Chapter 2
Number Fields

We've just seen examples where questions about integers were naturally treated by working in the slightly bigger set $\mathbb{Z}[i]$ of Gaussian integers. In this chapter we begin the development of some more general theory.

The aim of algebraic number theory is to study generalisations of the usual arithmetic in the natural numbers in more general settings. While studying these generalisations, it will become clear that there are new phenomena of interest in their own right.

In Chap. 1, we saw that unique factorisation plays a prominent role, and that this was a consequence of the Euclidean algorithm. In order to be able to talk about a Euclidean algorithm, we need to work in sets closed under addition and multiplication, i.e., in rings. As in the examples at the end of Chap. 1, we will also want to work in sets contained in the complex numbers, that is, with subrings of $\mathbb{C}$.

It turns out that there is a good theory of integers inside any field K which is a finite degree extension of $\mathbb{Q}$, and these finite extensions, known as number fields, form the setting for algebraic number theory. Finite degree extensions of $\mathbb{Q}$ are constructed by adjoining complex numbers which are the roots of polynomial equations with rational (or integer) coefficients. Although many complex numbers are roots of polynomial equations with integer coefficients, it turns out that not every complex number can be written in this way.

2.1 Algebraic Numbers

Definition 2.1 A complex number α is said to be *algebraic* if it is the root of a polynomial equation with integer coefficients. If α is not algebraic, it is *transcendental*.

Every rational number $\frac{m}{n}$ is algebraic, as it is a root of $nX - m = 0$; also, $\pm\sqrt{2}$ are roots of $X^2 - 2 = 0$, so $\pm\sqrt{2}$ are both algebraic. Indeed, every polynomial with integer coefficients of degree n will have n algebraic numbers as roots. This gives

F. Jarvis, *Algebraic Number Theory*, Springer Undergraduate Mathematics Series, DOI: 10.1007/978-3-319-07545-7_2,

such a large collection of algebraic numbers, that one might wonder whether every complex number could be written as a root of a polynomial.

However, this is not true. Liouville (1844) was the first to construct an explicit example of a transcendental number, while Hermite (1873) and Lindemann (1882) proved that e and π respectively are transcendental.

For readers with some knowledge of Cantor's theory of countability, the simplest proof of the existence of transcendental numbers is due to Cantor himself (1874), although it does not give any way to construct such numbers. We will give Liouville's construction of an explicit transcendental number below.

Write $\mathcal{A} \subseteq \mathbb{C}$ for the collection of all algebraic numbers.

Theorem 2.2 (Cantor) *The set $\mathcal{A}$ is countable; that is, there are only countably many algebraic numbers.*

Proof Given a polynomial equation $p(X) = c_0X^d + c_1X^{d-1} + \cdots + c_d = 0$ with all $c_i \in \mathbb{Z}$ and $c_0 \neq 0$, define the quantity

$$H(p) = d + |c_0| + \cdots + |c_d| \in \mathbb{Z}.$$

This process associates an integer to every polynomial with integer coefficients. Notice that $\deg(p) = d < H(p)$.

Let H be any natural number. Then it is easy to see that there are only finitely many polynomials $p(X)$ which satisfy $H(p) \leq H$. Say that an algebraic number $\alpha \in \mathcal{A}$ is *of level* H if α is a root of some polynomial p with $H(p) \leq H$. As there are only finitely many polynomials with $H(p) \leq H$, and all have at most H roots (since the degree of such a polynomial is bounded by H), there are only finitely many algebraic numbers of level H, for any given H.

On the other hand, every algebraic number is a root of such a polynomial, and is therefore of level H for some H. The collection of algebraic numbers can therefore be written as a union

$$\mathcal{A} = \bigcup_{H=1}^{\infty} \{\alpha \in \mathcal{A} \mid \alpha \text{ is of level } H\}.$$

We have already remarked that each set on the right-hand side is finite. Furthermore, the union is a countable union, as the indexing set consists of the natural numbers. Therefore $\mathcal{A}$ is a countable union of finite sets, and is therefore countable. □

Since $\mathbb{C}$ is uncountable, and its subset $\mathcal{A}$ is countable, we conclude that transcendental numbers exist. Even more, we see that the set of transcendental numbers is actually *uncountable*, so that, in some sense, almost every complex number is transcendental.

Now let us give Liouville's explicit construction of a transcendental number, which avoids use of countability arguments.

We need the following theorem:

Theorem 2.3 (Liouville) *Let α be a real algebraic number which is a root of an irreducible polynomial $f(X)$ over $\mathbb{Z}$ of degree $n > 1$. Then there is a constant c such that for all rational numbers $\frac{p}{q}$,*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^n}.$$

Proof The result is clear in the case where $|\alpha - p/q| > 1$; choosing $c = 1$ covers these values. We therefore consider the remaining case where $|\alpha - p/q| \leq 1$.

Apply the Mean Value Theorem to $f(X)$ at the points α and p/q to deduce the existence of a number γ strictly between α and p/q such that

$$\frac{f(\alpha) - f(p/q)}{\alpha - p/q} = f'(\gamma).$$

As α is a root of f, we see that $f(\alpha) = 0$. Also, as $f(X)$ is an irreducible polynomial of degree $n > 1$, it has no rational roots, so $f(p/q) \neq 0$. However, as $f(X)$ has integer coefficients, the denominator of $f(p/q)$ must divide q^n, so $q^n f(p/q)$ is a non-zero integer. Therefore $|f(p/q)| \geq 1/q^n$.

Now $|\gamma - \alpha| < 1$ as γ is strictly between α and p/q, and $|\alpha - p/q| \leq 1$. By continuity of f' at α, we see that $|f'(\gamma)| < 1/c_0$ for some constant c_0 for all γ within 1 of α, where the constant c_0 depends only on α. Then

$$\left|\alpha - \frac{p}{q}\right| = \left|\frac{f(p/q)}{f'(\gamma)}\right| > \frac{c_0}{q^n}.$$

Choose $c = \min(c_0, 1)$ to cover both cases, and the result follows. □

In order to find a transcendental number, we simply need to find an α where the inequality of Theorem 2.3 fails for all n. Liouville suggested choosing

$$\alpha = \sum_{k=1}^{\infty} 10^{-k!} = 0.11000100000000000000000100\ldots.$$

Define $p_r/q_r = \sum_{k=1}^{r} 10^{-k!}$. The first three numbers are $p_1/q_1 = 0.1$, $p_2/q_2 = 0.11$ and $p_3/q_3 = 0.110001$. Then $q_r = 10^{r!}$, and

$$\left|\alpha - \frac{p_r}{q_r}\right| = \sum_{k=r+1}^{\infty} 10^{-k!} < \frac{2}{10^{(r+1)!}} = \frac{2}{(10^{r!})^{r+1}} = \frac{2}{q_r^{r+1}}. \tag{2.1}$$

If α were algebraic of some degree n, there would be a constant c such that $|\alpha - p/q| > c/q^n$ for all rationals p/q. However, choosing $p/q = p_r/q_r$ for large enough $r > n$ gives a contradiction, using (2.1).

Exercise 2.1 Show that all numbers $\sum_{k=1}^{\infty} s_k 10^{-k!}$ are transcendental, where $s_k \in \{1, -1\}$.

By considering a variant of Cantor's diagonal argument, prove that the set of numbers of this form is uncountable. This gives another proof of the uncountability of the set of transcendental numbers.

Hermite's proof of the transcendence of e, and Lindemann's proof of the transcendence of π, are (only just) beyond the scope of this book. References for the arguments include [11].

2.2 Minimal Polynomials

As already mentioned, we will be able to do arithmetic in fields which are obtained by adjoining roots of polynomials to $\mathbb{Q}$, i.e., algebraic numbers. In this section, we will look at some properties of polynomials.

Recall that a *monic* polynomial is one whose leading coefficient is 1.

Lemma 2.4 *If α is algebraic, then there is a unique monic polynomial $f(X) \in \mathbb{Q}[X]$ of smallest degree with α as a root.*

Proof If α is a root of a polynomial $f(X) = c_0X^n + c_1X^{n-1} + \cdots + c_n$ with $c_0 \neq 0$, it will also be a root of $X^n + \frac{c_1}{c_0}X^{n-1} + \cdots + \frac{c_n}{c_0}$ got by dividing through by the leading coefficient.

Amongst all the monic polynomials with α as a root, let $f(X)$ be one with smallest degree. We claim that $f(X)$ is unique.

Suppose that $g(X)$ is another monic polynomial of the same degree with α as a root. Then α is also a root of $(f - g)(X)$, and since the leading terms of $f(X)$ and $g(X)$ cancel, the degree of $f - g$ is smaller than that of f or g. If $f - g \neq 0$, then we can divide through by its leading coefficient to find a monic polynomial of smaller degree than f with α as a root, contradicting the choice of $f(X)$. □

Definition 2.5 Let α be an algebraic number. The *minimal polynomial* of α over $\mathbb{Q}$ is the monic polynomial over $\mathbb{Q}$ of smallest degree with α as a root.

Lemma 2.6 *If $m(X)$ is the minimal polynomial of the algebraic number α, then it is irreducible.*

Proof Indeed, if $m(X)$ were to factorise as the product $f(X)g(X)$ of two polynomials over $\mathbb{Q}$ of smaller degree, then since $m(\alpha) = 0$, we would have $f(\alpha)g(\alpha) = 0$, and α would be a root of either f or g, and this contradicts the choice of m as the polynomial *of smallest degree* with α as a root. □

The minimal polynomial has a particularly useful property: every polynomial with α as a root is necessarily a multiple of the minimal polynomial of α. We'll prove that next, with the aid of Euclid's algorithm for polynomials.

Lemma 2.7 *Suppose that α is a root of some polynomial $f(X) \in \mathbb{Q}[X]$. If $m(X)$ is the minimal polynomial of α, then $m(X)|f(X)$.*

Proof Just like $\mathbb{Z}$, the ring of rational polynomials $\mathbb{Q}[X]$ has an obvious division algorithm (see Exercise 1.6), and we can find polynomials $q(X), r(X) \in \mathbb{Q}[X]$ such that

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

where $r(X)$ is the zero polynomial, or has smaller degree than $m(X)$. Substitute $X = \alpha$:

$$f(\alpha) = q(\alpha)m(\alpha) + r(\alpha);$$

as $f(\alpha) = m(\alpha) = 0$, we must have $r(\alpha) = 0$. However, $r(X)$ has smaller degree than $m(X)$, and $m(X)$ was the monic polynomial of smallest degree with α as a root. If $r(X)$ were non-zero, we could scale it to get a monic polynomial of smaller degree than $m(X)$ with α as a root, and this would contradict the definition of $m(X)$. Therefore $r(X)$ must be the zero polynomial. In particular, $f(X) = q(X)m(X)$, and so $f(X)$ is a multiple of $m(X)$. □

If K is any field, and if α satisfies some equation over K, then we also have a notion of *minimal polynomial over* K, the monic polynomial with coefficients in K of smallest degree with α as a root; any other polynomial with coefficients in K with α as a root is a multiple of the minimal polynomial. The argument is identical to the one just given.

Exercise 2.2 Find the minimal polynomial of $\sqrt{2}+\sqrt{3}$ (over $\mathbb{Q}$). Would the minimal polynomial over $\mathbb{Q}(\sqrt{2})$ be the same?

Exercise 2.3 Find the minimal polynomial of $\alpha = \frac{1+i}{\sqrt{2}}$ over $\mathbb{Q}$. What is the minimal polynomial of α over each of $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$?

2.3 The Field of Algebraic Numbers

The main aim of this section is to establish the basic algebraic properties of algebraic numbers; indeed, we prove that the set $\mathcal{A}$ of algebraic numbers is actually a *field*. Recall that a field is a set which satisfies exactly the same algebraic properties as $\mathbb{Q}$, so that we must be able to add, subtract, multiply and divide (by non-zero elements) in $\mathbb{Q}$, and the usual algebraic rules (e.g., addition and multiplication are commutative and associative) are satisfied. Since we are dealing with subsets of the complex numbers $\mathbb{C}$, all these rules are inherited from $\mathbb{C}$, and we just have to check that the collection of algebraic numbers is closed under the usual arithmetic operations. That is, we want to see that if α and β are algebraic numbers, then so are $\alpha + \beta$, $\alpha - \beta$ and $\alpha\beta$, and if $\beta \neq 0$, so is α/β.

Although one could write a proof using no abstract algebra (using the ideas of the end of Sect. 2.6), we will give a more algebraic argument now, since some of the definitions will reappear later in the book.

We are going to give an equivalent algebraic formulation for what it means for the complex number α to be algebraic. Let's recall that for any complex number α, $\mathbb{Q}(\alpha)$ denotes the smallest *field* one can obtain by applying all the usual arithmetic operations (addition, subtraction, multiplication, division) to the rational numbers and α; it consists of all quotients $p(\alpha)/q(\alpha)$ where $p(X)$ and $q(X)$ are polynomials with rational coefficients, and where $q(\alpha) \neq 0$.

On the other hand, we also have the notation $\mathbb{Q}[\alpha]$, which means the *ring* of all *polynomial expressions* in α. It is the smallest ring one can obtain by applying the arithmetic operations of addition, subtraction and multiplication (but not division) to the rational numbers and α.

For example, $\frac{3\alpha^3+\alpha-1}{\alpha^2+2}$ is in $\mathbb{Q}(\alpha)$, but not necessarily in $\mathbb{Q}[\alpha]$. Of course, $\mathbb{Q}[\alpha] \subseteq \mathbb{Q}(\alpha)$.

Let's begin with a simple remark about algebraic numbers:

Proposition 2.8 *If α is algebraic, $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$, and so every element of $\mathbb{Q}(\alpha)$ can be written as a polynomial in α.*

Proof We have to explain that every quotient of polynomials $p(\alpha)/q(\alpha)$ with $q(\alpha) \neq 0$ can be written alternatively as a polynomial in α.

Let $m(X)$ denote the minimal polynomial of α over $\mathbb{Q}$. The highest common factor of the two polynomials $m(X)$ and $q(X)$ must be a factor of $m(X)$; as $m(X)$ is irreducible, its only factors are 1 and $m(X)$ itself. However, $m(X)$ is not a factor of $q(X)$, as $m(\alpha) = 0$, but $q(\alpha) \neq 0$. By a similar argument to the discussion of the Euclidean algorithm in Chap. 1 (see Exercise 1.6), there are polynomials $s(X)$ and $t(X)$ over $\mathbb{Q}$ such that

$$s(X)q(X) + t(X)m(X) = 1.$$

In particular, $s(\alpha)q(\alpha) + t(\alpha)m(\alpha) = 1$, and therefore $s(\alpha)q(\alpha) = 1$, because $m(\alpha) = 0$. We conclude that $1/q(\alpha) = s(\alpha)$, and so $p(\alpha)/q(\alpha) = p(\alpha)s(\alpha)$, a polynomial expression in α, as required. □

Note that if α is transcendental, there is no way to write $1/\alpha$ as a polynomial in α; otherwise, we could multiply through by α and find a rational polynomial with α as a root. Therefore $1/\alpha$ is in $\mathbb{Q}(\alpha)$, but not in $\mathbb{Q}[\alpha]$. Thus if α is not algebraic, then $\mathbb{Q}(\alpha)$ is strictly bigger than $\mathbb{Q}[\alpha]$, and the property of Proposition 2.8 therefore characterises algebraic numbers.

Recall that the *degree* of the field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is the dimension of the set $\mathbb{Q}(\alpha)$ when regarded as a vector space over $\mathbb{Q}$; that is, it is the number of elements in a basis $\{\omega_1, \ldots, \omega_n\}$ so that every element of $\mathbb{Q}(\alpha)$ can be expressed uniquely as a sum $a_1\omega_1 + \cdots + a_n\omega_n$ with $a_i \in \mathbb{Q}$. It is denoted $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. For example, $\mathbb{Q}(\sqrt{2})$ has degree 2 over $\mathbb{Q}$, as each element can be written as $a + b\sqrt{2}$.

Exercise 2.4 Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ has degree 4 over $\mathbb{Q}$ by proving that 1, $\sqrt{2}$, $\sqrt{3}$ and $\sqrt{6}$ are linearly independent.

Now we can give an equivalent formulation of what it means for a complex number to be algebraic:

Proposition 2.9 *Let α be a complex number. Then the following are equivalent:*

1. *α is algebraic;*
2. *the field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is of finite degree.*

Proof (1) $\Rightarrow$ (2). Suppose that α is algebraic. Then let $m(X) = X^n + c_1X^{n-1} + \cdots + c_n$ denote the minimal polynomial for α, so that

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

or, rearranging:

$$\alpha^n = -(c_1\alpha^{n-1} + \cdots + c_n). \tag{2.2}$$

As α is algebraic, every element of $\mathbb{Q}(\alpha)$ can be written as a polynomial in α. Further, if this polynomial has degree n or above, we can reduce the degree by replacing all occurrences of α^r for $r \geq n$ using (2.2). It follows that every element of $\mathbb{Q}(\alpha)$ can be written as an expression

$$a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_0$$

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

Furthermore, this expression is unique—if an element can be written in two different ways

$$a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_0 = b_{n-1}\alpha^{n-1} + b_{n-2}\alpha^{n-2} + \cdots + b_0$$

then subtracting one side from the other gives a polynomial of degree strictly smaller than n with α as a root. However, the minimal polynomial is $m(X)$, of degree n, so there can be no polynomial of degree less than n with α as a root.

So every element of $\mathbb{Q}(\alpha)$ is a unique rational linear combination of the n elements $1, \alpha, \ldots, \alpha^{n-1}$. Thus $\mathbb{Q}(\alpha)$ is n-dimensional as a vector space over $\mathbb{Q}$, and therefore $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is finite.

(2) $\Rightarrow$ (1). If $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is some finite number, n, say, then any $n + 1$ elements of the $\mathbb{Q}$-vector space $\mathbb{Q}(\alpha)$ are linearly dependent. In particular, the elements $1, \alpha, \ldots, \alpha^n$ are linearly dependent, so that there exists a linear relationship

$$a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0,$$

and consequently α satisfies a polynomial equation over $\mathbb{Q}$, and is algebraic. □

The proof actually shows something more:

Corollary 2.10 *Suppose that α is algebraic. Then the degree of the extension $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is the same as the degree of the minimal polynomial of α over $\mathbb{Q}$. Every element of $\mathbb{Q}(\alpha)$ can be written as a polynomial in α of degree less than $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.*

Proof This just follows from the proof of Proposition 2.9. □

More generally, the same argument shows that if K is any field, then an element α is algebraic over K (i.e., satisfies a polynomial equation with coefficients in K) if and only if $[K(\alpha) : K]$ is finite, and that then this degree is also the degree of the minimal polynomial of α over K.

We now use Proposition 2.9 to prove that the algebraic numbers form a *field*; that is, the sum, difference and product of any two algebraic numbers is again algebraic, as is the quotient of an algebraic number by a non-zero algebraic number.

We can adjoin more than one number to a field; for example, if both α and β are algebraic, define $\mathbb{Q}(\alpha, \beta)$ to be $\mathbb{Q}(\alpha)(\beta)$, that is, all polynomial expressions in β with coefficients in $\mathbb{Q}(\alpha)$. It is easy to see that this just gives all the polynomials in the two variables α and β.

Corollary 2.11 *Suppose that α and β are algebraic. Then $\alpha + \beta$, $\alpha - \beta$ and $\alpha\beta$ are algebraic; if also $\beta \neq 0$, then α/β is algebraic.*

Proof As α and β are algebraic, Proposition 2.9 states that $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ and $[\mathbb{Q}(\beta) : \mathbb{Q}]$ are both finite. Write

$$m = [\mathbb{Q}(\alpha) : \mathbb{Q}],$$
$$n = [\mathbb{Q}(\beta) : \mathbb{Q}].$$

Let's explain that $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ is finite. A typical element of $\mathbb{Q}(\alpha, \beta)$ is a polynomial expression $\sum_{i=0}^{k} \sum_{j=0}^{l} a_{ij} \alpha^i \beta^j$. However, every α^i with $i \geq m$ can be written as a polynomial in α of degree at most $m - 1$ (by Corollary 2.10), and similarly every β^j with $j \geq n$ can be written as a polynomial in β of degree at most $n - 1$. Substituting these in, we see that any element of $\mathbb{Q}(\alpha, \beta)$ can be written

$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a'_{ij} \alpha^i \beta^j$$

for some a'_{ij}. It therefore follows that $\mathbb{Q}(\alpha, \beta)$ is spanned by the set $\{\alpha^i \beta^j \mid 0 \leq i \leq m - 1, 0 \leq j \leq n - 1\}$. Thus $\mathbb{Q}(\alpha, \beta)$ has a finite spanning set as a $\mathbb{Q}$-vector space, and therefore $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ is finite.

To prove that $\alpha + \beta$ is algebraic, we simply note that $\alpha + \beta \in \mathbb{Q}(\alpha, \beta)$, so that $\mathbb{Q}(\alpha + \beta) \subseteq \mathbb{Q}(\alpha, \beta)$, and so $[\mathbb{Q}(\alpha + \beta) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$. It follows that $[\mathbb{Q}(\alpha + \beta) : \mathbb{Q}]$ is finite, and, again applying Proposition 2.9, $\alpha + \beta$ must be algebraic.

The arguments for $\alpha - \beta$, $\alpha\beta$ and α/β are all similar, as each lies in $\mathbb{Q}(\alpha, \beta)$. □

While this proof is easy, it doesn't give any recipe for writing down a polynomial with $\alpha + \beta$ as a root, given polynomials with α and β as roots. We will discuss this at the end of Sect. 2.6.

This is exactly what we need to deduce our desired result:

Corollary 2.12 *The algebraic numbers $\mathcal{A}$ form a field.*

Exercise 2.5 Find an algebraic number α where $\mathbb{Q}(\alpha)$ is strictly larger than the set $\{a + b\alpha \mid a, b \in \mathbb{Q}\}$.

Exercise 2.6 Let $\alpha = \sqrt[3]{2}$. Write $\frac{\alpha^2-1}{\alpha+2}$ as a polynomial in α with rational coefficients.

Exercise 2.7 Let α be a root of $X^4 + 2X + 1 = 0$. Write $\frac{\alpha+1}{\alpha^2-2\alpha+2}$ as a polynomial in α with rational coefficients.

2.4 Number Fields

Although $\mathcal{A}$ is countable, it is still very much larger than the rational numbers $\mathbb{Q}$ (it has infinite degree over $\mathbb{Q}$, for example), and is too large to be really useful.

The fields in which we are going to generalise ideas of primes, factorisations, and so on, are the finite extensions of $\mathbb{Q}$:

Definition 2.13 A field K is a *number field* if it is a finite extension of $\mathbb{Q}$. The *degree* of K is the degree of the field extension $[K : \mathbb{Q}]$, i.e., the dimension of K as a vector space over $\mathbb{Q}$.

In particular, every element in K lies inside a finite extension of $\mathbb{Q}$, and, by Proposition 2.9, is necessarily algebraic.

Example 2.14

1. $\mathbb{Q}$ itself is a number field. Indeed, it will serve as the inspiration for our general theory.
2. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a number field, since every element is a $\mathbb{Q}$-linear combination of 1 and $\sqrt{2}$, so $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, which is finite.
3. Similarly, $\mathbb{Q}(i)$ is a number field, as is $\mathbb{Q}(\sqrt{d})$ for any integer d. Note that we may assume that d is not divisible by a square ("squarefree"), because if $d = m^2 d'$, $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$.
   Indeed, it is easy to see (from the quadratic formula) that every quadratic field $\mathbb{Q}(\alpha)$ is of this form. So every quadratic number field is $\mathbb{Q}(\sqrt{d})$ for some squarefree d.
4. $\mathbb{Q}(\sqrt[3]{2})$ is a number field, as $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, which is finite. Every element can be written in the form

$$a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2,$$

   for $a, b, c \in \mathbb{Q}$, so 1, $\sqrt[3]{2}$ and $(\sqrt[3]{2})^2$ form a basis for $\mathbb{Q}(\sqrt[3]{2})$ as a vector space over $\mathbb{Q}$.

5. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is also a number field; every element can be written in the form $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ for rational numbers a, b, c and d, so that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ forms a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$—it follows that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ (we showed the linear independence in Exercise 2.4).
6. $\mathbb{Q}(\pi)$ is *not* a number field; π does not satisfy any polynomial equation over $\mathbb{Q}$ (as it is transcendental); therefore $[\mathbb{Q}(\pi) : \mathbb{Q}]$ is infinite.

Notice that every number field contains the rationals, so is infinite and is of characteristic 0.

Recall that the *characteristic* of a field is 0 if $1 + 1 + \cdots + 1$ is never equal to 0, and is p if p is the smallest number such that $1 + 1 + \cdots + 1 = 0$, where p is the number of 1s in the left-hand sum. Fields of characteristic 0 always contain $\mathbb{Q}$. Fields of characteristic p exist for any prime number p. They always contain the integers modulo p, $\{0, 1, \ldots, p-1\}$, which is the smallest field of characteristic p, and which we denote by $\mathbb{F}_p$.

On the other hand, every element of a number field is algebraic, so is a root of a polynomial with rational coefficients. As all roots of such polynomials are complex numbers, this means that we can view every number field as a subfield of the complex numbers $\mathbb{C}$. However, it is sometimes important to realise that there is not usually a natural way to do this; if a number field contains a square root $\sqrt{-1}$ of -1, we have a choice whether to view this as i or as $-i$ inside the complex numbers. In Chap. 3 we will think more about this issue.

Occasionally it will be useful to know that every extension is *simple*, that is, it is generated by a single element.

We need a preliminary result.

Lemma 2.15 *Suppose that $f(X) \in \mathbb{Q}[X]$ is an irreducible polynomial. Then it has distinct roots in $\mathbb{C}$.*

Proof Over $\mathbb{C}$, factorise $f(X)$ as $c\prod_{i=1}^{r}(X-\gamma_i)^{d_i}$.

If the lemma were false, $d_i > 1$ for some i, and so $f(X)$ would have a factor $(X-\gamma_i)^2$.

Writing $f(X) = (X-\gamma_i)^2 g(X)$, we see that $(X-\gamma_i)$ is also a factor of the derivative $f'(X)$. So $(X-\gamma_i)$ is a common factor of f and f', thus showing that the highest common factor h of f and f' must be of degree at least 1. But the highest common factor of f and f' is obtained by Euclid's algorithm in $\mathbb{Q}[X]$, and is a polynomial with rational coefficients that divides into both f and f'. However, f is irreducible, so its only factors are 1 and f. Since h has degree at least 1, we conclude that $h = f$. But then $f \mid f'$, which is absurd, since the degree of f is bigger than the degree of f', which is a nonzero polynomial (as f has degree $d \geq 1$). □

Remark 2.16 More generally, the proof shows that any irreducible polynomial over a field of characteristic 0 has distinct roots. In characteristic p, it can happen for an irreducible polynomial that its derivative is 0, since it may only involve terms in X^p, whose derivatives are divisible by p, and which therefore vanish; consider the polynomial $f(X) = X^p$ in a field of characteristic p; although this is not irreducible, it is an example where f divides f', as $f' = 0$.

Theorem 2.17 (Primitive Element) *Suppose $K \subseteq L$ is a finite extension of fields of characteristic 0 (e.g., number fields). Then $L = K(\gamma)$ for some element $\gamma \in L$.*

Proof Suppose L is generated over K by m elements. We first treat the case $m = 2$. So suppose $L = K(\alpha, \beta)$, and let f and g denote the minimal polynomials of α and β over K. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_s$ be the roots of f in $\mathbb{C}$, and let $\beta_1 = \beta, \beta_2, \ldots, \beta_t$ be the roots of g. Irreducible polynomials always have distinct roots (Lemma 2.15). Thus $X = \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}$ is the only solution (if $j \neq 1$) to

$$\alpha_i + X\beta_j = \alpha_1 + X\beta_1.$$

Choosing a $c \in K$ different from each of these X's, then each $\alpha_i + c\beta_j$ is different from $\alpha + c\beta$. We claim that $\gamma = \alpha + c\beta$ generates L over K. Certainly $\gamma \in K(\alpha, \beta) = L$. Now it suffices to verify that $\alpha, \beta \in K(\gamma)$.

The polynomials $g(X)$ and $f(\gamma - cX)$ both have coefficients in $K(\gamma)$, and have β as a root. The other roots of $g(X)$ are $\beta_2, \ldots, \beta_t$, and, as $\gamma - c\beta_j$ is not any α_i, unless $i = j = 1$, β is the only common root of $g(X)$ and $f(\gamma - cX)$. Thus, $(X - \beta)$ is the highest common factor of $g(X)$ and $f(\gamma - cX)$. But the highest common factor is a polynomial defined over any field containing the coefficients of the original two polynomials (think about how the Euclidean algorithm works for polynomials). In particular, it follows that $X - \beta$ has coefficients in $K(\gamma)$, so that $\beta \in K(\gamma)$. Then $\alpha = \gamma - c\beta \in K(\gamma)$. The result follows for $m = 2$.

Now we turn to the case where $m > 2$. We can prove this using the result we have just proven. After all, if $L = K(\alpha_1, \ldots, \alpha_m)$, we can view this as $K(\alpha_1, \ldots, \alpha_{m-2})(\alpha_{m-1}, \alpha_m)$, and the case $m = 2$ allows us to write this as $K(\alpha_1, \ldots, \alpha_{m-2})(\gamma_{m-1})$. Rewriting this as $K(\alpha_1, \ldots, \alpha_{m-3})(\alpha_{m-2}, \gamma_{m-1})$, and using the case $m = 2$ again reduces the number further still. Continuing in this way, we eventually get down to just one element. □

This proof uses properties of fields of characteristic 0 in two places. Firstly, we used the fact that irreducible polynomials always have distinct roots, which is true for any field of characteristic 0. And then we chose a value of c different from all values in some finite set, which we can do because fields of characteristic 0 contain $\mathbb{Q}$, and so are infinite.

Corollary 2.18 *Let K be a number field. Then $K = \mathbb{Q}(\gamma)$ for some element γ.*

Proof Simply apply Theorem 2.17. □

Let's illustrate this argument with one example.

Example 2.19 By the previous corollary, it should be possible to express the number field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ as $\mathbb{Q}(\gamma)$ for some element γ. By looking at the proof of Theorem 2.17, it seems that we should be able to take $\gamma = \sqrt{2} + c\sqrt{3}$ for almost any choice of c (only finitely many values might be excluded). Let's try $c = 1$, so that $\gamma = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then

$$\begin{aligned} 1 &= 1 \\ \gamma &= \sqrt{2} + \sqrt{3} \\ \gamma^2 &= 5 + 2\sqrt{6} \\ \gamma^3 &= 11\sqrt{2} + 9\sqrt{3} \end{aligned}$$

and we see that $\sqrt{2} = (\gamma^3 - 9\gamma)/2$ and $\sqrt{3} = (11\gamma - \gamma^3)/2$. It follows that both $\sqrt{2}$ and $\sqrt{3}$ can be written as polynomials in γ, so that $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\gamma)$. Therefore $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\gamma)$. On the other hand, $\gamma \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, which gives the other inclusion $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and shows that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\gamma)$, as required.

Exercise 2.8 What is the degree of $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2})$ over $\mathbb{Q}$?

Exercise 2.9 Show that $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

2.5 Integrality

We are going to do number theory in number fields, enlarged versions of the rational numbers. That is, we are going to study prime numbers, divisibility, and so on, in these larger fields.

Recall that prime numbers are defined as those positive integers which have no divisors other than themselves and 1. Even to talk about divisibility needs some notion of integrality; in $\mathbb{Q}$, any rational number is divisible by any non-zero rational number. It is only in the integers that divisibility and prime numbers are properly defined.

When we "do number theory", we almost always refer to properties of the integers $\mathbb{Z}$, rather than $\mathbb{Q}$. So to work in a number field K, we need to define a subset $\mathbb{Z}_K$ of "integers in K".

It would be nice if this subset satisfied the same algebraic properties as $\mathbb{Z}$—namely, $\mathbb{Z}_K$ should be a ring, so that we can add, subtract and multiply within $\mathbb{Z}_K$. Clearly we would like the integers in $\mathbb{Q}$ to turn out to be $\mathbb{Z}$!

It would also be desirable to arrange that, given two number fields $K \subseteq L$ and an element $\alpha \in K$, that α is an integer in K if and only if it is an integer in L. That is, if $K \subseteq L$ is an extension of number fields, we require $\mathbb{Z}_L \cap K = \mathbb{Z}_K$.

At the end of Chap. 1, we saw our first example of working in a more general number field. There, we looked at the Gaussian integers,

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

which seemed to have the appropriate properties in $\mathbb{Q}(i)$. It seems reasonable to hope that our definition of integers should give $\mathbb{Z}[i]$ as the integers for $\mathbb{Q}(i)$.

We have also seen that every number field can be written in the form $\mathbb{Q}(\gamma)$, and at first glance, it might seem reasonable to suggest that we define its integers to be $\mathbb{Z}[\gamma]$. This is, after all, a ring; the elements are polynomials in γ with integer coefficients,

and two of these can be added, subtracted or multiplied. In addition, it gives the right answer for $\mathbb{Q}(i)$.

Unfortunately, a moment's reflection will reveal that this is not a good definition. Indeed, it isn't even well-defined! That is, we may be able to write our number field in more than one way as $\mathbb{Q}(\gamma)$, but these may give different answers for the integers. For example, as $\sqrt{8} = 2\sqrt{2}$, we see that $\mathbb{Q}(\sqrt{8}) = \mathbb{Q}(\sqrt{2})$; on the other hand, $\mathbb{Z}[\sqrt{8}] \neq \mathbb{Z}[\sqrt{2}]$, since $\sqrt{2} \notin \mathbb{Z}[\sqrt{8}]$.

We need some more intrinsic way to determine which element of a given number field is an integer.

Associated to α is its minimal polynomial over $\mathbb{Q}$, the monic polynomial with rational coefficients of smallest degree which has α as a root. We're going to use this to give our definition of an integer:

Definition 2.20 Let α be an algebraic number. We say that α is an *algebraic integer* if the minimal polynomial of α over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.

Before we explain that the algebraic integers form a *ring*, that is, they are closed under addition, subtraction and multiplication, let's look at some examples:

Example 2.21

1. Every integer n is an algebraic integer. Its minimal polynomial over $\mathbb{Q}$ is $X - n$, and the coefficients of this polynomial are indeed integral.
2. i is an algebraic integer, as its minimal polynomial is $X^2 + 1$, which is in $\mathbb{Z}[X]$.
3. $\sqrt{2}$ is an algebraic integer, as its minimal polynomial is $X^2 - 2$, again in $\mathbb{Z}[X]$.
4. $\omega = (-1 + \sqrt{-3})/2$ is an algebraic integer, perhaps surprisingly; it is a root of the polynomial $X^2 + X + 1$—since this polynomial is irreducible, this must be the minimal polynomial of ω.
5. $(-1 + \sqrt{3})/2$ is *not* an algebraic integer, as its minimal polynomial is $X^2 + X - \frac{1}{2}$, which involves fractional coefficients.
6. π is not an algebraic integer, since it is not even an algebraic number.

You might be surprised that $(-1 + \sqrt{-3})/2$ should be an integer, but that $(-1 + \sqrt{3})/2$ isn't, but apart from that, I hope that you agree that the definition looks reasonable.

When it comes to checking whether or not a given algebraic number α is an algebraic integer, it is sometimes convenient to be able to check a weaker condition.

Lemma 2.22 *Suppose that α satisfies any monic polynomial with coefficients in $\mathbb{Z}$. Then α is an algebraic integer.*

Proof Suppose α is a root of the monic polynomial $f(X) \in \mathbb{Z}[X]$. Let $m(X) \in \mathbb{Q}[X]$ denote the minimal polynomial of α over $\mathbb{Q}$. We will show that $m(X) \in \mathbb{Z}[X]$. We have already seen that $m(X) | f(X)$, so that $f(X) = q(X)m(X)$ for some polynomial $q(X) \in \mathbb{Q}[X]$. Since $f(X)$ and $m(X)$ are both monic, clearly $q(X)$ is also.

So $f(X) = q(X)m(X)$ expresses $f(X) \in \mathbb{Z}[X]$ as a product of two monic polynomials $q(X)$ and $m(X)$ with rational coefficients. We explain that this implies $q(X)$ and $m(X)$ are both in $\mathbb{Z}[X]$.

Choose positive integers a and b so that $aq(X)$ and $bm(X)$ are polynomials with integer coefficients, and where the highest common factors of the coefficients of $aq(X)$ and $bm(X)$ are both 1. (Indeed, a and b are just the least common multiples of the denominators of the coefficients of q and m respectively.) Then

$$(ab)f(X) = aq(X).bm(X).$$

If $ab \neq 1$, choose a prime number $p|ab$. There are coefficients of $aq(X)$ and $bm(X)$ not divisible by p. So there are also terms in the product whose coefficients are not divisible by p (consider the term in the product coming from the first term of $aq(X)$ with coefficient not divisible by p with the first term of $bm(X)$ with coefficient not divisible by p). On the other hand, the product is $(ab)f(X)$, so all the coefficients must be divisible by the integer ab, and therefore by p. This contradiction shows that $ab = 1$, and therefore $a = b = 1$, as a and b are positive integers.

Therefore both $q(X)$ and $m(X)$ are already in $\mathbb{Z}[X]$. In particular, $m(X) \in \mathbb{Z}[X]$, and so the minimal polynomial of α has integral coefficients. □

Remark 2.23 Here, we have essentially proven Gauss's Lemma: If a polynomial $f(X) \in \mathbb{Z}[X]$ is reducible in $\mathbb{Q}[X]$ then it is reducible in $\mathbb{Z}[X]$ (that is, if $f(X)$ factorises into polynomials with rational coefficients then it factorises into polynomials with integer coefficients).

Remark 2.24 Suppose that α is an algebraic number. Then α is the root of some monic polynomial with coefficients in $\mathbb{Q}$:

$$X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_0 = 0.$$

Let d be an integer which is a common multiple of all the denominators of $a_{n-1}, \ldots, a_0$. Then $d\alpha$ is a root of

$$X^n + a_{n-1}dX^{n-1} + a_{n-2}d^2X^{n-2} + \cdots + a_0d^n = 0,$$

which is a monic polynomial with integer coefficients. Therefore $d\alpha$ is an algebraic integer. This shows that every algebraic number has an integer multiple which is an algebraic integer. Equivalently, every algebraic number can be expressed as the quotient of an algebraic integer by an element of $\mathbb{Z}$.

Exercise 2.10 Show that $\frac{1+\sqrt{5}}{2}$ is an algebraic integer.

Exercise 2.11 Show that $\frac{1+\sqrt{3}}{\sqrt{2}}$ is an algebraic integer.

Exercise 2.12 Let a be an integer. Show that $\alpha = (1 + a^{1/3} + a^{2/3})/3$ is a root of

$$X^3 - X^2 + \frac{1-a}{3}X - \frac{(1-a)^2}{27} = 0.$$

[*Hint: Expand* $(\alpha - 1/3)^3$.] Deduce that if $a \equiv 1 \pmod 9$, then α is an algebraic integer.

2.6 The Ring of All Algebraic Integers

We will want to study factorisation and so on in number fields. This will require a definition of integers and primes in these fields. Amongst the properties that we would like to hold is that the integers in a number field have the same algebraic structure as the integers $\mathbb{Z}$; in particular, that they form a ring, so that we can add, subtract and multiply two integers.

Given two integers α and β, we will need to prove, for example, that $\alpha + \beta$ is an integer. From the definition, it looks as if this will mean finding a monic polynomial with integer coefficients that has $\alpha + \beta$ as a root.

Our approach will resemble the method we used earlier to show that the algebraic numbers form a field: we will reformulate the condition on integrality into one involving abstract algebra and which resembles Proposition 2.9. By a process rather similar to Corollary 2.11, we will show that if α and β are algebraic integers, so are $\alpha + \beta$, $\alpha - \beta$ and $\alpha\beta$.

Looking back at Proposition 2.9, we reformulated the property of being an algebraic number in terms of field extensions of $\mathbb{Q}$ of finite degree. We will do something similar for $\mathbb{Z}$, and our reformulation will involve the ring $\mathbb{Z}[\alpha]$, consisting of all polynomial expressions in α with integer coefficients. For algebraic numbers, we then used results and terminology from vector spaces over fields; the analogous concept for rings is called a *module*.

Recall that a *module* M over a ring R is like a vector space over a field; we should be able to add two elements of M together to get another element of M, and to multiply an element of M by an element of R, in such a way that the same rules are satisfied as for vector spaces.

The theory of modules over rings is a little more complicated than vector spaces over fields, but for now at least, we just need the concept which is analogous to "finite dimensional" for vector spaces. The appropriate condition is that the module $\mathbb{Z}[\alpha]$ is *finitely generated* over $\mathbb{Z}$. This means that there are finitely many elements $\omega_1, \ldots, \omega_n \in \mathbb{Z}[\alpha]$ such that every element of $\mathbb{Z}[\alpha]$ can be written as a sum $a_1\omega_1 + \cdots + a_n\omega_n$ for suitable integers $a_1, \ldots, a_n \in \mathbb{Z}$.

Proposition 2.25 *Let $\alpha \in \mathbb{C}$. The following are equivalent:*

1. *α is an algebraic integer;*
2. *$\mathbb{Z}[\alpha]$ is a finitely generated module over $\mathbb{Z}$.*

Proof (1) $\Rightarrow$ (2). Suppose that α is an algebraic integer. Then it is a root of a monic polynomial $f(X) \in \mathbb{Z}[X]$ of some degree n. Given any polynomial $g(X) \in \mathbb{Z}[X]$, write

$$g(X) = q(X)f(X) + r(X)$$

for $q(X), r(X) \in \mathbb{Z}[X]$, and where $r(X) = 0$ or the degree of $r(X)$ is less than n. (If $f(X)$ were not monic, we could only deduce that $q(X)$ and $r(X)$ would have *rational* coefficients.)

Substitute in $X = \alpha$; then $g(\alpha) = r(\alpha)$ as α is a root of f. This shows that $g(\alpha)$ can also be expressed as a polynomial expression of degree less than n, so $g(\alpha)$ can be written as a linear combination of $1, \alpha, \ldots, \alpha^{n-1}$ with integer coefficients.

We conclude that any polynomial expression in α with integer coefficients can be expressed as an integer linear combination of $1, \alpha, \ldots, \alpha^{n-1}$. Therefore $\mathbb{Z}[\alpha]$ is finitely generated as a $\mathbb{Z}$-module.

(2) $\Rightarrow$ (1). Suppose that $\mathbb{Z}[\alpha] = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$. For each i, the product $\alpha\omega_i$ is again in $\mathbb{Z}[\alpha]$, so can be written as a linear combination of the spanning set:

$$\alpha\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j \tag{2.3}$$

with each $a_{ij} \in \mathbb{Z}$. Consider the column vector $\mathbf{v} = (\omega_1 \ \cdots \ \omega_n)^t$. Then (2.3) implies that $\alpha\mathbf{v} = A\mathbf{v}$ where $A = (a_{ij})$. That is, $\mathbf{v}$ is an eigenvector of A with eigenvalue α. As α is an eigenvalue, it is a root of the characteristic polynomial of A. Characteristic polynomials are always monic; also, as the entries of A are integral, its characteristic polynomial has coefficients in $\mathbb{Z}$. Thus α is a root of a monic polynomial with integer coefficients, and so α is integral. □

The next result is really a corollary to the proof of the previous proposition, and is a mild generalisation:

Corollary 2.26 *Let R be a ring containing $\mathbb{Z}$. If R is finitely generated as a $\mathbb{Z}$-module, then every element $\alpha \in R$ is the root of a monic polynomial with coefficients in $\mathbb{Z}$.*

Proof We argue exactly as above; since R is finitely generated, $R = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$. For each i, we have $\alpha\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j$ for some integers $a_{ij} \in \mathbb{Z}$, and then α is a root of the characteristic polynomial for the matrix (a_{ij}), as required. □

Next, consider what happens for two algebraic integers α and β:

Proposition 2.27 *Suppose that α and β are algebraic integers. Then $\mathbb{Z}[\alpha, \beta]$ is finitely generated as a $\mathbb{Z}$-module.*

Proof By Proposition 2.25, $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are both finitely generated as $\mathbb{Z}$-modules. That is, there are elements $\omega_1, \ldots, \omega_m \in \mathbb{Z}[\alpha]$ such that every element of $\mathbb{Z}[\alpha]$ can be written as a $\mathbb{Z}$-linear combination of these elements. Similarly, there are elements $\theta_1, \ldots, \theta_n \in \mathbb{Z}[\beta]$ such that every element of $\mathbb{Z}[\beta]$ is a $\mathbb{Z}$-linear combination of these elements. Let's show that every element of $\mathbb{Z}[\alpha, \beta]$ is a $\mathbb{Z}$-linear combination of the finite set $\{\omega_i\theta_j \mid 1 \le i \le m, 1 \le j \le n\}$.

Every element of $\mathbb{Z}[\alpha, \beta]$ can be written as a polynomial $\sum_{k,l} a_{kl}\alpha^k\beta^l$, with $a_{kl} \in \mathbb{Z}$. Since each $\alpha^k \in \mathbb{Z}[\alpha]$, it can be written as some $\mathbb{Z}$-linear combination

of $\{\omega_i \mid 1 \leq i \leq m\}$. Similarly, β^j can be written as a $\mathbb{Z}$-linear combination of $\{\theta_j \mid 1 \leq j \leq n\}$. Substituting these in, we see that every element can be written as a $\mathbb{Z}$-linear combination of the set $\{\omega_i\theta_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$, as required. □

After this reformulation, it is easy to prove that algebraic integers form a ring:

Corollary 2.28 *The set of all algebraic integers forms a ring.*

Proof Let α and β be algebraic integers. We need to check that $\alpha + \beta$, $\alpha - \beta$ and $\alpha\beta$ are algebraic integers. Since $\alpha + \beta \in \mathbb{Z}[\alpha, \beta]$, and Proposition 2.27 shows that $\mathbb{Z}[\alpha, \beta]$ is finitely generated as a $\mathbb{Z}$-module, Proposition 2.25 implies that $\alpha + \beta$ is an algebraic integer.

As $\alpha - \beta$ and $\alpha\beta$ are also in $\mathbb{Z}[\alpha, \beta]$, the same argument applies to show that they are also integral. □

Not only does this prove the result we want, but the argument of Proposition 2.25 also suggests a way to construct polynomials satisfied by the sum (or difference, or product) of two algebraic numbers.

Example 2.29 To explain the procedure, let's show that the sum

$$\theta = \left(\frac{1+\sqrt{5}}{2}\right) + \left(\frac{-1+\sqrt{-3}}{2}\right) = (\sqrt{5} + \sqrt{-3})/2$$

is an algebraic integer, by computing its minimal polynomial.

Write $\alpha = (1+\sqrt{5})/2$ and $\beta = (-1+\sqrt{-3})/2$. Then α has minimal polynomial $X^2 - X - 1$ and β has minimal polynomial $X^2 + X + 1$. One way to proceed is as follows.

Form the vector $\mathbf{v} = (1\ \alpha\ \beta\ \alpha\beta)^t$. We are going to find matrices A and B with entries in $\mathbb{Z}$ such that $A\mathbf{v} = \alpha\mathbf{v}$ and $B\mathbf{v} = \beta\mathbf{v}$. That is, α is an eigenvalue of A, and β is an eigenvalue of B. Then $(A + B)\mathbf{v} = (\alpha + \beta)\mathbf{v}$, and so $\alpha + \beta$ is an eigenvalue of $A + B$. It is therefore a root of the characteristic polynomial of $A + B$, which is defined over $\mathbb{Z}$, since the entries of $A + B$ are integers. This gives a polynomial with $\alpha + \beta$ as a root.

Let's first try to construct the matrix A. It should be a 4×4 matrix such that

$$A\begin{pmatrix}1\\ \alpha\\ \beta\\ \alpha\beta\end{pmatrix} = \alpha\begin{pmatrix}1\\ \alpha\\ \beta\\ \alpha\beta\end{pmatrix} = \begin{pmatrix}\alpha\\ \alpha^2\\ \alpha\beta\\ \alpha^2\beta\end{pmatrix}.$$

But α is a root of $X^2 = X + 1$, so $\alpha^2 = \alpha + 1$, and so we need to solve

$$A\begin{pmatrix}1\\ \alpha\\ \beta\\ \alpha\beta\end{pmatrix} = \begin{pmatrix}\alpha\\ \alpha+1\\ \alpha\beta\\ (\alpha+1)\beta\end{pmatrix},$$

and it is easy to see that

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Similarly, we can find a matrix B with the property that

$$B \begin{pmatrix} 1 \\ \alpha \\ \beta \\ \alpha\beta \end{pmatrix} = \beta \begin{pmatrix} 1 \\ \alpha \\ \beta \\ \alpha\beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha\beta \\ \beta^2 \\ \alpha\beta^2 \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha\beta \\ -(\beta+1) \\ -\alpha(\beta+1) \end{pmatrix};$$

take

$$B = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & -1 & 0 \\ 0 & -1 & 0 & -1 \end{pmatrix}.$$

Then

$$A + B = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ -1 & 0 & -1 & 1 \\ 0 & -1 & 1 & 0 \end{pmatrix},$$

and the argument above shows that θ should be a root of the characteristic polynomial of $A + B$.

Exercise 2.13 Show that this characteristic polynomial is $X^4 - X^2 + 4$, and verify explicitly that θ is a root of this polynomial.

In the same way, as $AB\mathbf{v} = A(B\mathbf{v}) = A(\beta\mathbf{v}) = \beta(A\mathbf{v}) = \alpha\beta\mathbf{v}$, $\alpha\beta$ is an eigenvalue of AB, and is therefore a root of the characteristic polynomial of AB.

More generally, if α is a root of an equation of degree m, and β is a root of an equation of degree n, form the vector of length mn:

$$\mathbf{v} = (1, \ldots, \alpha^{m-1}, \beta, \ldots, \alpha^{m-1}\beta, \ldots \ \ldots; \beta^{n-1}, \ldots, \alpha^{m-1}\beta^{n-1})^t.$$

As above, we can find $mn \times mn$-matrices A and B such that $A\mathbf{v} = \alpha\mathbf{v}$ and $B\mathbf{v} = \beta\mathbf{v}$. Then A and B will be $mn \times mn$-matrices, $\alpha + \beta$, $\alpha - \beta$ and $\alpha\beta$ are easily seen to be eigenvalues of $A + B$, $A - B$ and AB respectively (with $\mathbf{v}$ as eigenvector), and the characteristic polynomials of $A + B$, $A - B$ and AB have degree mn.

Further, notice that if α and β are both algebraic integers, then the matrices A and B have entries in $\mathbb{Z}$, and so the entries of $A + B$, $A - B$ and AB are all also in $\mathbb{Z}$. Therefore the characteristic polynomials of these three matrices are all integral, and are monic by definition, so this gives another proof that the eigenvalues $\alpha + \beta$, $\alpha - \beta$ and $\alpha\beta$ are all algebraic integers.

Exercise 2.14 Use this method to find a degree 6 polynomial satisfied by $\sqrt{2}+\sqrt[3]{2}$.

Of course, the same method also shows that the sum, difference and product of any two algebraic numbers is again algebraic; the two matrices A and B will in general no longer be integral, but have rational entries. We can extend the method to the case of quotients; if $\beta \neq 0$, then B will be invertible, and then $\mathbf{v}$ is an eigenvector of AB^{-1} with eigenvalue α/β. This quotient is a root of the characteristic polynomial of the rational matrix AB^{-1}, as required.

2.7 Rings of Integers of Number Fields

Now we have an obvious definition for the integers in a number field.

Definition 2.30 Let K be a number field. Then the integers in K are

$$\mathbb{Z}_K = \{\alpha \in K \mid \alpha \text{ is an algebraic integer}\}.$$

Probably the first check to make is that this gives the right answer for the rational number field $\mathbb{Q}$. Luckily, this is straightforward; a rational $a \in \mathbb{Q}$ has minimal polynomial $X - a$, and the coefficients are in $\mathbb{Z}$ if and only if $a \in \mathbb{Z}$. So the integers in $\mathbb{Q}$ using Definition 2.30 are indeed $\mathbb{Z}$, as one hopes.

Also, if $K \subseteq L$ is an extension of number fields and $\alpha \in K$, then α is an integer in K if and only if it is an integer in L. This follows simply because the condition determining whether or not α is an algebraic integer makes no reference to any field K.

Corollary 2.31 *Let K be a number field. Then $\mathbb{Z}_K$ is a ring.*

Proof Given $\alpha, \beta \in \mathbb{Z}_K$, we need to check that $\alpha + \beta$, $\alpha - \beta$ and $\alpha\beta$ all lie in $\mathbb{Z}_K$. But they certainly all lie in K, and Corollary 2.28 implies that they are all algebraic integers, so they lie in $\mathbb{Z}_K$, as required. □

Remark 2.32 $\mathbb{Z}_K$ is even an integral domain, since $\mathbb{Z}_K \subset K$, and as K is a field, it has no zero-divisors.

We say that $\mathbb{Z}_K$ is the *ring of integers* of K. In the literature, you will often see the ring of integers written as $\mathcal{O}_K$, for historical reasons (an older terminology for ring of integers is *order*—this word is still used to refer to certain subrings of $\mathbb{Z}_K$).

The following generalisation of Proposition 2.25 allows us to characterise the ring of integers $\mathbb{Z}_K$ as the largest subring of K which is a finitely generated $\mathbb{Z}$-module:

Proposition 2.33 *Suppose R is a subring of a number field K, and that R is finitely generated as a $\mathbb{Z}$-module. Then $R \subseteq \mathbb{Z}_K$.*

Proof This is immediate from Corollary 2.26. □

Earlier, we suggested that the ring of integers in $\mathbb{Q}(i)$ should be $\mathbb{Z}[i]$. We will now compute the rings of integers in all quadratic fields $\mathbb{Q}(\sqrt{d})$.

Proposition 2.34 *Suppose that d is a squarefree integer (i.e., not divisible by the square of any prime). Then*

1. *If $d \equiv 2$ or $3 \pmod 4$, then the ring of integers in $\mathbb{Q}(\sqrt{d})$ is*

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$

2. *If $d \equiv 1 \pmod 4$, then the ring of integers in $\mathbb{Q}(\sqrt{d})$ is*

$$\mathbb{Z}[\rho_d] = \{a + b\rho_d \mid a, b \in \mathbb{Z}\}$$

where $\rho_d = \frac{1+\sqrt{d}}{2}$.

Proof Let $\alpha = a+b\sqrt{d}$ with $a, b \in \mathbb{Q}$. Then α satisfies the equation $(X-a)^2 = b^2 d$, or

$$X^2 - 2aX + (a^2 - b^2 d) = 0.$$

We seek conditions on a and b to make this have integer coefficients. This implies that

$$\begin{aligned} 2a &\in \mathbb{Z} \\ a^2 - b^2 d &\in \mathbb{Z} \end{aligned}$$

Clearly the first condition implies $a \in \mathbb{Z}$ or $a = \frac{A}{2}$ where A is an odd integer. In the first case, the second condition becomes $b^2 d \in \mathbb{Z}$, and, as d is squarefree, this requires $b \in \mathbb{Z}$. So the set $\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ is always contained in the ring of integers.

Let's examine when the second case can arise. Here $a = \frac{A}{2}$, and we need

$$\frac{A^2}{4} - b^2 d \in \mathbb{Z},$$

or

$$A^2 - 4b^2 d \equiv 0 \,(\mathrm{mod}\, 4).$$

This certainly requires $4b^2 d \in \mathbb{Z}$; again, as d is squarefree, $2b$ must be an integer, B say. Further, b itself cannot be in $\mathbb{Z}$; otherwise

$$\frac{A^2}{4} - b^2 d \notin \mathbb{Z}.$$

Thus B is an odd integer. Then

$$A^2 - B^2 d \equiv 0 \,(\mathrm{mod}\, 4)$$

with A and B odd integers. But the squares of odd numbers are all 1 (mod 4). Thus

$$1 - d \equiv 0 \,(\mathrm{mod}\, 4).$$

If $d \equiv 1 \,(\mathrm{mod}\, 4)$, the second case can arise, and the integers are

$$\{a + b\sqrt{d} \mid \text{either } a, b \in \mathbb{Z}, \text{ or both } a \text{ and } b \text{ are halves of odd integers}\},$$

a set which is easily seen to be the same as that of the statement. On the other hand, if $d \not\equiv 1 \,(\mathrm{mod}\, 4)$, then the only integers are $\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ as claimed. □

In particular, if $d = -1$, so that $d \equiv 3 (\mathrm{mod}\, 4)$, this result shows that the ring of integers of $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$.

However, as already remarked, the ring of integers of $\mathbb{Q}(\sqrt{d})$ is not always just $\mathbb{Z}[\sqrt{d}]$. Although every element in $\mathbb{Z}[\sqrt{d}]$ is an algebraic integer, there are sometimes additional integers; if $d = -3$, for example, then $(-1 + \sqrt{-3})/2$ is an integer, as it is a root of $X^2 + X + 1$. Similarly, if $d = 5$, then $(1 + \sqrt{5})/2$ is an integer, as it is a root of $X^2 - X - 1$.

Exercise 2.15 Show that the square of the modulus of the complex number $a + b(\frac{1+\sqrt{-3}}{2}) \in \mathbb{Q}(\sqrt{-3})$ is $a^2 + ab + b^2$.

[*Hint: As usual, write down the real and imaginary parts, and consider the sum of their squares.*]

Find the elements in the ring of integers of $\mathbb{Q}(\sqrt{-3})$ with squared modulus 19. And which elements in the ring of integers of $\mathbb{Q}(\sqrt{-2})$ have squared modulus 19?

Exercise 2.16 Use Exercise 2.11 to see that the ring of integers of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is bigger than $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$.

http://www.springer.com/978-3-319-07544-0

Algebraic Number Theory
Jarvis, F.
2014, XIII, 292 p. 3 illus., Softcover
ISBN: 978-3-319-07544-0