \alpha' = [a'_1, \ldots, a'_{n'}].$$

Hence

$$\alpha = \alpha',$$

and the result follows by induction. ◀

Proposition A.5. *The even convergents $x_0, x_2, x_4, \ldots$ to*

$$\alpha = [a_0, \ldots, a_n]$$

are monotonically increasing, while the odd convergents $x_1, x_3, x_5, \ldots$ are monotonically decreasing. Moreover, every even convergent is less then every odd convergent, and α is sandwiched between the even and odd convergents:

$$x_0 < x_2 < x_4 < \cdots < \alpha < \cdots < x_5 < x_3 < x_1.$$

Proof ▶. By Proposition A.3,

$$x_n - x_{n-1} = \frac{(-1)^{n-1}}{q_n q_{n-1}}, x_{n-1} - x_{n-2} \qquad = \frac{(-1)^n}{q_{n-1} q_{n-2}}.$$

Thus

$$\begin{aligned} x_n - x_{n-2} &= \frac{(-1)^n}{q_{n-1}} \left(\frac{1}{q_{n-2}} - \frac{1}{q_n} \right) \\ &= (-1)^n \epsilon_n, \end{aligned}$$

where $\epsilon_n > 0$ since the q_n are increasing (as $q_{n+1} = a_{n+1} q_n + q_{n-1} \geq q_n + q_{n-1}$). It follows that x_n is increasing for even n, and decreasing for odd n.

Also if n is even then

$$x_{n+1} - x_n = \frac{1}{q_{n+1} q_n} > 0,$$

ie

$$x_{n+1} > x_n.$$

It follows that

$$x_{2r} < x_{2s+1}$$

for all r, s.

Finally, the last convergent

$$\alpha = \frac{p_n}{q_n}$$

is in the middle of the chain, whether n is even or odd. ◀

A.2 Infinite continued fractions

So far we have been considering *finite* continued fractions, representing *rational* numbers. But it is easy now to pass to the infinite case.

Proposition A.6. *Suppose*

$$a_0, a_1, a_2, \dots$$

is an infinite sequence of integers, with $a_1, a_2, \cdots > 0$. *Then the sequence*

$$x_n = [a_0, \dots, a_n]$$

converges as $n \to infty$.

Proof ▶. It follows from the finite case that the even convergents x_{2r} are increasing, and

$$x_{2r} < x_1.$$

Hence the even convergents converge, say

$$x_{2r} \to l.$$

Similarly the odd convergents converge, say

$$x_{2s+1} \to L.$$

Also, since

$$|x_{n+1} - x_n| = \frac{1}{q_{n+1}q_n} \to 0$$

it follows that

$$L = l,$$

ie the sequence x_n converges. ◀

Definition A.2. *We write*

$$\alpha = [a_0, a_1, \dots]$$

if

$$x_n = [a_0, \dots, a_n] \to \alpha$$

as $n \to \infty$.

Thus the *infinite continued fraction* $[a_0, a_1, \dots]$ is said to have value α.

Proposition A.7. *The value of an infinite continued fraction* $[a_0, a_1, \dots]$ *is an irrational number* $\alpha \in \mathbb{R}$*; and every irrational* $\alpha \in \mathbb{R}$ *has a unique expression as an infinite continued fraction.*

Proof ▶. Observe that we can carry out the Euclidean Algorithm — perhaps we should call it the Continued Fraction Algorithm — for any $\alpha \in \mathbb{R}$. Thus we set

$$\begin{aligned} a_0 &= [\alpha], \\ a_1 &= \left[\frac{1}{\alpha - a_0}\right], \end{aligned}$$

etc. If α is irrational, this process will never end, and we will obtain an infinite sequence

$$[a_0, a_1, \dots].$$

By Proposition A.5, the even convergents x_{2r} and the odd convergents x_{2s+1} will converge to the same limit, α' say.

We don't really need the following Lemma to see that $\alpha' = \alpha$, but we shall find the result useful later.

Lemma 16. *Let*

$$f(x) = [a_0, \dots, a_n, x].$$

If n *is even then* $f(x)$ *is strictly increasing for* $x \geq 1$*; while if* n *is odd then* $f(x)$ *is strictly decreasing for* $x \geq 1$*.*

Proof ▶ We argue by induction on n. By Proposition A.1,

$$f(x) = a_0 + \frac{1}{g(x)},$$

where

$$g(x) = \alpha_1 = [a_1, \dots, a_n].$$

If n is even then by the inductive hypothesis $g(x)$ is decreasing for $x \geq 1$, and so $f(x)$ is increasing. Similarly, if n is odd then by the inductive hypothesis $g(x)$ is increasing for $x \geq 1$, and so $f(x)$ is decreasing. ◀

If follows from this Lemma that

$$x_n = [a_0, \dots, a_n] \leq \alpha = [a_0. \dots, \alpha_n],$$

if n is odd, while

$$x_n = [a_0, \dots, a_n] \geq \alpha = [a_0. \dots, \alpha_n],$$

if n is even.

Thus both α, α' are both sandwiched between the odd convergents and the even convergents, and so

$$\alpha = \alpha',$$

ie

$$\alpha = [a_0, a_1, \dots].$$

To see that the continued fraction for irrational $\alpha \in \mathbb{R}$ is unique, we argue by induction, our hypothesis being that if

$$\alpha = [a_0, a_1, \dots] = [a'_0, a'_1, \dots]$$

then $a_i = a'_i$ for $i = 0, 1, \dots, n$.

This holds trivially for $n = 0$ since

$$a_0 = [\alpha].$$

Now suppose

$$\alpha = [a_0, \dots, a_n, a_{n+1}, \dots] = [a_0, \dots, a_n, a'_{n+1}, \dots].$$

By Proposition A.1,

$$\alpha = a_0 + \frac{1}{\alpha_1} = a_0 + \frac{1}{\alpha'_1},$$

where

$$\alpha_1 = [a_1, \dots, a_n, a_{n+1}, \dots], \quad \alpha'_1 = [a_1, \dots, a_n, a'_{n+1}, \dots].$$

Since

$$\alpha_1 = \alpha'_1$$

it follows from the inductive hypothesis that

$$a_{n+1} = a'_{n+1}.$$

◀

Thus each irrational number has a unique expression as a continued fraction while each rational number, as we have seen, has two such expressions.

A.3 Diophantine approximation

Diophantine approximation is the study of rational approximations to real numbers. The successive convergents to α are very good approximants.

Proposition A.8. *The convergents p_n/q_n to α all satisfy*

$$|\alpha - \frac{p_n}{q_n}| < \frac{1}{q_n^2}.$$

Proof ▶. Since α lies between x_n and x_{n+1},

$$\begin{aligned} |\alpha - x_n| &< |x_{n+1} - x_n| \\ &= \frac{1}{q_{n+1}q_n} \\ &< \frac{1}{q_n^2}. \end{aligned}$$

◀

Remarks:

1. Since
$$q_{n+1} \geq a_{n+1}q_n + q_{n-1},$$
we actually we have the stronger result
$$|\alpha - \frac{p_n}{q_n}| < \frac{1}{a_{n+1}q_n^2}.$$

2. One can establish the Proposition without using continued fractions by an argument due to Kronecker. Given $N > 0$, divide the interval $[0, 1)$ into N equal sub-intervals:
$$[0, 1/N), [1/N, 2/N), \ldots, [(N-1)/N].$$
Let $\{x\}$ denote the fractional part of $x \in \mathbb{R}$:
$$\{x\} = x - [x].$$
Consider the $N + 1$ fractional parts
$$\{0\alpha\}, \{1\alpha\}, \ldots, \{N\alpha\}.$$

Two of these, say $\{r\alpha\}, \{s\alpha\}$ (where we may assume that $r < s$) must lie in the same sub-interval. But then

$$|\{r\alpha\} - \{s\alpha\}| < \frac{1}{N}.$$

ie

$$|(r-s)\alpha - [r\alpha] - [s\alpha]| < \frac{1}{N},$$

ie

$$|q\alpha - p| < \frac{1}{N},$$

where

$$q = r - s \leq N,\ p \in \mathbb{Z}.$$

Thus

$$|q\alpha - p| < \frac{1}{q},$$

ie

$$|\alpha - \frac{p}{q}| < 1/q^2,$$

Proposition A.9. *Of two successive convergents p_n/q_n to α one at least will satisfy*

$$|\alpha - \frac{p_n}{q_n}| < \frac{1}{2q_n^2}.$$

Proof ▶. Suppose to the contrary,

$$|\alpha - \frac{p_n}{q_n}| < \frac{1}{2q_n^2}, \quad |\alpha - \frac{p_{n+1}}{q_{n+1}}| < \frac{1}{2q_{n+1}^2}.$$

Since α lies between the two convergents,

$$|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}| < \frac{1}{2q_{n+1}^2} + \frac{1}{2q_n^2}.$$

But

$$|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}| = \frac{1}{q_{n+1}q_n}.$$

Thus

$$\frac{1}{2q_{n+1}^2} + \frac{1}{2q_n^2} < \frac{1}{q_{n+1}q_n},$$

ie

$$q_{n+1}^2 + q_n^2 < 2q_{n+1}q_n,$$

ie

$$(q_{n+1} - q_n)^2 < 0,$$

which is impossible. ◀

Proposition A.10. *If*

$$|\alpha - \frac{p}{q}| < \frac{1}{2q^2}$$

then p/q is a convergent to α.

Proof ▶. Let the continued fraction for p/q be

$$\frac{p}{q} = [a_0, \ldots, a_n],$$

where we choose n even or odd according as

$$\alpha > \frac{p}{q} \text{ or } \alpha < \frac{p}{q}.$$

Let the last 2 convergents to the continued fraction be

$$\frac{p_{n-1}}{q_{n-1}}, \ \frac{p_n}{q_n} = \frac{p}{q}.$$

(Our choice of n means that α lies on the same side of p/q as the penultimate convergent p_{n-1}/q_{n-1}.)

Consider the function

$$f(x) = [a_0, \ldots, a_n, x] = \frac{p_n x + p_{n-1}}{q_n x + q_{n-1}}.$$

This has an inverse of the same form; to be precise,

$$f^{-1}(x) = (-1)^{n-1} \frac{q_{n-1}x - q_n}{p_{n-1}x - p_n}.$$

(More accurately, $f(x)$ defines a bijective map from the real projective line $\mathbb{R} \cup \{\infty\}$ to itself.)

In particular, there is exactly one $\theta \in \mathbb{R}$ such that

$$\alpha = f(\theta) = \frac{p_n\theta + p_{n-1}}{q_n\theta + q_{n-1}}.$$

If we can show that

$$\theta > 1,$$

with continued fraction

$$\theta = [b_0, b_1, \dots]$$

then it will follow from Proposition A.1 that

$$\alpha = [a_0, \dots, b_1, b_1, \dots],$$

implying in particular that

$$\frac{p}{q} = \frac{p_n}{q_n}$$

is a convergent to α.

Since

$$\begin{aligned}\alpha - \frac{p}{q} &= \frac{p_n\theta + q_n}{q_n\theta + q_{n-1}} - \frac{p_n}{q_n} \\ &= \frac{(-1)^{n-1}}{q_n(q_n\theta + q_{n-1}},\end{aligned}$$

it follows that

$$0 \leq \frac{1}{q_n(q_n\theta + q_{n-1}} < \frac{1}{2q_n^2},$$

ie

$$q_n\theta + q_{n-1} > 2q_n,$$

from which it follows that

$$\theta > 1,$$

which as we have seen establishes the result. ◀

A.4 Quadratic surds

Examples:

1. Let us compute the continued fraction for $\sqrt{2}$. We have

$$\begin{aligned}\sqrt{2} &= 1 + (\sqrt{2} - 1),\\ \frac{1}{\sqrt{2}-1} &= \frac{\sqrt{2}+1}{(\sqrt{2}+1)(\sqrt{2}-1)} = \sqrt{2}+1\\ \frac{1}{\sqrt{2}-1} &= 2 + (\sqrt{2} - 1),\end{aligned}$$

   and so on. Thus

$$\sqrt{2} = [1, 2, 2, \dots] = [1, \dot{2}],$$

   where the dotted number indicates recurrence.

2. Let us compute the continued fraction for $\sqrt{3}$ similarly.

$$\begin{aligned}\sqrt{3} &= 1 + (\sqrt{3} - 1),\\ \frac{1}{\sqrt{3}-1} &= \frac{\sqrt{3}+1}{2}\\ &= 1 + \frac{\sqrt{3}-1}{2},\\ \frac{2}{\sqrt{3}-1} &= \sqrt{3}+1\\ &= 2 + (\sqrt{3} - 1).\\ \frac{1}{\sqrt{3}-1} &= 1 + \frac{\sqrt{3}-1}{2},\end{aligned}$$

   and so on. Thus

$$\sqrt{3} = [1, 1, 2, 1, 2, 1, \dots] = [1, \dot{1}, \dot{2}],$$

   with a cycle of length 2.

Recall that a *quadratic surd* is a real number of the form

$$\alpha = x + y\sqrt{d},$$

where $d > 1$ is a non-square: $d \neq m^2$.

In other words, a quadratic surd is an irrational element of a real quadratic field.

Theorem A.1. *The continued fraction for $\alpha \in \mathbb{R}$ is periodic if and only if α is a quadratic surd.*

Proof ▶. Suppose first the continued fraction for α is periodic, say

$$\alpha = [a_0, \dots, a_n, \dot{c_0}, \dots, \dot{c_m}].$$

By Proposition A.1,

$$\alpha = \frac{p_n\beta + p_{n-1}}{q_n\beta + q_{n-1}},$$

where β is purely periodic:

$$\beta = [\dot{c_0}, \dots, \dot{c_m}].$$

By Proposition A.1,

$$\beta = \frac{P_m\beta + P_{m-1}}{Q_m\beta + Q_{m-1}},$$

where P_i/Q_i are the convergents to β. Thus β is a root of

$$Q_m x^2 + (Q_{m-1} - P_m)x - P_{m-1} = 0.$$

Hence β is a quadratic surd.

It follows at once that α is also a quadratic surd, in the same quadratic field. (It cannot be rational, or the continued fraction would be finite.)

The converse is more difficult. Suppose

$$\alpha = [a_0, a_1, \dots]$$

satisfies the quadratic equation

$$ax^2 + 2bx + c = 0.$$

By Proposition A.1,

$$\alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n p_{n-1} + p_{n-2}},$$

where

$$\alpha_n = [a_n, a_{n+1}, \dots].$$

Thus α_n satisfies the quadratic equation

$$Ax^2 + 2Bx + C,$$

where

$$\begin{aligned} A &= ap_{n-1}^2 + 2bp_{n-1}q_{n-1} + cq_{n-1}^2, \\ B &= ap_{n-1}p_{n-2} + b(p_{n-1}q_{n-2} + q_{n-1}p_{n-2}) + cq_{n-1}q_{n-2}, \\ C &= ap_{n-2}^2 + 2bp_{n-2}q_{n-2} + cq_{n-2}^2. \end{aligned}$$

We shall show that A, B, C are *bounded*. It will follow that some triple (A, B, C) must be repeated an infinity of times, from which it will follow that there is a repeat

$$\alpha_{m+r} = \alpha_m,$$

and it will follow from this that α_m, and so α, is a quadratic surd.

To see that A is bounded, note that

$$\frac{A}{q_n^2} = ar^2 + 2br + c,$$

where

$$r = \frac{p_{n-1}}{q_{n-1}}.$$

Since $a\alpha^2 + 2b\alpha + c = 0$.

$$\begin{aligned} ar^2 + 2br + c &= a(\alpha^2 - r^2) + 2b(\alpha - r) \\ &= (\alpha - r)(a(\alpha + r) + 2b). \end{aligned}$$

Since

$$|\alpha - r| < \frac{1}{q_n^2}$$

it follows that

$$\begin{aligned} |\alpha + r| &= |2\alpha - (\alpha - r)| \\ &< 2|\alpha| + \frac{1}{q_n^2} \\ &< 2|\alpha| + 1. \end{aligned}$$

Hence

$$|ar^2 + 2br + c| < \frac{a(2\alpha + 1) + 2|b|}{q_n^2}.$$

Thus

$$|A| < 2a(|\alpha| + 1) + 2|b|.$$

By exactly the same argument (with $n - 1$ in place of n),

$$|C| < 2a(|\alpha| + 1) + 2|b|.$$

We could prove that B is bounded in much the same way, using the fact that

$$\frac{B}{q_{n-1}q_{n-2}} = ars + b(r+s) + c$$

where $r = p_{n-1}/q_{n-1},\ s = p_{n-2}/q_{n-2}$ are both close to α.

Alternatively, one can verify by a straightforward (if lengthy) computation — which is left to the student — that

$$B^2 - AC = b^2 - ac.$$

This is not a surprising result since

$$\alpha = [a_0, a_1, \dots] \in \mathbb{Q}(\sqrt{b^2 - ac}), \quad \alpha_n = [a_n, a_{n+1}, \dots] \in \mathbb{Q}(\sqrt{B^2 - AC}),$$

while we know they lie in the same quadratic field.

In any case, A, B, C are bounded, and so some triple (A, B, C) must occur an infinity of times. In particular,

$$\alpha_n = \alpha_{n+m}$$

for some n, m with $m > 0$. But then, if $\alpha_n = [b_0, b_1, \dots]$,

$$\alpha_n = \alpha_{n+m} = \frac{p'_{m-1}\alpha_n + p'_{m-2}}{q'_{m-1}\alpha_n + q'_{m-2}},$$

where the p', q' are convergents to α_n. Thus α_n is a quadratic surd; and so therefore is

$$\alpha = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}.$$

◀

A.5 Pell's Equation

Proposition A.11. *Suppose the integer $d > 1$ is not a perfect square. If $x, y > 0$ is a solution to Pell's Equation*

$$x^2 - dy^2 = \pm 1$$

then x/y is a convergent to $\sqrt{d}$.

Proof ▶. Since

$$x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d}),$$

it follows that

$$|\sqrt{d} - \frac{x}{y}| = \frac{1}{x^2} \frac{1}{\sqrt{d} + \frac{x}{y}}$$

But

$$\begin{aligned}
\sqrt{d} + \frac{x}{y} &\geq 2\sqrt{d} - |\sqrt{d} - \frac{x}{y}| \\
&= 2\sqrt{d} - \frac{|x - y\sqrt{d}|}{x} \\
&= 2\sqrt{d} - \frac{1}{x(|x + \sqrt{d})|} \\
&=\geq 2\sqrt{d} - \frac{1}{\sqrt{d}}.
\end{aligned}$$

But

$$2\sqrt{d} - \frac{1}{\sqrt{d}} > 2$$

for $d \geq 2$. Hence

$$|\sqrt{d} - \frac{x}{y}| < \frac{1}{y^2};$$

and so x/y is a convergent to $\sqrt{d}$, by Proposition A.10. ◀

Appendix B

P-adic numbers

B.1 Valuations

Definition B.1. *A* valuation *on a field k is a map*

$$x \mapsto \|x\| : k \to \mathbb{R}$$

such that

1. $\|x\| \geq 0$ *and* $\|x\| = 0 \iff x = 0$;
2. $\|x + y\| \leq \|x\| + \|y\|$;
3. $\|xy\| = \|x\|\|y\|$;
4. $\|x\| \neq 1$ *for some* $x \neq 0$.

We sometimes use the term *valued field* for a field k together with a valuation $\|\cdot\|$ on k.

Proposition B.1. 1. $\|1\| = 1$;

2. $\|-1\| = 1$;
3. $\|-x\| = \|x\|$.

Proof ►. 1. This follows from $1^2 = 1$;

2. Similarly, this follows from $(-1)^2 = 1$;
3. $\|-x\| = \|-1\|\|x\|\|x\|$.

◄

Examples:

1. The absolute value $|x|$ defines valuations on $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

2. Suppose k is a field. Recall that $k(x)$ denotes the field of rational functions
$$f(x) = \frac{u(x)}{v(x)},$$
where $u(x), v(x) \in k[x]$ are polynomials.

   If $f(x)$ is not identically zero then we can write
$$f(x) = x^n \, \frac{r(x)}{s(x)},$$
where $r(0), s(0) \neq 0$ (ie $x \nmid r(x), s(x)$).

   It is readily verifed that
$$\|f(x)\| = 2^{-n}$$
defines a valuation on $k(x)$.

   Thus $\|f(x)\|$ is determined by the order of the pole (or zero) at $x = 0$.

   The choice of 2 was arbitrary. We could equally well have set $\|f(x)\| = e^{-n}$. We shall return to this point (or place) shortly.

   More generally, for any $a \in k$ we can define a norm $\|f(x)\|_a$ on $k(x)$ by setting
$$\|f(x)\|_a = 2^{-n}$$
if n is the order of the pole (or zero) at $x = a$.

3. We can define another norm on $k(x)$ by setting
$$\|u(x)/v(x)\|_\infty = \deg u(x) - \deg v(x).$$
   We can think of this as the 'norm at infinity' since
$$\|f(x)\|_\infty = \|f(1/x)\|_0.$$

Each non-zero rational
$$r = \frac{n}{d}$$
can be written as
$$r = p^e \, \frac{u}{v},$$

where $p \nmid u, v$. We may say that

$$p^e \mid\mid r.$$

Recall that if p is a prime and $n \in \mathbb{Z}$ then we write

$$p^e \mid\mid n \text{ if } p^e \mid n \text{ but } p^{e+1} \nmid n.$$

We can extend this to $\mathbb{Q}$ by setting

$$p^e \mid\mid r = \frac{n}{d} \text{ if } r = p^e \, \frac{u}{v} \quad (p \nmid u, v).$$

Definition B.2. *Let p be a prime. Suppose $r \in \mathbb{Q},\ r \neq 0$. If*

$$p^e \mid\mid r$$

then we set

$$\|x\|_p = p^{-e}.$$

We call $\|\cdot\|_p$ the p-adic valuation *on $\mathbb{Q}$.*

Proposition B.2. *The p-adic valuation is indeed a valuation of $\mathbb{Q}$.*

Proof ▶. If

$$p^e \mid\mid r, \quad p^f \mid\mid s$$

then

$$p^{e+f} \mid\mid rs$$

while

$$p^{\min(e.f)} \mid r + s.$$

◀

We sometimes denote the absolute valuation on $\mathbb{Q}$ by

$$\|x\|_\infty = |x|.$$

However, the p-adic valuations $\|x\|_p$ differ in one important way from the absolute valuation $\|x\|_\infty$; they satisfy a much stronger triangle inequality.

Proposition B.3. *If $r, s \in \mathbb{Q}$ then*

$$\|r + s\| \leq \max(\|r\|, \|s\|)$$

Proof ►. Suppose

$$\|r\|_p = e, \quad \|s\|_p = f,$$

ie

$$p^{-e} \mid\mid r, \quad p^{-f} \mid\mid s.$$

Then

$$p^{\min(-e,-f)} = p^{-\max(e,f)} \mid r + s,$$

and so

$$\|r + s\|_p \leq \max(e, f).$$

◄

Definition B.3. *The valuation* $\|x\|$ *is said to be* non-archimedean *if*

$$\|x + y\| \leq \max(\|x\|, \|y\|)$$

for all x, y. *If this is not so the valuation is said to be* archimedean.

Evidently the p-adic valuation on $\mathbb{Q}$ is non-archimedean, while the absolute value is archimedean.

The term "ultrametric" is sometimes used for a non-archimedean valuation.

For any field k. there is a unique ring-homomorphism

$$\mathbb{Z} \to k$$

If $n \in \mathbb{Z}$ we write $n \in k$ for the image of n under this homomorphism.

Proposition B.4. *The valuation* $\|\cdot\|$ *on* k *is archimedean if and only if*

$$\|n\| > 1$$

for some $n \in \mathbb{Z}$.

Proof ►. We have to show that if

$$\|n\| \leq 1$$

for all $n \in \mathbb{Z}$ then the valuation is non-archimedean.

Suppose $x, y \in k$. Then

$$(x + y)^n = x^n + c_1 x^{n-1} y + \cdots + y^n,$$

where

$$c_i = \binom{n}{i} \in \mathbb{Z} \implies \|c_i\| \leq 1.$$

Thus

$$\begin{aligned}\|x+y\|^n &= \|(x+y)^n\| \\ &= \|x^n + c_1 x^{n-1} y + \cdots + y^n\| \\ &\leq \|x^n\| + \|x^{n-1}y\| + \cdots + \|y^n\| \\ &= \|x\|^n + \|x\|^{n-1}\|y\| + \cdots + \|y\|^n \\ &\leq (n+1)\max(\|x\|, \|y\|)^n.\end{aligned}$$

Hence

$$\|x+y\| \leq (n+1)^{1/n} \max(\|x\|, \|y\|).$$

Since $(n+1)^{1/n} \to 1$ as $n \to \infty$ (as one can see by taking logarithms),

$$\|x+y\| \leq \max(\|x\|, \|y\|).$$

◀

Corollary B.1. *A valuation on a number field k restricts to a valuation on $\mathbb{Q}$; and the valuation is archimedean or non-archimedean according as the restriction is archimedean or non-archimedean.*

Proof ▶. All is immediate, except perhaps that a valuation on k might become trivial on $\mathbb{Q}$, ie $\|c\| = 1$ for all $c \in \mathbb{Q}$.

Suppose that is so. Then the valuation on k must be non-archimedean. Suppose $\|\alpha\| \neq 1$ for $\alpha \in k,\ \alpha \neq 0$. Taking α^{-1} in place of α, if necessary, we may assume that $\|\alpha\| > 1$.

Since α is an algebraic number it satisfies some equation

$$\alpha^n + c_1\alpha^{n-1} + \cdots + c_n = 0,$$

with $c_i \in \mathbb{Q}$. Since $\|c_i\| = 1$,

$$\begin{aligned}\|\alpha\|^n &= \|c_1\alpha^{n-1} + \cdots + c_n\| \\ &\leq \max(\|\alpha\|^{n-1}, \|\alpha\|^{n-1}, \ldots, 1) \\ &= \|\alpha\|^{n-1},\end{aligned}$$

whence

$$\|\alpha\| \leq 1,$$

contrary to assumption. ◀

B.2 Places

A valuation on k defines a metric

$$d(x, y) = \|x - y\|;$$

and this in turn defines a topology on k.

Definition B.4. *Two valuations on k are said to be* equivalent *if they define the same topology.*

An equivalence class of valuations is called a place.

Proposition B.5. *The valuations $\|\cdot\|_1,\ \|\cdot\|_2$ are equivalent if and only if*

$$\|x\|_2 = \|x\|_1^\rho$$

for some $\rho > 0$.

Proof ▶. It is evident the valuations will be equivalent if they satisfy such a relation.

Conversely, suppose the valuations are equivalent. With any valuation,

$$x^n \to 0 \iff \|x\| < 1.$$

Thus, since the topologies are the same,

$$\|x\|_1 < 1 \iff \|x\|_2 < 1.$$

Hence, taking x/y in place of x,

$$\|x\|_1 < \|y\|_1 \iff \|x\|_2 < \|y\|_2.$$

We have to show, in effect, that

$$\frac{\log\|x\|_1}{\log\|x\|_2}$$

is constant, ie

$$\frac{\log\|x\|_1}{\log\|y\|_1} = \frac{\log\|x\|_2}{\log\|y\|_2}$$

for all $x, y \neq 0$.

It is sufficient to prove this when $\|x\|_1, \|y\|_1 > 1$. Take a high power x^n, and suppose

$$\|y\|_1^m \leq \|x\|_1^n \leq \|y\|_1^{m+1}.$$

Then

$$\|y\|_2^m \leq \|x\|_2^n \leq \|y\|_2^{m+1}.$$

Taking logs,

$$\frac{m}{n} \leq \frac{\log\|x\|_1}{\log\|y\|_1}, \frac{\log\|x\|_2}{\log\|y\|_2} \leq \frac{m+1}{n}$$

Since this is true for arbitrarily large n,

$$\frac{\log\|x\|_1}{\log\|y\|_1} = \frac{\log\|x\|_2}{\log\|y\|_2},$$

as required. ◀

Note that we do not assert that if $\|x\|$ is a valuation on k then so is $\|x\|^\rho$. This is true if $0 < \rho < 1$, but is not true in general; for example, $|x|^2$ does not satisfy the triangle inequality in $\mathbb{R}$. All we are saying is that if we have two equivalent valuations then they must be related in this way.

B.3 Places in $\mathbb{Q}$

Theorem B.1. *A valuation on $\mathbb{Q}$ is equivalent either to a p-adic valuations $\|\cdot\|_p$ or to the absolute valuation $|\cdot|$.*

Proof ▶. Suppose first that $\|\cdot\|$ is a non-archimedean valuation on $\mathbb{Q}$, so that

$$\|n\| \leq 1$$

for all $n \in \mathbb{Z}$.

We must have $\|n\| < 1$ for some $n \neq 0$; for otherwise we would have $\|x\| = 1$ for all non-zero $x = m/n$. Let

$$n = \pm p_1^{e_1} \cdots p_n^{e_n}.$$

Then $\|p_i\| < 1$ for some i.

Set $p = p_i$; and suppose q is another prime. Then we can find $u, v \in \mathbb{Z}$ such that

$$up + vq = 1.$$

It follows that $\|q\| = 1$, since otherwise $\|1\| < 1$.

But now we see that $\|n\|$ depends only on the power p^e of p dividing n:

$$\|n\| = \|p\|^e;$$

from which it follows that $\|\cdot\|$ is equivalent to the p-adic valuation $\|\cdot\|_p$.

Now suppose $\|\cdot\|$ is archimedean. We want to show that

$$\|x\| = |x|^\rho$$

for some ρ.

It is sufficient to prove this for all $a \in \mathbb{N}$. This is equivalent to showing that

$$\frac{\|a\|}{\|b\|} = \frac{|a|}{|b|}$$

for all integers $a, b > 1$.

Take a high power b^f of b; and suppose

$$a^e \leq b^f < a^{e+1}.$$

Then

$$e \log a \leq f \log b < (e+1) \log a$$

ie

$$\frac{e}{f} \leq \frac{\log b}{\log a} \leq \frac{e+1}{f}.$$

Now let us express b^f to base a, say

$$b^f = a^e + c_1 a^{e-1} + \cdots + c_r,$$

where

$$0 \leq c_i < a \quad (1 \leq i \leq r).$$

It follows that

$$\begin{aligned} \|b\|^f &\leq \|a\|^e + \|c_1\|\|a\|^{e-1} + \cdots + \|c_r\| \\ &\leq C\left(\|a\|^e + \|a\|^{e-1} + ...1\right), \end{aligned}$$

where

$$C = \max(\|1\|, \|2\|, \ldots, \|r-1\|).$$

If $\|a\| \leq 1$ this gives

$$\|b\|^f \leq C(e+1).$$

Thus

$$\|b\| \leq \left(C(e+1)^{1/f}\right)$$

As $f \to \infty$,

$$\leq \left(C(e+1)^{1/f}\right) \to 1,$$

since

$$e \leq \frac{\log b}{\log a} f.$$

It follows that

$$\|b\| \leq 1.$$

Since this is true for all b, the valuation is non-archimedean, contrary to hypothesis. We conclude that

$$\|a\| > 1$$

for all $a > 1$.

Now the inequality above yields

$$\|b\|^f \leq C(e+1)\|a\|^e$$

ie

$$f \log\|b\| \leq e \log\|a\| + \log C(e+1).$$

Thus

$$\begin{aligned} \frac{\log\|b\|}{\log\|a\|} &\leq \frac{e}{f} + \frac{\log C(e+1)}{f \log\|a\|} \\ &\leq \frac{\log b}{\log a} + \frac{\log C(e+1)}{f \log\|a\|}. \end{aligned}$$

As before, the last term $\to 0$ as $f \to \infty$. Hence

$$\frac{\log\|b\|}{\log\|a\|} \leq \frac{\log b}{\log a}.$$

Similarly,

$$\frac{\log\|a\|}{\log\|b\|} \leq \frac{\log a}{\log b}.$$

Thus

$$\frac{\log\|b\|}{\log\|a\|} = \frac{\log b}{\log a},$$

as required. ◀

We have shown, accordingly, that there is a place in $\mathbb{Q}$ corresponding to each prime p, together with a place corresponding to the absolute valuation, which we denote by ∞. In general, the places in a number field corresponding to archimedean valuations are said to be infinite.

B.4 P-adic numbers

The reals $\mathbb{R}$ can be constructed from the rationals $\mathbb{Q}$ by *completing* the latter with respect to the valuation $|x|$. In this construction each Cauchy sequence

$$\{x_i \in \mathbb{Q} : |x_i - x_j| \to 0 \text{ as } i, j \to \infty\}$$

defines a real number, with 2 sequences defining the same number if $|x_i - y_i| \to 0$.

(There are 2 very different ways of constructing $\mathbb{R}$ from $\mathbb{Q}$: by completing $\mathbb{Q}$, as above; or alternatively, by the use of *Dedekind sections*. In this each real number corresponds to a partition of $\mathbb{Q}$ into 2 subsets L, R where

$$l \in L,\ r \in R \implies l < r.$$

The construction by completion is much more general, since it applies to any metric space; while the alternative construction uses the fact that $\mathbb{Q}$ is an *ordered* field. John Conway, in *On Numbers and Games,* has generalized Dedekind sections to give an extraordinary construction of rationals, reals and infinite and infinitesimal numbers, starting 'from nothing'. Knuth has given a popular account of Conway numbers in *Surreal Numbers.*)

We can complete $\mathbb{Q}$ with respect to the p-adic valuation in just the same way. The resulting field is called *the field of p-adic numbers*, and is denoted by $\mathbb{Q}_p$. We can identify $x \in \mathbb{Q}$ with the Cauchy sequence $(x, x, x, \dots)$. Thus

$$\mathbb{Q} \subset \mathbb{Q}_p.$$

To bring out the parallel with the reals, we sometimes write

$$\mathbb{R} = \mathbb{Q}_\infty.$$

The numbers $x \in \mathbb{Q}_p$ with $\|x\|_p \leq 1$ are called *p-adic integers.* The p-adic integers form a ring, denoted by $\mathbb{Z}_p$. For if $x, y \in \mathbb{Z}_p$ then by property (3) above,

$$\|x + y\|_p \leq \max(\|x\|_p, \|y\|_p) \leq 1,$$

and so $x + y \in \mathbb{Z}_p$. Similarly, by property (1),

$$\|xy\|_p = \|x\|_p \|y\|_p \leq 1,$$

and so $xy \in \mathbb{Z}_p$.

Evidently

$$\mathbb{Z} \subset \mathbb{Z}_p.$$

More generally,

$$x = \frac{m}{n} \in \mathbb{Z}_p$$

if $p \nmid n$. (We sometimes say that a rational number x of this form is *p-integral*.) In other words,

$$\mathbb{Q} \cap \mathbb{Z}_p = \{\frac{m}{n} : p \nmid n\}.$$

Evidently the p-integral numbers form a sub-ring of $\mathbb{Q}$.

The p-adic numbers are in many ways simpler than real numbers, as the following result suggests.

Proposition B.6. *The series*

$$\sum a_n$$

in $\mathbb{Q}_p$ converges if and only if

$$a_n \to 0 \text{ as } n \to \infty.$$

Proposition B.7. *Each element $x \in \mathbb{Z}_p$ is uniquely expressible in the form*

$$x = c_0 + c_1 p + c_2 p^2 + \cdots$$

with $c_i \in \{0, 1, \ldots, p-1\}$.

More generally, each element $x \in \mathbb{Q}_p$ is uniquely expressible in the form

$$x = c_{-i} p^{-i} + c_{-i+1} p^{-i+1} + \cdots + c_0 + c_1 p + \cdots \quad (0 \le c_i < p).$$

We can think of this as the p-adic analogue of the decimal expansion of a real number $x \in \mathbb{R}$.

Suppose for example $p = 3$. Let us express $1/2 \in \mathbb{Q}_3$ in standard form. The first step is to determine if

$$\frac{1}{2} \equiv 0, 1 \text{ or } 2 \bmod 3.$$

In fact $2^2 \equiv 1 \bmod 3$; and so

$$\frac{1}{2} \equiv 2 \bmod 3.$$

Next

$$\frac{1}{3}\left(\frac{1}{2} - 2\right) = -\frac{1}{2} \equiv 1 \bmod 3$$

ie

$$\frac{1}{2} - 2 \equiv 1 \cdot 3 \bmod 3^2.$$

Thus

$$\frac{1}{2} \equiv 2 + 1 \cdot 3 \bmod 3^2$$

For the next step,

$$\frac{1}{3}\left(-\frac{1}{2} - 1\right) = -\frac{1}{2} \equiv 1 \bmod 3$$

giving

$$\frac{1}{2} \equiv 2 + 1 \cdot 3 + 1 \cdot 3^2 \bmod 3^3$$

It is clear that this pattern will be repeated indefinitely. Thus

$$\frac{1}{2} = 2 + 3 + 3^2 + 3^3 + \cdots .$$

To check this,

$$\begin{aligned} 2 + 3 + 3^2 + \cdots &= 1 + (1 + 3 + 3^2 + \cdots) \\ &= 1 + \frac{1}{1-3} \\ &= 1 - \frac{1}{2} \\ &= \frac{1}{2}. \end{aligned}$$

As another illustration, let us expand $3/5 \in \mathbb{Q}_7$. We have

$$\begin{aligned} \frac{3}{5} &\equiv 2 \bmod 7 \\ \frac{1}{7}\left(\frac{3}{5} - 2\right) &= -\frac{1}{5} \equiv 4 \bmod 7 \\ \frac{1}{7}\left(-\frac{1}{5} - 4\right) &= -\frac{3}{5} \equiv 5 \bmod 7 \\ \frac{1}{7}\left(-\frac{3}{5} - 5\right) &= -\frac{4}{5} \equiv 2 \bmod 7 \\ \frac{1}{7}\left(-\frac{4}{5} - 2\right) &= -\frac{2}{5} \equiv 1 \bmod 7 \\ \frac{1}{7}\left(-\frac{2}{5} - 1\right) &= -\frac{1}{5} \equiv 4 \bmod 7 \end{aligned}$$

We have entered a loop; and so (in $\mathbb{Q}_7$)

$$\frac{3}{5} = 2 + 4 \cdot 7 + 5 \cdot 7^2 + 2 \cdot 7^3 + 1 \cdot 7^4 + 4 \cdot 7^5 + 5 \cdot 7^6 + \cdots$$

Checking,

$$\begin{aligned} 1 + \left(1 + 4 \cdot 7 + 5 \cdot 7^2 + 2 \cdot 7\right) \frac{1}{1 - 7^4} &= 1 - \frac{960}{2400} \\ &= 1 - \frac{2}{5} \\ &= \frac{3}{5}. \end{aligned}$$

It is not difficult to see that a number $x \in \mathbb{Q}_p$ has a recurring p-adic expansion if and only if it is rational (as is true of decimals).

Let $x \in \mathbb{Z}_p$. Suppose $\|x\|_p = 1$. Then

$$x = c + yp,$$

where $0 < c < p$ and $y \in \mathbb{Z}_p$. Suppose first that $c = 1$, ie

$$x = 1 + yp.$$

Then x is invertible in $\mathbb{Z}_p$, with

$$x^{-1} = 1 - yp + y^2p^2 - y^3p^3 + \cdots .$$

Even if $c \neq 1$ we can find d such that

$$dc \equiv 1 \bmod p.$$

Then

$$dx \equiv dc \equiv 1 \bmod p,$$

say

$$dx = 1 + py,$$

and so x is again invertible in $\mathbb{Z}_p$, with

$$x^{-1} = d\left(1 - yp + y^2p^2 - \cdots\right).$$

Thus the elements $x \in \mathbb{Z}_p$ with $\|x\|_p = 1$ are all *units* in $\mathbb{Z}_p$, ie they have inverses in $\mathbb{Z}_p$; and all such units are of this form. These units form the multiplicative group

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p : \|x\|_p = 1\}.$$

B.5 The product formula

Proposition B.8. *Suppose* $\alpha \in \mathbb{Q}$, $\alpha \neq 0$. *Then*

$$\|\alpha\|_p = 1$$

for almost all places p, *ie for all but a finite number of* p; *and*

$$\prod_p \|\alpha\|_p = 1,$$

where the product extends over all the places in $\mathbb{Q}$.