Chapter 3 : Number fields and number rings

After much ado we are finally in the subject. Let me recapitulate the definitions of the basic objects. The reader may wonder for a while why we had to be so formal and general in the last two chapters. The fact is that more often than not the proofs for the special cases of interest in this course are no easier than those for the general cases. That is to say that we had to prove essentially the same results in essentially the same way with A (a general ring) replaced by $\mathfrak{O}_K$ (a number ring). We lost practically nothing by being general. On the other hand, that general treatment should have by now given the reader the confidence regarding the applicability of these tools in other branches of mathematics.

The extension $\mathbb{Q} \subseteq \mathbb{C}$ is not algebraic (nor is the extension $\mathbb{Q} \subseteq \mathbb{R}$), since we all know about the (provable) existence of real numbers like e and π which do not satisfy any polynomial with rational (or integer) coefficients. Let $\bar{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Clearly $\bar{\mathbb{Q}} \subsetneqq \mathbb{C}$, since $\mathbb{C}$ is already an algebraically closed field. A complex number α is called an algebraic number, if $\alpha \in \bar{\mathbb{Q}}$. The (unique) non-zero monic polynomial $\mathrm{minpoly}_\alpha(X) = \mathrm{minpoly}_{\alpha,\mathbb{Q}}(X) \in \mathbb{Q}[X]$ satisfied by an algebraic number α is called the minimal polynomial of α (over $\mathbb{Q}$). Of special interest to us are the elements $\alpha \in \bar{\mathbb{Q}}$ for which $\mathrm{minpoly}_\alpha(X)$ are in $\mathbb{Z}[X]$. Such elements are called algebraic integers. The set of algebraic integers is denoted by $\mathbb{A}$ and is a ring known as the ring of algebraic integers.

A finite (and hence algebraic) extension K of $\mathbb{Q}$ is called a number field. The extension degree $d := [K : \mathbb{Q}]$ is called the degree of the number field K. By Corollary 1.68 K is a simple extension of $\mathbb{Q}$, i.e., there exists an element $\alpha \in K$ such that $\deg(\mathrm{minpoly}_\alpha(X)) = d$ and $K = \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha] \cong \mathbb{Q}[X]/\langle \mathrm{minpoly}_\alpha(X) \rangle$. The field K is a $\mathbb{Q}$-vector space of dimension d with basis $1, \alpha, \ldots, \alpha^{d-1}$. There exists a non-zero integer a such that $\beta := a\alpha \in K$ is an algebraic integer and we continue to have $K = \mathbb{Q}(\beta)$. Thus without loss of generality we may take α to be an algebraic integer. In this case the $\mathbb{Q}$-basis $1, \alpha, \ldots, \alpha^{d-1}$ of K consists only of algebraic integers.

For a number field K the set $\mathfrak{O}_K := K \cap \mathbb{A}$ of all algebraic integers contained in K is a ring (an integral domain) called the ring of integers of K. The rings $\mathfrak{O}_K$ for number fields K are the central objects of study in this course (if not in algebraic number theory in general). Unfortunately the rings $\mathfrak{O}_K$ are less well-behaved than the ring $\mathbb{Z} = \mathfrak{O}_\mathbb{Q}$ of rational integers. For example, unique factorization of (non-zero) elements into primes need not hold in $\mathfrak{O}_K$. But we will see (in Chapter 4) that unique factorization holds in $\mathfrak{O}_K$ at the level of ideals.

$\mathfrak{O}_K$ is a $\mathbb{Z}$-module. (Any Abelian group is so.) We will prove later in this section that $\mathfrak{O}_K$ is indeed a *free* $\mathbb{Z}$-module of rank $d := [K : \mathbb{Q}]$. But the unfortunate fact is that for $K = \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$ for some algebraic integer $\alpha \in K$ we do not in general have $\mathfrak{O}_K = \mathbb{Z}[\alpha]$. For example, for $K = \mathbb{Q}(\sqrt{-3})$ we have $\mathbb{Z}[\sqrt{-3}\,] \subsetneqq \mathfrak{O}_K$ (See Exercise 2.2.7), since $\frac{1+\sqrt{-3}}{2} \in K$ satisfies the monic irreducible polynomial $X^2 - X + 1 \in \mathbb{Z}[X]$ and hence is a member of $\mathfrak{O}_K$, but it clearly does not belong to $\mathbb{Z}[\sqrt{-3}\,]$. However, in this case we have $K = \mathbb{Q}(\gamma)$ and $\mathfrak{O}_K = \mathbb{Z}[\gamma]$, where $\gamma := \frac{1+\sqrt{-3}}{2}$. But there are number fields K for which $\mathfrak{O}_K$ does not at all have a $\mathbb{Z}$-basis of the form $1, \alpha, \ldots, \alpha^{d-1}$.

In this chapter we study the overall structures of the number fields K and their rings $\mathfrak{O}_K$ of integers. A number field $K \neq \mathbb{Q}$ has more than one isomorphic copies sitting inside the field $\mathbb{C}$. But how many such copies are there? I start by providing an answer to this question. Next I concentrate on the $\mathbb{Z}$-module structure of $\mathfrak{O}_K$. I will develop the notions of traces and norms and eventually prove the existence of (integral) bases of $\mathfrak{O}_K$ over $\mathbb{Z}$. Inner structures (ideals, units etc.) of number rings will be studied in the following two chapters.

3.1 Complex embeddings

Let $f(X) \in \mathbb{Q}[X]$ be an irreducible polynomial of degree $d \geqslant 1$. Then the field $K := \mathbb{Q}[X]/\langle f(X)\rangle$ is a number field of degree d and the elements of K can be represented by polynomials with rational coefficients and of degrees $< d$. Arithmetic in K is carried out as the polynomial arithmetic of $\mathbb{Q}[X]$ followed by reduction modulo the defining irreducible polynomial $f(X)$. This gives us an algebraic representation of K independent of any element of K. Now K can also be viewed as a subfield of $\mathbb{C}$ and the elements of K can be represented as complex numbers.[1] A representation $K' \subseteq \mathbb{C}$ with a field isomorphism $\sigma : K = \mathbb{Q}[X]/\langle f(X)\rangle \to K'$ is called a complex embedding of K in $\mathbb{C}$.[2] Unfortunately such a representation is not unique as the following proposition demonstrates.

3.1 Proposition A number field K of degree $d \geqslant 1$ has exactly d distinct complex embeddings.

Proof As above we take $K := \mathbb{Q}[X]/\langle f(X)\rangle$ for some irreducible polynomial $f(X) \in \mathbb{Q}[X]$ of degree d. Since $\mathbb{Q}$ is a perfect field (See Exercise 1.5.6), the d roots $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ of $f(X)$ are all distinct. For each $i = 1, \ldots, d$ the map sending $X + \langle f(X)\rangle \mapsto \alpha_i$ clearly extends to a field isomorphism $\sigma_i : \mathbb{Q}[X]/\langle f(X)\rangle \to \mathbb{Q}(\alpha_i)$. Thus we get d distinct complex embeddings $\mathbb{Q}(\alpha_i) \subseteq \mathbb{C}$ of K in $\mathbb{C}$. Now let K' be a subfield of $\mathbb{C}$, such that $\sigma : \mathbb{Q}[X]/\langle f(X)\rangle \to K'$ is a $\mathbb{Q}$-isomorphism. Let $\alpha := \sigma(X + \langle f(X)\rangle)$. Then $0 = \sigma(0) = \sigma(f(X + \langle f(X)\rangle)) = f(\sigma(X + \langle f(X)\rangle)) = f(\alpha)$. Thus α is a root of f, i.e., $\alpha = \alpha_i$ for some $i \in \{1, \ldots, d\}$. But then $K' = \mathbb{Q}(\alpha_i)$, since K' is a field containing $\mathbb{Q}$ and α and having $[K' : \mathbb{Q}] = [K : \mathbb{Q}] = d$. ◀

This proposition says that the conjugates $\alpha_1, \ldots, \alpha_d$ are *algebraically indistinguishable*. For example, $X^2 + 1$ has two roots $\pm\mathrm{i}$, where $\mathrm{i} = \sqrt{-1}$. But then what does one mean, when one talks about the 'positive' and the 'negative' square roots of -1? They are algebraically indistinguishable and if one calls one of these i, the other one becomes $-\mathrm{i}$. However, if a representation of $\mathbb{C}$ is given, we can distinguish between $+\sqrt{-5}$ and $-\sqrt{-5}$ by associating these quantities with the elements $\mathrm{i}\sqrt{5}$ and $-\mathrm{i}\sqrt{5}$ respectively, where $\sqrt{5}$ is the *positive* real square root of 5 and where $\mathrm{i} = \sqrt{-1}$ is the imaginary 'unit' available from the given representation of $\mathbb{C}$.

It is also quite customary to start with $K = \mathbb{Q}(\alpha)$ for some algebraic $\alpha \in \mathbb{C}$ and seek for the 'complex embeddings' of K in $\mathbb{C}$. One then defines $f(X) := \mathrm{minpoly}_{\alpha,\mathbb{Q}}(X) \in \mathbb{Q}[X]$ and proceeds as in the proof of Proposition 3.1 but now defining the map $\sigma_i : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha_i)$ as the unique field isomorphism that fixes $\mathbb{Q}$ and takes $\alpha \mapsto \alpha_i$. If we take $\alpha = \alpha_1$, then σ_1 is the identity map, whereas $\sigma_2, \ldots, \sigma_d$ are non-identity field isomorphisms.

The moral of this story is that whether one wants to view the number field K as $\mathbb{Q}[X]/\langle f(X)\rangle$ or as $\mathbb{Q}(\alpha_i)$ for any $i \in \{1, \ldots, d\}$ is one's personal choice. In any case one will be dealing with the same mathematical object and as long as representation issues are not brought into the scene, all these definitions of a number field are absolutely equivalent.

Finally note that the embeddings $\mathbb{Q}(\alpha_i)$ need not be all distinct as sets. For example, the two embeddings $\mathbb{Q}(\mathrm{i})$ and $\mathbb{Q}(-\mathrm{i})$ of $\mathbb{Q}[X]/\langle X^2 + 1\rangle$ are identical as sets. But the maps $x \mapsto \mathrm{i}$ and $x \mapsto -\mathrm{i}$ are distinct (where $x := X + \langle X^2 + 1\rangle$). Thus while specifying a complex embedding of a number field K it is necessary to mention not only the subfield K' of $\mathbb{C}$ isomorphic to K, but also the explicit field isomorphism $K \to K'$.

3.2 Definition Let K be a number field of degree d defined by an irreducible polynomial $f(X) \in \mathbb{Q}[X]$ or by any root of $f(X)$. Let r_1 be the number of real roots and $2r_2$ the number of non-real roots of f. (Note that the non-real roots of a real polynomial occur in (complex) conjugates.) By the fundamental theorem of

[1] A complex number $z := a + \mathrm{i}b \in \mathbb{C}$ has a representation by a pair (a, b) of real numbers. Here $\mathrm{i} := \sqrt{-1}$ plays the rôle of $X + \langle X^2 + 1\rangle$ in $\mathbb{R}[X]/\langle X^2 + 1\rangle$. Finally every real number has a decimal (or binary or hexadecimal etc.) representation.

[2] The field $\mathbb{Q}$ is canonically embedded in K. It is evident that the embedding $\sigma : K \to K'$ fixes $\mathbb{Q}$ element-wise.

algebra we have $d = r_1 + 2r_2$. For any real root α of f the complex embedding $\mathbb{Q}(\alpha)$ of K is completely contained in $\mathbb{R}$ and hence is often called a *real embedding* of K. On the other hand, for a non-real root β of f the complex embedding $\mathbb{Q}(\beta)$ of K is termed a *non-real* or a *properly complex embedding* of K. The pair (r_1, r_2) is called the *signature* of the number field K. It is clear that K has r_1 real embeddings and $2r_2$ properly complex embeddings. If $r_2 = 0$, i.e., if all of the embeddings of K are real, one calls K a *totally real* number field. On the other hand, if $r_1 = 0$, i.e., if all the embeddings of K are properly complex, then K is called a *totally complex* number field.

3.3 Example (1) The number field $\mathbb{Q}[X]/\langle X^2 - 2\rangle$ is totally real and has the signature $(2, 0)$. (The roots of $X^2 - 2$ are $\pm\sqrt{2}$.)

(2) The number field $\mathbb{Q}[X]/\langle X^2 + 2\rangle$ is totally complex and has the signature $(0, 1)$. (The roots of $X^2 + 2$ are $\pm\mathrm{i}\sqrt{2}$.)

(3) The number field $K := \mathbb{Q}[X]/\langle X^3 - 2\rangle$ is neither totally real nor totally complex. The roots of $X^3 - 2$ are $\sqrt[3]{2}$ and $\sqrt[3]{2}\left(\frac{-1\pm\sqrt{-3}}{2}\right)$. The signature of K is $(1, 1)$, i.e., K has one real embedding and two properly complex embeddings.

We now investigate how complex embeddings behave for extensions of number fields.

3.4 Proposition Let $K \subseteq L$ be an extension of number fields, $d := [K : \mathbb{Q}]$ and $n := [L : \mathbb{Q}]$. Then every complex embedding σ of K extends to exactly n/d complex embeddings τ of L satisfying $\tau|_K = \sigma$.

Proof Let $r := [L : K] = n/d$. For $r = 1$ the proposition is obvious. So consider the case that $r > 1$. The extension $K \subseteq L$ is simple (Corollary 1.68). Choose some $\alpha \in L$ with $L = K(\alpha)$, let $f(X) := \operatorname{minpoly}_{\alpha,K}(X) = \sum_{j=0}^{r} a_j X^j \in K[X]$ and define $g(X) := \sigma(f) := \sum_{j=0}^{r} \sigma(a_j) X^j \in \sigma(K)[X]$. Since f is irreducible over K, g is also irreducible over $\sigma(K)$ and hence has exactly r distinct (simple) roots $\beta_1, \ldots, \beta_r \in \bar{\mathbb{Q}}$. For each $i = 1, \ldots, r$ the map $\tau_i : K(\alpha) \to (\sigma(K))(\beta_i)$ taking $b_0 + b_1\alpha + \cdots + b_{r-1}\alpha^{r-1} \mapsto \sigma(b_0) + \sigma(b_1)\beta_i + \cdots + \sigma(b_{r-1})\beta_i^{r-1}$ is a unique embedding of $L = K(\alpha)$ in $\mathbb{C}$ whose restriction to K is σ and which maps $\alpha \mapsto \beta_i$.

Now let τ be any complex embedding of L with $\tau|_K = \sigma$. We have $g(\tau(\alpha)) = \sum_{j=0}^{r} \sigma(a_j)\tau(\alpha)^j = \sum_{j=0}^{r} \tau(a_j)\tau(\alpha)^j = \tau(\sum_{j=0}^{r} a_j \alpha^j) = \tau(0) = 0$, i.e., $\tau(\alpha) = \beta_i$ for some $i \in \{1, \ldots, r\}$. It then follows that $\tau = \tau_i$. ◀

We will now concentrate on a special class of number fields. Let $n \in \mathbb{N}$. A complex number α is called an *n-th root of unity*, if $\alpha^n = 1$, i.e., if α is a root of the (monic) polynomial $X^n - 1$. It immediately follows that the n-th roots of unity are algebraic integers. One can easily check that the set

$$\mu_n := \{\alpha \in \mathbb{C} \mid \alpha \text{ is an } n\text{-th root of unity}\}$$

is a subgroup of the multiplicative group $\mathbb{C}^*$. In fact, the elements of μ_n are ω_n^i, where $\omega_n := e^{\mathrm{i}2\pi/n}$ and $i = 0, 1, \ldots, n-1$. In particular, μ_n is cyclic (of order n) and has exactly $\phi(n)$ generators ω_n^i, $0 \leqslant i \leqslant n-1$, $\gcd(i, n) = 1$. Any generator of μ_n is called a *primitive n-th root of unity*. It is easy to verify that $\omega \in \mathbb{C}$ is a primitive n-th root of unity, if and only if ω is an n-th root of unity and is not an m-th root of unity for any $m \in \{1, \ldots, n-1\}$.

The (monic) polynomial

$$\Phi_n(X) := \prod_{\omega} (X - \omega) \in \mathbb{C}[X],$$

where the product runs over all primitive n-th roots of unity, is called the n-th cyclotomic polynomial. Clearly $\deg \Phi_n(X) = \phi(n)$. This definition does not make it clear that $\Phi_n(X)$ is actually a polynomial in $\mathbb{Z}[X]$. This (and something more) are what we will prove next. The most non-trivial part in this proof is establishing the following lemma.

3.5 Lemma Two primitive n-th roots ω and ω' of unity have the same minimal polynomial over $\mathbb{Q}$.

Proof We have $\omega' = \omega^i$ for some i coprime to n. If $i = 1$, we are done. Next let $i = p$ be a prime. Then $p \not| n$. Let $f(X) := \operatorname{minpoly}_\omega(X)$. Since ω is a root of $X^n - 1$, it follows that $X^n - 1 = f(X)g(X)$ for some $g(X) \in \mathbb{Q}[X]$. Since ω is an algebraic integer, $f(X)$ is in $\mathbb{Z}[X]$ and is also monic. Therefore, $g(X) \in \mathbb{Z}[X]$ and is again monic. We will now show that $f(\omega') = 0$. Assume not. Since $(w')^n - 1 = 0$, we must have $g(\omega') = g(\omega^p) = 0$, i.e., ω is a root of $g(X^p)$. Since $f(X)$ is the minimal polynomial of ω, this implies that $f(X) \mid g(X^p)$, i.e., $g(X^p) = f(X)h(X)$ for some $h(X) \in \mathbb{Q}[X]$. Again it is easy to see that $h(X) \in \mathbb{Z}[X]$.

Now we reduce modulo p. Consider the canonical surjection $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ with the image of $r(X)$ denoted as $\bar{r}(X)$. Thus $\bar{g}(X^p) = \bar{f}(X)\bar{h}(X)$. But by the binomial theorem $\bar{g}(X^p) = \bar{g}(X)^p$, i.e, $\bar{g}(X)^p = \bar{f}(X)\bar{h}(X)$, i.e., any irreducible factor of $\bar{f}$ divides $\bar{g}(X)^p$ and hence $\bar{g}(X)$, i.e., $\bar{f}$ and $\bar{g}$ have common root(s) in $\bar{\mathbb{F}}_p$, i.e., $\overline{X^n - 1} = X^n - \bar{1} = \bar{f}(X)\bar{g}(X)$ has multiple roots. Now since $p \not| n$, the (formal) derivative of $X^n - \bar{1}$ is nonzero in $\mathbb{F}_p[X]$ and hence is coprime to $X^n - \bar{1}$, i.e., $X^n - \bar{1}$ does not contain multiple roots, a contradiction.

Thus we must have $f(\omega') = f(\omega^i) = 0$ in the case when $i = p$ is a prime. Since f is irreducible over $\mathbb{Q}$, it follows that $\operatorname{minpoly}_{\omega'}(X) = f(X)$ in this case.

Finally consider the general case $i = p_1 \cdots p_s$, where the primes p_i (not necessarily all distinct) are all coprime to n. By repeated uses of the special case discussed above we then have $\operatorname{minpoly}_\omega(X) = \operatorname{minpoly}_{\omega^{p_1}}(X) = \operatorname{minpoly}_{\omega^{p_1 p_2}}(X) = \cdots = \operatorname{minpoly}_{\omega^{p_1 \cdots p_s}}(X) = \operatorname{minpoly}_{\omega'}(X)$. ◀

Now we are in a position to prove the promised results about $\Phi_n(X)$.

3.6 Proposition Let $n \in \mathbb{N}$. Then $\Phi_n(X)$ is the minimal polynomial of every primitive n-th root of unity. In particular, $\Phi_n(X) \in \mathbb{Z}[X]$ and is irreducible in $\mathbb{Z}[X]$ (or in $\mathbb{Q}[X]$).

Proof Let ω be a primitive n-th root of unity, $f(X) := \operatorname{minpoly}_\omega(X)$ and $K := \mathbb{Q}(\omega)$. Lemma 3.5 asserts that every primitive n-th root of unity is a conjugate of ω, i.e., $f(X) = \Phi_n(X)g(X)$ for some $g(X) \in \mathbb{C}[X]$. In particular, $\deg f \geqslant \deg \Phi_n = \phi(n)$.

Conversely if $K \xrightarrow{\sigma} K' \subseteq \mathbb{C}$ is a complex embedding of K and if $\sigma(\omega) = \omega'$, then $1 = \sigma(1) = \sigma(\omega^n) = (\omega')^n$, i.e., ω' is also an n-th root of unity. If ω' is an m-th root of unity for some $m < n$, we have $\sigma(1) = \sigma(\omega^m) = 1$, i.e., σ is not injective. Thus ω' must also be a *primitive* n-th root of unity, i.e., K has $\leqslant \phi(n)$ complex embeddings, i.e., $\deg f \leqslant \phi(n) = \deg \Phi_n$.

It follows that $\deg f = \deg \Phi_n$, i.e., $f(X) = \Phi_n(X)$. The proposition is now obvious. ◀

3.7 Definition Let $n \in \mathbb{N}$. The number field $K := \mathbb{Q}[X]/\langle \Phi_n(X) \rangle \cong \mathbb{Q}(\omega)$ for any primitive n-th root ω of unity is called a cyclotomic extension of $\mathbb{Q}$. We have $[K : \mathbb{Q}] = \phi(n)$.

Cyclotomic fields constitute a rich set of examples of number fields. We will study the properties of these fields and their rings of integers throughout the course as case studies. Another interesting set of examples is provided by the quadratic fields $\mathbb{Q}(\sqrt{D})$, where D is a square-free integer $\neq 0, 1$ (Exercise 2.2.7).

Exercises for Section 3.1

1. Find the minimal polynomial and the conjugates of α and also the degree of $\mathbb{Q}(\alpha)$, where:

(a) $\alpha = \sqrt{3+\sqrt{5}}\,.$

(b) $\alpha = \sqrt{(3+\sqrt{5})/2}\,.$

(c) $\alpha = 1 + 2^{1/3} + 2^{2/3}$.

2. Let $K := \mathbb{Q}(\alpha)$, where $\alpha = \sqrt[3]{2}$.

(a) Find the complex embeddings $K \overset{\sigma_i}{\to} K_i \subseteq \mathbb{C}$, $i = 1, 2, 3$, of K.

(b) Show that K_1, K_2 and K_3 are pairwise distinct as sets.

(c) Compute $\sigma_1(\alpha) + \sigma_2(\alpha) + \sigma_3(\alpha)$ and $\sigma_1(\alpha)\sigma_2(\alpha)\sigma_3(\alpha)$.

3. Let α be an algebraic number with $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ odd. Show that $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2)$.

4. A root of unity is an n-th root of unity for some $n \in \mathbb{N}$. Show that all the roots of unity constitute a multiplicative subgroup G of $\mathbb{C}^*$. Deduce that G is infinite and not cyclic. (**Hint:** An infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$.)

5. Let $n \in \mathbb{N}$ and $p \in \mathbb{P}$.

(a) Show that $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$. (**Hint:** Look at the roots of the polynomials on the two sides.)

(b) Using Part (a) conclude that $\Phi_n(X) \in \mathbb{Z}[X]$. (**Hint:** Use induction on n.) Recall that this fact was proved in a different manner in Proposition 3.6.

(c) Use Möbius inversion formula to deduce that $\Phi_n(X) = \prod_{d \mid n}(X^d - 1)^{\mu(n/d)}$, where μ is the Möbius function. This gives yet another way to conclude that $\Phi_n(X) \in \mathbb{Z}[X]$.

(d) If $n \neq 1$ is odd, show that $\Phi_{2n}(X) = \Phi_n(-X)$. (**Hint:** If $\operatorname{ord}\omega = n$, then $\operatorname{ord}(-\omega) = 2n$.)

(e) Show that $\Phi_{p^n}(X) = X^{p^{n-1}(p-1)} + X^{p^{n-1}(p-2)} + \cdots + X^{p^{n-1}} + 1$.

6. Let $K := \mathbb{Q}(\mathrm{i}) \cong \mathbb{Q}[X]/\langle X^2+1\rangle$. By Exercise 2.2.7 we have $\mathfrak{O}_K = \mathbb{Z}[\mathrm{i}]$, the ring of Gaussian integers.

(a) Show that $a + \mathrm{i}b$ (with $a, b \in \mathbb{Z}$) is a unit in $\mathbb{Z}[\mathrm{i}]$, if and only if $a^2 + b^2 = 1$.

*** (b)** Show that the prime elements of $\mathbb{Z}[\mathrm{i}]$ are the associates to:

p, where $p \in \mathbb{P}$ is a rational prime congruent to 3 modulo 4,

$a + \mathrm{i}b$, where $a, b \in \mathbb{N}$ and $a^2 + b^2$ is 2 or a rational prime congruent to 1 modulo 4.

7. Show that:

(a) For a rational prime p the equation $x^2 + y^2 = p$ has a solution $(x, y) \in \mathbb{Z}^2$, if and only if $p = 2$ or $p \equiv 1 \pmod 4$.

(b) For $n \in \mathbb{N}$ the equation $x^2 + y^2 = n$ has a solution $(x, y) \in \mathbb{Z}^2$, if and only if $\mathrm{v}_p(n) \equiv 0 \pmod 2$ for all rational primes $p \in \mathbb{P}$ with $p \equiv 3 \pmod 4$.

*** 8.** Let ω be a primitive cube root of unity. What is the degree of $\mathbb{Q}(\omega)$? Show that $\mathbb{Q}(\omega)$ is an ED. (**Hint:** Consider the function $\nu(a + b\omega) := a^2 - ab + b^2$.)

9. Let p be an odd rational prime, ω a primitive p-th root of unity and $K := \mathbb{Q}(\omega + \omega^{-1})$. Show that K is a number field of degree $(p-1)/2$.

10. Let α and β be algebraic numbers with $m := [\mathbb{Q}(\alpha) : \mathbb{Q}] > 1$ and $n := [\mathbb{Q}(\beta) : \mathbb{Q}] > 1$. Let $K := \mathbb{Q}(\alpha, \beta)$.

(a) Show that $[K : \mathbb{Q}] \leqslant mn$.

(b) Give an example where $[K : \mathbb{Q}] < mn$. (Avoid the trivial case: $\alpha \in \mathbb{Q}(\beta)$ or $\beta \in \mathbb{Q}(\alpha)$.)

(c) Prove that if $\gcd(m, n) = 1$, then $[K : \mathbb{Q}] = mn$.

*** (d)** Prove or disprove: If $\gcd(m, n) = 1$, then $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = mn$.

**** (e)** Prove or disprove: If $\gcd(m, n) = 1$, then $[\mathbb{Q}(\alpha + \beta) : \mathbb{Q}] = mn$.

3.2 Traces and norms

Let me now introduce some important concepts from linear algebra, that will be useful in the next section for proving the existence of integral bases of number rings.

3.8 Definition Let $F \subseteq K$ be an extension of fields with $d := [K : F] < \infty$. For any $\alpha \in K$ the multiplication map $\lambda_\alpha : K \to K$ taking $x \mapsto \alpha x$ is an F-linear transformation. Let $T_{\mathcal{B}}$ denote the matrix of the transformation λ_α with respect to some F-basis $\mathcal{B}$ of K. We know that the trace (i.e., the sum of the elements in the principal diagonal) and the determinant of $T_{\mathcal{B}}$ are independent of the basis $\mathcal{B}$ and is an invariant of the transformation λ_α. This allows us to define the trace $\mathrm{Tr}_{K|F}(\alpha)$ and the norm $\mathrm{N}_{K|F}(\alpha)$ of α as

$$\mathrm{Tr}_{K|F}(\alpha) := \mathrm{Tr}(T_{\mathcal{B}}) \qquad \text{and} \qquad \mathrm{N}_{K|F}(\alpha) := \det T_{\mathcal{B}}\,.$$

If F is understood from the context, we simply write $\mathrm{Tr}_K(\alpha)$ and $\mathrm{N}_K(\alpha)$. If K is also clear in the context, we may even omit the K. $\mathrm{Tr}(\alpha)$ *and* $\mathrm{N}(\alpha)$ *are elements of* F, since $T_{\mathcal{B}}$ is a matrix with entries from F.

In a similar manner the characteristic polynomial of α is defined as

$$\mathrm{charpoly}_{\alpha,K|F}(X) := \mathrm{charpoly}_{\lambda_\alpha}(X) = \mathrm{charpoly}_{T_{\mathcal{B}}}(X) = \det(X\mathrm{I}_d - T_{\mathcal{B}}) \in F[X],$$

where I_d is the $d \times d$ identity matrix (over F). Once again it follows from linear algebra that this characteristic polynomial is independent of the basis $\mathcal{B}$. Again we drop the suffix $K|F$, if there is no scope of confusion.

The three items introduced in the last definition are related by the following important formula:

$$\mathrm{charpoly}_\alpha(X) = X^d - \mathrm{Tr}(\alpha)X^{d-1} + \cdots + (-1)^d\,\mathrm{N}(\alpha)\,. \tag{3.1}$$

Now we specialize to the case $F := \mathbb{Q}$ and $K :=$ a number field of degree d. In this case we have equivalent characterizations of the trace and norm functions. Before discussing about these characterizations let us prove some auxiliary results.

3.9 Proposition Let K be a number field of degree d and $\alpha \in K$. Then the characteristic polynomial of α over $\mathbb{Q}$ satisfies $\mathrm{charpoly}_{\alpha,K|\mathbb{Q}}(X) = (\mathrm{minpoly}_{\alpha,\mathbb{Q}}(X))^{d/r}$, where $r = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Proof First consider the case $r = d$ (i.e., $K = \mathbb{Q}(\alpha)$). By the Cayley-Hamilton theorem $T_{\mathcal{B}}$ and λ_α satisfy $\mathrm{charpoly}_{\alpha,K|\mathbb{Q}}(X)$. Thus $(\mathrm{charpoly}_{\alpha,K|\mathbb{Q}}(\lambda_\alpha))(1) = 0$, i.e., $\mathrm{charpoly}_{\alpha,K|\mathbb{Q}}(\alpha) = 0$, i.e., $\mathrm{minpoly}_{\alpha,\mathbb{Q}}(X)$ divides $\mathrm{charpoly}_{\alpha,K|\mathbb{Q}}(X)$. Since both these polynomials have the same degree ($= r = d$) and are monic, we have $\mathrm{charpoly}_{\alpha,K|\mathbb{Q}}(X) = \mathrm{minpoly}_{\alpha,\mathbb{Q}}(X)$ and the result follows.

Now suppose that $r < d$ and consider the tower of field extensions $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K$ of extension degrees r and $s := d/r$ respectively. By the special case proved above we have $\mathrm{charpoly}_{\alpha,\mathbb{Q}(\alpha)|\mathbb{Q}}(X) = \mathrm{minpoly}_{\alpha,\mathbb{Q}}(X)$. So it is sufficient to prove that $\mathrm{charpoly}_{\alpha,K|\mathbb{Q}}(X) = (\mathrm{charpoly}_{\alpha,\mathbb{Q}(\alpha)|\mathbb{Q}}(X))^s$. Let $\mathcal{B}_1 := (\beta_1, \ldots, \beta_r)$ be a $\mathbb{Q}$-basis of $\mathbb{Q}(\alpha)$ and $\mathcal{B}_2 := (\gamma_1, \ldots, \gamma_s)$ a $\mathbb{Q}(\alpha)$-basis of K. Then $\mathcal{B} := (\gamma_1\beta_1, \ldots, \gamma_1\beta_r, \ldots, \gamma_s\beta_1, \ldots, \gamma_s\beta_r)$ is a $\mathbb{Q}$-basis of K. Let us denote by T_1 the matrix of the multiplication map $\mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$, $x \mapsto \alpha x$, with respect to the ordered basis $\mathcal{B}_1$. It is now an easy check that the matrix of the multiplication map $K \to K$, $x \mapsto \alpha x$, with respect to the ordered basis $\mathcal{B}$ is

$$T := \begin{pmatrix} T_1 & 0 & \cdots & 0 \\ 0 & T_1 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & T_1 \end{pmatrix}.$$

Therefore, $\det(X\mathrm{I}_d - T) = (\det(X\mathrm{I}_r - T_1))^s$, whence the proposition follows. ◀

3.10 Corollary Let $\alpha \in \mathfrak{O}_K$. Then $\mathrm{Tr}_{K|\mathbb{Q}}(\alpha)$ and $\mathrm{N}_{K|\mathbb{Q}}(\alpha)$ are in $\mathbb{Z}$.

Proof Since α is an algebraic integer, $\mathrm{minpoly}_{\alpha,\mathbb{Q}}(X) \in \mathbb{Z}[X]$. By Proposition 3.9 we then also have $\mathrm{charpoly}_{\alpha,K|\mathbb{Q}}(X) \in \mathbb{Z}[X]$. Equation (3.1) now completes the proof. ◀

3.11 Corollary Let K be a number field of degree d, $\alpha \in K$, $r := [\mathbb{Q}(\alpha) : \mathbb{Q}]$ and $\alpha_1, \ldots, \alpha_r$ the conjugates of α (i.e., the roots of $\mathrm{minpoly}_{\alpha,\mathbb{Q}}(X)$). Then we have:

$$\mathrm{charpoly}_{\alpha,K|\mathbb{Q}}(X) = \left(\prod_{i=1}^{r}(X - \alpha_i)\right)^{d/r}, \tag{3.2}$$

$$\mathrm{Tr}_{K|\mathbb{Q}}(\alpha) = \frac{d}{r}\sum_{i=1}^{r}\alpha_i\,, \tag{3.3}$$

$$\mathrm{N}_{K|\mathbb{Q}}(\alpha) = \left(\prod_{i=1}^{r}\alpha_i\right)^{d/r}. \tag{3.4}$$

Proof Since $\mathrm{minpoly}_{\alpha,\mathbb{Q}}(X) = \prod_{i=1}^{r}(X - \alpha_i)$, Proposition 3.9 establishes (3.2), whereas (3.3) and (3.4) follow from Equations (3.1) and (3.2). ◀

Now come the desired characterizations of traces and norms (over $\mathbb{Q}$) of elements of a number field.

3.12 Proposition Let K be a number field of degree d, $\sigma_1, \ldots, \sigma_d$ the d complex embeddings of K and $\alpha \in K$. Then we have:

$$\mathrm{Tr}_{K|\mathbb{Q}}(\alpha) = \sum_{i=1}^{d}\sigma_i(\alpha), \tag{3.5}$$

$$\mathrm{N}_{K|\mathbb{Q}}(\alpha) = \prod_{i=1}^{d}\sigma_i(\alpha). \tag{3.6}$$

In particular, for $\alpha, \beta \in K$ and $c \in \mathbb{Q}$ we have:

$$\mathrm{Tr}_{K|\mathbb{Q}}(\alpha + \beta) = \mathrm{Tr}_{K|\mathbb{Q}}(\alpha) + \mathrm{Tr}_{K|\mathbb{Q}}(\beta)\,, \tag{3.7}$$

$$\mathrm{N}_{K|\mathbb{Q}}(\alpha\beta) = \mathrm{N}_{K|\mathbb{Q}}(\alpha)\,\mathrm{N}_{K|\mathbb{Q}}(\beta)\,, \tag{3.8}$$

$$\mathrm{Tr}_{K|\mathbb{Q}}(c\alpha) = c\,\mathrm{Tr}_{K|\mathbb{Q}}(\alpha)\,, \tag{3.9}$$

$$\mathrm{N}_{K|\mathbb{Q}}(c\alpha) = c^d\,\mathrm{N}_{K|\mathbb{Q}}(\alpha)\,, \tag{3.10}$$

$$\mathrm{Tr}_{K|\mathbb{Q}}(c) = cd\,, \tag{3.11}$$

$$\mathrm{N}_{K|\mathbb{Q}}(c) = c^d\,. \tag{3.12}$$

Proof Let $r := [\mathbb{Q}(\alpha) : \mathbb{Q}]$ (We have $r \mid d$.) and let $\tau_1, \ldots, \tau_r$ be the complex embeddings of $\mathbb{Q}(\alpha)$ mapping α to its conjugates $\alpha_1, \ldots, \alpha_r$ respectively. By Proposition 3.4 each τ_j extends to exactly d/r complex embeddings $\sigma_{j,l}$ of K and all complex embeddings $\sigma_1, \ldots, \sigma_d$ of K are obtained this way. Therefore, $\sum_{i=1}^{d}\sigma_i(\alpha) = \sum_{j=1}^{r}\sum_{l=1}^{d/r}\sigma_{j,l}(\alpha) = \sum_{j=1}^{r}(d/r)\alpha_j = \frac{d}{r}\sum_{j=1}^{r}\alpha_j = \mathrm{Tr}_{K|\mathbb{Q}}(\alpha)$, where the last equality follows from Equation (3.3). In an analogous way one can derive the formula (3.6) for norms. The remaining assertions in the proposition are immediate consequences of (3.5) and (3.6). ◀

One may take (3.5) and (3.6) as the definitions of the trace and the norm of an algebraic number. However, these definitions do not immediately make it clear that $\mathrm{Tr}(\alpha)$ and $\mathrm{N}(\alpha)$ are elements of $\mathbb{Q}$. Furthermore, if the extension $F \subseteq K$ is not separable[3], embeddings of K in $\bar{F}$ fail to satisfy the nice properties as in the case of number fields, whereas Definition 3.8 continues to make sense, because it does not require any embedding at all.

Exercises for Section 3.2

1. Let $\alpha := \sqrt[3]{2}$ and ω a primitive cube root of unity. Define $K := \mathbb{Q}(\alpha)$ and $L := K(\omega) = \mathbb{Q}(\alpha, \omega)$.

(a) What are the degrees $[K : \mathbb{Q}]$, $[L : \mathbb{Q}]$ and $[L : K]$?

(b) Compute $\mathrm{Tr}_{K|\mathbb{Q}}(\alpha)$ and $\mathrm{N}_{K|\mathbb{Q}}(\alpha)$.

(c) Compute $\mathrm{Tr}_{L|\mathbb{Q}}(\alpha)$ and $\mathrm{N}_{L|\mathbb{Q}}(\alpha)$.

2. Show that if $\alpha \mid \beta$ in $\mathfrak{O}_K$, then $\mathrm{N}_{K|\mathbb{Q}}(\alpha) \mid \mathrm{N}_{K|\mathbb{Q}}(\beta)$ in $\mathbb{Z}$.

3. **(a)** Let K be a number field. Show that $\alpha \in \mathfrak{O}_K$ is a unit (in $\mathfrak{O}_K$), if and only if $\mathrm{N}_{K|\mathbb{Q}}(\alpha) = \pm 1$.

(b) Let D be a square-free integer $\neq 0, 1$ and $K := \mathbb{Q}(\sqrt{D})$. If $D \equiv 2, 3 \pmod 4$, show that the (integer) solutions of the Diophantine equations $x^2 - Dy^2 = \pm 1$ are in one-to-one correspondence with the units of $\mathfrak{O}_K$. Derive a similar result for the case $D \equiv 1 \pmod 4$.

(c) Let $D < 0$. Show that the only units of $\mathfrak{O}_K$ are ± 1 except in the cases $D = -1$ and $D = -3$. What are the units of $\mathfrak{O}_K$ for these two special values of D?

4. Prove that $\mathbb{Q}(\mathrm{i})$ does not contain an element of norm 3.

5. Let $p \in \mathbb{P}$, ω a primitive p-th root of unity and $K := \mathbb{Q}(\omega)$. Then $[K : \mathbb{Q}] = \deg \Phi_p = \phi(p) = p - 1$. Show that:

(a) $\mathrm{Tr}_{K|\mathbb{Q}}(\omega) = -1$ and $\mathrm{Tr}_{K|\mathbb{Q}}(1 - \omega) = p$.

(b) For any $\alpha \in \mathfrak{O}_K$ we have $p \mid \mathrm{Tr}_{K|\mathbb{Q}}(\alpha(1 - \omega))$. (Note that $\alpha(1 - \omega) \in \mathfrak{O}_K$ and hence $\mathrm{Tr}_{K|\mathbb{Q}}(\alpha(1 - \omega)) \in \mathbb{Z}$.)

6. Let $\mathbb{Q} \subseteq K \subseteq L$ be extensions of number fields and $\alpha \in L$. Further let $d := [L : K]$ and $\sigma_1, \ldots, \sigma_d$ be all the complex embeddings of L that fix K (i.e., all the complex embeddings of L that extend the identity embedding of K). Prove the generalized formulas for trace and norm:

$$\mathrm{Tr}_{L|K}(\alpha) = \sum_{i=1}^{d} \sigma_i(\alpha)\,, \tag{3.13}$$

$$\mathrm{N}_{L|K}(\alpha) = \prod_{i=1}^{d} \sigma_i(\alpha)\,. \tag{3.14}$$

(**Hint:** Imitate the proof for the special case $K = \mathbb{Q}$ as given in the text.)

7. Let $\mathbb{Q} \subseteq F \subseteq K \subseteq L$ be extensions of number fields and $\alpha \in L$. Prove the following transitivity properties of trace and norm:

$$\mathrm{Tr}_{L|F}(\alpha) = \mathrm{Tr}_{K|F}(\mathrm{Tr}_{L|K}(\alpha))\,, \tag{3.15}$$

$$\mathrm{N}_{L|F}(\alpha) = \mathrm{N}_{K|F}(\mathrm{N}_{L|K}(\alpha))\,. \tag{3.16}$$

[3] Let F be a field and K an algebraic extension of F. An *irreducible* polynomial $f(X) \in F[X]$ is called separable over F, if f does not admit a multiple root in any extension of F. An element $\alpha \in K$ is called separable over F, if $\mathrm{minpoly}_{\alpha,F}(X)$ is separable over F. Finally the (algebraic) extension $F \subseteq K$ is called separable, if every $\alpha \in K$ is separable over F. By Exercise 1.5.6 every algebraic extension of a perfect field (e.g. a field of characteristic zero or a finite field) is separable.

(**Hint:** Let $r := [K : F]$, $s := [L : K]$, $\sigma_1, \ldots, \sigma_r$ the embeddings of K in $\mathbb{C}$ that fix F and $\tau_1, \ldots, \tau_s$ the embeddings of L in $\mathbb{C}$ that fix K. For each $j \in \{1, \ldots, s\}$ consider $\gamma_j \in \mathbb{C}$ with $\tau_j(L) = F(\gamma_j)$. Define $E := K(\gamma_1, \ldots, \gamma_s)$. For each $i \in \{1, \ldots, r\}$ let ρ_i be an embedding of E in $\mathbb{C}$ that extends σ_i. First show that $\rho_i \circ \tau_j$ for $i = 1, \ldots, r$ and $j = 1, \ldots, s$ give all the embeddings of L in $\mathbb{C}$ that fix F. Then use the formulas (3.13) and (3.14).)

8. Let K be a number field. We say that K is norm-Euclidean, if for every $\alpha, \beta \in \mathfrak{O}_K$, $\beta \neq 0$, there exist $q, r \in \mathfrak{O}_K$ such that $\alpha = q\beta + r$ and $|\mathrm{N}(r)| < |\mathrm{N}(\beta)|$.

(a) Conclude that if K is norm-Euclidean, then $\mathfrak{O}_K$ is an ED with the Euclidean degree function $\nu(\alpha) := |\mathrm{N}(\alpha)|$. (**Remark:** The converse of this is not true. For example, it is known that $K := \mathbb{Q}(\sqrt{69})$ is not norm-Euclidean, but $\mathfrak{O}_K$ is an ED.)

(b) Prove the following equivalent characterization of a norm-Euclidean number field: K is norm-Euclidean, if and only if for every $\alpha \in K$ there exists $\beta \in \mathfrak{O}_K$ such that $|\mathrm{N}(\alpha - \beta)| < 1$.

(c) Show that the following number fields are norm-Euclidean: $\mathbb{Q}$, $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$.

(d) Show that $\mathbb{Q}(\sqrt{-6})$ is not norm-Euclidean. (**Hint:** Take $\alpha := \frac{1+\sqrt{-6}}{2}$ in Part (b).)

3.3 Discriminants and integral bases

Recall that for the quadratic polynomial $f(X) := X^2 + bX + c$ we call the quantity $b^2 - 4c$ the discriminant $\Delta(f)$ of f. The sign of $\Delta(f)$ gives us information about the roots of f. We generalize this concept now and define the discriminant of any non-constant irreducible polynomial in $\mathbb{Q}[X]$ or even of a set of elements in a number field. Throughout this section we denote by K a number field of degree d and by $\mathfrak{O}_K$ the ring of integers of K. Our aim in this section is to the prove the fact that $\mathfrak{O}_K$ is a free $\mathbb{Z}$-module of rank d. The language of discriminants is one usual weapon to win this battle. The trace and norm of an element $\alpha \in K$ over $\mathbb{Q}$ will be denoted simply as $\mathrm{Tr}(\alpha)$ and $\mathrm{N}(\alpha)$ without the subscript $K|\mathbb{Q}$.

3.13 Definition Let $\beta_1, \ldots, \beta_d \in K$. We call the determinant of the matrix $(\mathrm{Tr}(\beta_i\beta_j))_{1\leqslant i,j\leqslant d}$ (i.e., of the matrix whose ij-th entry is equal to $\mathrm{Tr}(\beta_i\beta_j)$) the discriminant of $\beta_1, \ldots, \beta_d$ and denote this as $\Delta(\beta_1, \ldots, \beta_d) := \det(\mathrm{Tr}(\beta_i\beta_j))$. Since $\mathrm{Tr}(\beta_i\beta_j)$ are all elements of $\mathbb{Q}$, it follows that $\Delta(\beta_1, \ldots, \beta_d) \in \mathbb{Q}$. Moreover, if $\beta_1, \ldots, \beta_d$ are all algebraic integers, then $\Delta(\beta_1, \ldots, \beta_d) \in \mathbb{Z}$.

Discriminants can be defined in an alternative way by using the complex embeddings $\sigma_1, \ldots, \sigma_d$ of K.

3.14 Proposition $\Delta(\beta_1, \ldots, \beta_d) = (\det(\sigma_j(\beta_i)))^2$.

Proof Consider the matrices $D := (\mathrm{Tr}(\beta_i\beta_j))$ and $E := (\sigma_j(\beta_i))$. By definition $\Delta(\beta_1, \ldots, \beta_d) = \det D$. We will show that $D = EE^{\mathrm{t}}$, which implies that $\det D = (\det E)^2$ and thereby proves the proposition. The ij-th entry of EE^{t} is $\sum_{k=1}^{d} \sigma_k(\beta_i)\sigma_k(\beta_j) = \sum_{k=1}^{d} \sigma_k(\beta_i\beta_j) = \mathrm{Tr}(\beta_i\beta_j)$, where the last equality follows from Equation (3.5). ◀

Let $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$ and let $f(X) := \mathrm{minpoly}_{\alpha,\mathbb{Q}}(X)$. We define the discriminant of f as

$$\Delta(f) := \Delta(1, \alpha, \alpha^2, \ldots, \alpha^{d-1}) \,. \tag{3.17}$$

I have to show that the quantity $\Delta(f)$ is well-defined, i.e., independent of the choice of the root α of $f(X)$. Let $\alpha = \alpha_1, \alpha_2, \ldots . \alpha_d$ be all the roots of $f(X)$ and let the complex embedding σ_j of K map α to α_j. By Proposition 3.14 we have $\Delta(f) = (\det E)^2$, where $E = (\sigma_j(\alpha^{i-1})) = (\alpha_j^{i-1})$. By Exercise 3.3.1 we then get $\Delta(f) = (-1)^{d(d-1)/2} \prod_{\substack{i,j=1 \\ i\neq j}}^{d} (\alpha_j - \alpha_i)$, which implies that $\Delta(f)$ is independent of the permutations of the conjugates $\alpha_1, \ldots, \alpha_d$ of α. Notice that since $\alpha_1, \ldots, \alpha_d$ are all distinct, $\Delta(f) \neq 0$.

Now let me give a simpler description of $\Delta(f)$. First I write $f(X) = \prod_{i=1}^{d}(X - \alpha_i)$. Taking formal derivative gives $f'(X) = \sum_{j=1}^{d} \prod_{\substack{i=1 \\ i \neq j}}^{d} (X - \alpha_i)$, i.e., $f'(\alpha_j) = \prod_{\substack{i=1 \\ i \neq j}}^{d} (\alpha_j - \alpha_i)$. Therefore, $\Delta(f) = (-1)^{d(d-1)/2} \prod_{j=1}^{d} f'(\alpha_j) = (-1)^{d(d-1)/2} \prod_{j=1}^{d} \sigma_j(f'(\alpha))$, i.e.,

$$\Delta(f) = \Delta(1, \alpha, \alpha^2, \ldots, \alpha^{d-1}) = (-1)^{d(d-1)/2}\, \mathrm{N}(f'(\alpha)) \tag{3.18}$$

I will now show how the discriminant $\Delta(\beta_1, \ldots, \beta_d)$ discriminates between the cases that $\beta_1, \ldots, \beta_d$ form a $\mathbb{Q}$-basis of K and that they do not. I start with the following lemma.

3.15 Lemma Let $\beta_1, \ldots, \beta_d, \gamma_1, \ldots, \gamma_d \in K$ satisfy $\gamma_i = \sum_{k=1}^{d} t_{ik}\beta_k$ for $i = 1, \ldots, d$ and for $t_{ik} \in \mathbb{Q}$. Then $\Delta(\gamma_1, \ldots, \gamma_d) = (\det T)^2 \Delta(\beta_1, \ldots, \beta_d)$, where $T = (t_{ij})$.

Proof Let $E_1 := (\sigma_j(\beta_i))$ and $E_2 := (\sigma_j(\gamma_i))$. Now $\sigma_j(\gamma_i) = \sigma_j(\sum_{k=1}^{d} t_{ik}\beta_k) = \sum_{k=1}^{d} t_{ik}\sigma_j(\beta_k)$ is the ij-th entry of the matrix TE_1, i.e., $E_2 = TE_1$. Hence $\Delta(\gamma_1, \ldots, \gamma_d) = (\det E_2)^2 = (\det T)^2(\det E_1)^2 = (\det T)^2\Delta(\beta_1, \ldots, \beta_d)$. ◀

3.16 Corollary Let $\mathcal{B}_1 := (\beta_1, \ldots, \beta_d)$ and $\mathcal{B}_2 := (\gamma_1, \ldots, \gamma_d)$ be two $\mathbb{Q}$-bases of K. Let us denote $\Delta(\mathcal{B}_1) := \Delta(\beta_1, \ldots, \beta_d)$ and $\Delta(\mathcal{B}_2) := \Delta(\gamma_1, \ldots, \gamma_d)$. Then $\Delta(\mathcal{B}_2) = (\det T)^2\Delta(\mathcal{B}_1)$, where T is the change-of-basis matrix from $\mathcal{B}_1$ to $\mathcal{B}_2$. ◀

3.17 Corollary The elements $\beta_1, \ldots, \beta_d \in K$ form a $\mathbb{Q}$-basis of K, if and only if $\Delta(\beta_1, \ldots, \beta_d) \neq 0$.

Proof Let $K = \mathbb{Q}(\alpha)$ as above, $\mathcal{B}_1 := (1, \alpha, \ldots, \alpha^{d-1})$ and $\mathcal{B}_2 := (\beta_1, \ldots, \beta_d)$. Since $\mathcal{B}_1$ is a $\mathbb{Q}$-basis of K, each β_i can be written (uniquely) as $\beta_i = \sum_{j=0}^{d-1} t_{ij}\alpha^j$ with $t_{ij} \in \mathbb{Q}$. By Lemma 3.15 $\Delta(\mathcal{B}_2) = (\det T)^2\Delta(\mathcal{B}_1)$, where $T := (t_{ij})_{\substack{1 \leqslant i \leqslant d \\ 0 \leqslant j \leqslant d-1}}$. We have seen that $\Delta(\mathcal{B}_1) \neq 0$. Therefore, $\Delta(\mathcal{B}_2) \neq 0 \iff \det T \neq 0 \iff \mathcal{B}_2$ is a $\mathbb{Q}$-basis of K. ◀

Finally comes the main theorem of this section:

3.18 Theorem Let K be a number field of degree d. Then $\mathfrak{O}_K$ is a free $\mathbb{Z}$-module of rank d.

Proof Let $\beta_1, \ldots, \beta_d \in K$ form a $\mathbb{Q}$-basis of K. We know that for some $r_1, \ldots, r_d \in \mathbb{Z} \setminus \{0\}$ the elements $r_1\beta_1, \ldots, r_d\beta_d$ are in $\mathfrak{O}_K$ and clearly continue to constitute a $\mathbb{Q}$-basis of K. So we may assume that the elements $\beta_1, \ldots, \beta_d$ are already in $\mathfrak{O}_K$. Consider the set $\mathcal{S}$ of all $\mathbb{Q}$-bases $(\beta_1, \ldots, \beta_d)$ of K consisting of elements from $\mathfrak{O}_K$ only. By Definition 3.13 and Corollary 3.17 $\Delta(\mathcal{B}) \in \mathbb{Z} \setminus \{0\}$ for every $\mathcal{B} \in \mathcal{S}$. Choose $\mathcal{B} := (\beta_1, \ldots, \beta_d) \in \mathcal{S}$ such that $|\Delta(\mathcal{B})|$ is minimal in $\mathcal{S}$.

Claim $\mathcal{B}$ is linearly independent over $\mathbb{Z}$.

$\mathcal{B}$ is by definition a $\mathbb{Q}$-basis of K, i.e., linearly independent over $\mathbb{Q}$ and hence trivially over $\mathbb{Z}$ too.

Claim $\mathcal{B}$ generates $\mathfrak{O}_K$ as a $\mathbb{Z}$-module.

Assume not, i.e., there exists $\alpha \in \mathfrak{O}_K$ such that $\alpha = a_1\beta_1 + \cdots + a_d\beta_d$ with some $a_i \notin \mathbb{Z}$. Without loss of generality we may assume that $a_1 \notin \mathbb{Z}$ and write $a_1 = a + r$ with $a \in \mathbb{Z}$ and $0 < r < 1$. Now define

$\gamma_1 := \alpha - a\beta_1 = r\beta_1 + a_2\beta_2 + \cdots + a_d\beta_d, \gamma_2 := \beta_2, \ldots, \gamma_d := \beta_d$. Since $\mathfrak{O}_K$ is a ring, γ_1 (and hence all of $\gamma_1, \ldots, \gamma_d$) are in $\mathfrak{O}_K$. Furthermore, if

$$T := \begin{pmatrix} r & a_2 & a_3 & \cdots & a_d \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix},$$

by Lemma 3.15 we have $\Delta(\gamma_1, \ldots, \gamma_d) = (\det T)^2 \Delta(\beta_1, \ldots, \beta_d) = r^2 \Delta(\beta_1, \ldots, \beta_d)$. Since $r \neq 0$, $\Delta(\gamma_1, \ldots, \gamma_d) \neq 0$, i.e., $(\gamma_1, \ldots, \gamma_d)$ is again a $\mathbb{Q}$-basis of K (Corollary 3.17), i.e., $(\gamma_1, \ldots, \gamma_d) \in \mathcal{S}$. Finally since $r < 1$, we have $|\Delta(\gamma_1, \ldots, \gamma_d)| < |\Delta(\beta_1, \ldots, \beta_d)|$, a contradiction to the choice of $(\beta_1, \ldots, \beta_d)$. Thus every $\alpha \in \mathfrak{O}_K$ has to be a $\mathbb{Z}$-linear combination of $\beta_1, \ldots, \beta_d$. This completes the proof of the second claim and also of the theorem. ◀

3.19 Definition Any $\mathbb{Z}$-basis of the free $\mathbb{Z}$-module $\mathfrak{O}_K$ is called an integral basis of K (or of $\mathfrak{O}_K$).

3.20 Corollary Every integral basis of K has the same discriminant (for a given K).

Proof Let $\mathcal{B}_1 := (\beta_1, \ldots, \beta_d)$ and $\mathcal{B}_2 := (\gamma_1, \ldots, \gamma_d)$ be two integral bases of K. Let T be the transformation matrix for the change of basis from $\mathcal{B}_1$ to $\mathcal{B}_2$. $\mathcal{B}_1$ being an integral basis of K, all the entries of T are integers. Also from Corollary 3.16 we have $\Delta(\mathcal{B}_2) = (\det T)^2 \Delta(\mathcal{B}_1)$ and hence $\Delta(\mathcal{B}_1)$ divides and has the same sign as $\Delta(\mathcal{B}_2)$. In a similar manner one can show $\Delta(\mathcal{B}_2) \mid \Delta(\mathcal{B}_1)$. Therefore, $\Delta(\mathcal{B}_1) = \Delta(\mathcal{B}_2)$. ◀

3.21 Definition Let K be a number field and $\mathcal{B}$ an integral basis of K. The discriminant of K is defined to be the integer $\Delta_K := \Delta(\mathcal{B})$. By Theorem 3.18 and Corollary 3.20 Δ_K is well-defined, i.e., defined and independent of the choice of the integral basis $\mathcal{B}$ of K.

It's now time for some case studies. We will as usual consider quadratic fields and cyclotomic fields. In both these cases $\mathfrak{O}_K$ has an integral basis of the form $1, \alpha, \ldots, \alpha^{d-1}$ for some suitable α. Let me emphasize here that this is not the general case, i.e., *every number field K need not possess an integral basis of the form* $1, \alpha, \ldots, \alpha^{d-1}$. Whenever it does, $\mathfrak{O}_K = \mathbb{Z}[\alpha]$ is called monogenic and an integral basis $1, \alpha, \ldots, \alpha^{d-1}$ of K is called a power integral basis. Clearly if K has a power integral basis $1, \alpha, \ldots, \alpha^{d-1}$, then $K = \mathbb{Q}(\alpha)$. But the converse is not true, i.e., for $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathfrak{O}_K$ and with $\mathfrak{O}_K$ monogenic, $1, \alpha, \ldots, \alpha^{d-1}$ need not be an integral basis of K. This is demonstrated in the next example.

3.22 Example (1) Consider the quadratic number field $K := \mathbb{Q}(\sqrt{D})$ for some square-free integer $D \neq 0, 1$. We consider the two cases:

Case 1: $D \equiv 2, 3 \pmod 4$

Here $\mathfrak{O}_K = \mathbb{Z}[\sqrt{D}]$, i.e., $(1, \sqrt{D})$ is a power integral basis of K. The minimal polynomial of $\sqrt{D}$ is $X^2 - D$ and the conjugates of $\sqrt{D}$ are $\pm\sqrt{D}$. Therefore by Equation (3.18) we have $\Delta_K = (-1)^{2(2-1)/2}\,\mathrm{N}(2\sqrt{D}) = -(2\sqrt{D})(-2\sqrt{D}) = 4D$.

Case 2: $D \equiv 1 \pmod 4$

In this case $\mathfrak{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$, i.e., $(1, \frac{1+\sqrt{D}}{2})$ is a power integral basis of K. The minimal polynomial of $\frac{1+\sqrt{D}}{2}$ is $X^2 - X - \frac{D-1}{4}$ and the conjugates of $\frac{1+\sqrt{D}}{2}$ are $\frac{1\pm\sqrt{D}}{2}$. Therefore Equation (3.18) tells us that $\Delta_K = (-1)^{2(2-1)/2}\,\mathrm{N}(2\left(\frac{1+\sqrt{D}}{2}\right) - 1) = -\,\mathrm{N}(\sqrt{D}) = -(\sqrt{D})(-\sqrt{D}) = D$.

(2) Let $n \in \mathbb{N}$, ω a primitive n-th root of unity and $K := \mathbb{Q}(\omega)$. Then K is of degree $d := \phi(n)$. It can be shown (using lengthy calculations) that $\mathfrak{O}_K = \mathbb{Z}[\omega]$, i.e., $(1, \omega, \ldots, \omega^{d-1})$ is a power integral basis of K. The minimal polynomial of ω is the cyclotomic polynomial $\Phi_n(X)$. For the special case $n = p \in \mathbb{P}$ we have $\Phi_p(X) = X^{p-1} + \cdots + X + 1$ (Exercise 3.1.5). I leave it as an exercise to the reader to show that in this case $\Delta_K = (-1)^{(p-1)/2} p^{p-2}$, provided that p is odd.

Let us now prove some simple properties of integral bases. As in the proof of Theorem 3.18 we denote by $\mathcal{S}$ the set of all $\mathbb{Q}$-bases of K comprising elements of $\mathfrak{O}_K$ only. We have seen that a basis $\mathcal{B} \in \mathcal{S}$ with minimal $|\Delta(\mathcal{B})|$ is an integral basis of K. On the other hand, by Exercise 3.3.5 any integral basis $\mathcal{B}$ of K is in $\mathcal{S}$ and by Corollary 3.20 has minimal $|\Delta(\mathcal{B})|$ in $\mathcal{S}$.

3.23 Corollary Let $\mathcal{B} \in \mathcal{S}$. If $\Delta(\mathcal{B}) = \Delta_K$, then $\mathcal{B}$ is an integral basis of K. ◀

3.24 Corollary Let $\mathcal{B} \in \mathcal{S}$ have square-free discriminant $\Delta(\mathcal{B})$. Then $\mathcal{B}$ is an integral basis of K.

Proof Let $\mathcal{B}_1 := (\beta_1, \ldots, \beta_d)$ be an integral basis of K. Then $\Delta(\mathcal{B}) = (\det T)^2 \Delta(\mathcal{B}_1)$, where T is the $\mathcal{B}_1$-to-$\mathcal{B}$ change-of-basis matrix. Note that the entries of T are integers. Since $\Delta(\mathcal{B})$ is square-free and non-zero, we must then have $\det T = \pm 1$, i.e., $\Delta(\mathcal{B}) = \Delta(\mathcal{B}_1) = \Delta_K$. Corollary 3.23 now completes the proof. ◀

The converse of Corollary 3.24 is not necessarily true, i.e., the discriminant of an integral bases need not be square-free. For example, look at Case 1 of Example 3.22(1).

3.25 Corollary Let $f(X) \in \mathbb{Z}[X]$ be a monic irreducible non-constant polynomial with a square-free discriminant $\Delta(f)$. Further let α be a root of f and $K := \mathbb{Q}(\alpha)$. Then $\mathfrak{O}_K = \mathbb{Z}[\alpha]$.

Proof Consider $\mathcal{B} := (1, \alpha, \ldots, \alpha^{d-1}) \in \mathcal{S}$, where $d := \deg f$. Then $\Delta(\mathcal{B}) = \Delta(f)$ is square-free. Now use Corollary 3.24. ◀

Now we ask the question whether any integer can be the discriminant of a number field. The answer is 'No'. To see why let $\mathcal{B} := (\beta_1, \ldots, \beta_d)$ be an integral basis of K. Then $\Delta_K = \Delta(\mathcal{B}) = (\det E)^2$, where $E := (e_{i,j}) := (\sigma_j(\beta_i))$ (See Proposition 3.14). We have $\det E = \sum_{\pi \in S_d} \left(\text{Sign}(\pi) \prod_{i=1}^d e_{i,\pi(i)}\right) = s_{\text{even}} - s_{\text{odd}}$, where $s_{\text{even}} := \sum_{\pi \in A_d} \prod_{i=1}^d e_{i,\pi(i)}$ and $s_{\text{odd}} := \sum_{\pi \in S_d \setminus A_d} \prod_{i=1}^d e_{i,\pi(i)}$. For any $i \in \{1, \ldots, d\}$ note that $(\sigma_i \circ \sigma_1, \ldots, \sigma_i \circ \sigma_d)$ is a permutation of $(\sigma_1, \ldots, \sigma_d)$; call it Π_i. If Π_i is even, then $\sigma_i(s_{\text{even}}) = s_{\text{even}}$ and $\sigma_i(s_{\text{odd}}) = s_{\text{odd}}$. On the other hand, if Π_i is odd, then $\sigma_i(s_{\text{even}}) = s_{\text{odd}}$ and $\sigma_i(s_{\text{odd}}) = s_{\text{even}}$. In both the cases we have $\sigma_i(s_{\text{even}} + s_{\text{odd}}) = s_{\text{even}} + s_{\text{odd}}$ and $\sigma_i(s_{\text{even}} s_{\text{odd}}) = s_{\text{even}} s_{\text{odd}}$. By Exercise 3.3.4 we then have $s_{\text{even}} + s_{\text{odd}}, s_{\text{even}} s_{\text{odd}} \in \mathbb{Q}$. But each $e_{i,j} = \sigma_j(\beta_i)$ is an algebraic integer and, therefore, $s_{\text{even}} + s_{\text{odd}}, s_{\text{even}} s_{\text{odd}} \in \mathfrak{O}_K \cap \mathbb{Q} = \mathbb{Z}$. This implies that $\Delta_K = (s_{\text{even}} - s_{\text{odd}})^2 = (s_{\text{even}} + s_{\text{odd}})^2 - 4 s_{\text{even}} s_{\text{odd}} \equiv (s_{\text{even}} + s_{\text{odd}})^2 \pmod 4$. This gives us the following result.

3.26 Theorem [Stickelberger's criterion] Let K be a number field. Then $\Delta_K \equiv 0, 1 \pmod 4$. ◀

Finally we inquire about the sign of the discriminant Δ_K of a number field K. The following result is due to Kronecker.

3.27 Theorem Let K be a number field with signature (r_1, r_2). Then the sign of Δ_K is $(-1)^{r_2}$.

Proof As usual let $\mathcal{B} := (\beta_1, \ldots, \beta_d)$ be an integral basis of K. Then $\Delta_K = \Delta(\mathcal{B}) = (\det E)^2$, where $E = (\sigma_j(\beta_i))$. Consider the matrix $\bar{E} := (\overline{\sigma_j(\beta_i)})$, where bar denotes complex conjugate. If σ_j is a real embedding of K, then $\overline{\sigma_j(\beta_i)} = \sigma_j(\beta_i)$, whereas if σ_j is a properly complex embedding of K, then there exists a properly complex embedding $\sigma_{j'}$ of K with $\overline{\sigma_j(\beta_i)} = \sigma_{j'}(\beta_i)$. Thus $\bar{E}$ can be obtained from E by r_2 column exchanges. Hence $\overline{\det E} = \det \bar{E} = (-1)^{r_2} \det E$. It follows that $\det E$ is purely real or purely imaginary according as whether r_2 is even or odd. This proves the result. ◀

As a sample application of the theory developed so far let us look at Euler's solution of Bachet's equation:

$$y^2 = x^3 - 2\,. \tag{3.19}$$

Bachet pointed out in 1621 that the only solution of his equation in positive integers is $x = 3$, $y = 5$. If we allow negative solutions as well, it turns out that the only integer solutions of Bachet's equation are $x = 3$, $y = \pm 5$. Exercise 3.3.10 deals with a step-by-step derivation of this result. Bachet was a French mathematician who is famous for his Latin translation of Diophantus's Greek book 'Arithmetica'. He also published books on mathematical puzzles.

Exercises for Section 3.3

1. Let K be a field and $\alpha_1, \ldots, \alpha_d \in K$. Show that the determinant of the Vandermonde matrix

$$\mathrm{V} := \mathrm{V}(\alpha_1, \ldots, \alpha_d) := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_d \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_d^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{d-1} & \alpha_2^{d-1} & \alpha_3^{d-1} & \cdots & \alpha_d^{d-1} \end{pmatrix}$$

is $\prod\limits_{\substack{i,j=1 \\ i<j}}^{d} (\alpha_j - \alpha_i)$ and that the square of this determinant is $\prod\limits_{\substack{i,j=1 \\ i<j}}^{d} (\alpha_j - \alpha_i)^2 = (-1)^{d(d-1)/2} \prod\limits_{\substack{i,j=1 \\ i\neq j}}^{d} (\alpha_j - \alpha_i)$. (**Hint:** Use induction on d.) In particular, $\det \mathrm{V}$ is nonzero, if and only if $\alpha_1, \ldots, \alpha_d$ are pairwise distinct.

2. Let p be an odd (rational) prime, ω a primitive p-th root of unity, $K := \mathbb{Q}(\omega)$ and $d := \phi(p) = p - 1$. Show that $\Delta_K = \Delta(1, \omega, \ldots, \omega^{d-1}) = (-1)^{(p-1)/2} p^{p-2}$. (**Remark:** You may assume that $\mathfrak{O}_K = \mathbb{Z}[\omega]$.)

3. Let $n \in \mathbb{N}$ and ω a primitive n-th root of unity. Then $\operatorname{minpoly}_{\omega,\mathbb{Q}}(X) = \Phi_n(X)$. Show that $\Delta(\Phi_n(X)) \mid n^{\phi(n)}$. (**Hint:** In view of Equation 3.18 it is sufficient to look at $\mathrm{N}_{\mathbb{Q}(\omega)|\mathbb{Q}}(\Phi'_n(\omega))$. By Exercise 3.1.5 we have $X^n - 1 = \Phi_n(X) g(X)$ for some $g(X) \in \mathbb{Z}[X]$. Differentiate, substitute $X = \omega$ and take norm.)

4. Let $\alpha \in K$ be fixed by all complex embeddings of K. Show that $\alpha \in \mathbb{Q}$. (**Hint:** Assume that $r := [\mathbb{Q}(\alpha) : \mathbb{Q}] > 1$. Consider any extension of a non-identity embedding of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ to an embedding of K in $\mathbb{C}$.)

5. Show that any integral basis of K (i.e., of $\mathfrak{O}_K$) is a $\mathbb{Q}$-basis of K.

6. Let $a, b, c \in \mathbb{Q}$. Show that:

(a) The discriminant of the quadratic polynomial $X^2 + bX + c$ (assumed irreducible over $\mathbb{Q}$) is $b^2 - 4c$.

(b) Consider the cubic polynomial $X^3 + aX^2 + bX + c$ (assumed irreducible over $\mathbb{Q}$). Show that substituting X by $X - a/3$ reduces this general cubic polynomial to the standard form: $X^3 + uX + v$, where $u, v \in \mathbb{Q}$. Compute that $\Delta(X^3 + uX + v) = -4u^3 - 27v^2$.

7. Let $f(X) := X^d + aX + b \in \mathbb{Q}[X]$ be irreducible. Show that

$$\Delta(f) = (-1)^{d(d-1)/2} \left(d^d b^{d-1} + (-1)^{d-1} (d-1)^{d-1} a^d \right).$$

(**Hint:** Let α be a root of $f(X)$. Then $\Delta(f) = (-1)^{d(d-1)/2}\,\mathrm{N}(\beta)$, where $\beta = f'(\alpha)$. First show that $\alpha = \frac{-db}{\beta+(d-1)a}$, so that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, i.e., $\deg(\mathrm{minpoly}_{\beta,\mathbb{Q}}(X)) = d$. From $f(\alpha) = 0$ compute the minimal polynomial and hence the norm of β.)

8. **(a)** Let $K := \mathbb{Q}(\alpha)$, where α is a root of $f(X) := X^3 + X + 1$. (Argue that f is irreducible over $\mathbb{Q}$.) Compute $\Delta(f) = \Delta(1, \alpha, \alpha^2)$ and conclude that $\mathfrak{O}_K = \mathbb{Z}[\alpha]$. (**Hint:** Corollary 3.25.)

(b) Repeat Part (a) with $f(X) := X^3 - X - 1$.

(c) Repeat Part (a) with $f(X) := X^5 - X - 1$.

9. Let Δ_1 and Δ_2 be two square-free rational integers $\neq 0, 1$ and let $K_1 := \mathbb{Q}(\sqrt{\Delta_1})$ and $K_2 := \mathbb{Q}(\sqrt{\Delta_2})$. Show that $K_1 = K_2$, if and only if $\Delta_1 = \Delta_2$.

10. (Bachet's equation) In this exercise one derives that the only (rational) integer solutions of Equation (3.19) (i.e., of $y^2 = x^3 - 2$) are $x = 3$, $y = \pm 5$.

(a) Show that (3.19) has no solutions with x or y even. (**Hint:** Reduce modulo 4.)

Let (x, y) be a solution of (3.19) with both x and y odd. Then x^3 admits a factorization in $\mathbb{Z}[\sqrt{-2}]$ as $x^3 = (y + \sqrt{-2})(y - \sqrt{-2})$.

(b) Let $K := \mathbb{Q}(\sqrt{-2})$. Show that $\mathfrak{O}_K = \mathbb{Z}[\sqrt{-2}]$ and that $\mathfrak{O}_K$ is a UFD. Also the only units of $\mathfrak{O}_K$ are ± 1.

(c) Show that $\gcd(y + \sqrt{-2}, y - \sqrt{-2}) = 1$. (**Hint:** Let $a + b\sqrt{-2} \in \mathfrak{O}_K$ divide this gcd. Then $a + b\sqrt{-2}$ divides $2y$ and $2\sqrt{-2}$. Take norms.)

(d) Because of unique factorization one can write $y + \sqrt{-2} = \pm(c + d\sqrt{-2})^3$ for $c, d \in \mathbb{Z}$. Expand the cube and equate the real and imaginary parts to conclude that we must have $y = \pm 5$, so that $x = 3$.

11. Show that the only (rational) integer solutions of $y^2 = x^3 - 4$ are $(x, y) = (2, \pm 2), (5, \pm 11)$.

12. We have seen that the discriminant of a non-constant irreducible polynomial in $\mathbb{Q}[X]$ can be obtained by calculating the norm of a certain element. Here is an alternative way to proceed.

Let $f(X) := a_m X^m + \cdots + a_1 X + a_0$ and $g(X) := b_n X^n + \cdots + b_1 X + b_0$ be non-constant polynomials with rational coefficients. The Sylvester matrix associated to (f, g) is defined as the $(m + n) \times (m + n)$ matrix:

$$\mathrm{Syl}(f,g) := \begin{pmatrix}
a_m & a_{m-1} & \cdots & \cdots & a_1 & a_0 & 0 & 0 & \cdots & 0 \\
0 & a_m & a_{m-1} & \cdots & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\
 & & \ddots & & & & \ddots & & & \\
0 & \cdots & 0 & a_m & a_{m-1} & \cdots & \cdots & \cdots & a_1 & a_0 \\
b_n & b_{n-1} & \cdots & \cdots & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\
0 & b_n & b_{n-1} & \cdots & \cdots & \cdots & b_1 & b_0 & \cdots & 0 \\
 & & \ddots & & & & \ddots & & & \\
0 & \cdots & b_n & b_{n-1} & \cdots & \cdots & \cdots & \cdots & b_1 & b_0
\end{pmatrix}$$

The resultant of f and g is defined as:

$$\mathrm{Res}(f, g) := \det(\mathrm{Syl}(f, g)).$$

(a) Show that $\mathrm{Res}(f, g) = 0$, if and only if f and g have a common root in $\mathbb{C}$ (or equivalently, if and only if f and g admit a nonconstant common divisor in $\mathbb{Q}[X]$.) (**Hint:** Argue that f and g have a common root, if and only if there exist polynomials $u(X), v(X) \in \mathbb{C}[X]$ (or in $\mathbb{Q}[X]$) with $\deg u \leqslant n - 1$ and $\deg v \leqslant m - 1$ such that $uf + vg = 0$. An attempt to solve for the $m + n$ unknown coefficients of u and v gives a linear system. Look at the determinant of this system.)

**** (b)** Let $\alpha_1, \ldots, \alpha_m$ be the roots of f and $\beta_1, \ldots, \beta_n$ the roots of g. Show that

$$\mathrm{Res}(f, g) = a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j) = a_m^n \prod_{i=1}^{m} g(\alpha_i) = (-1)^{mn} b_n^m \prod_{j=1}^{n} f(\beta_j)\,.$$

(c) Let $f(X) \in \mathbb{Q}[X]$ be irreducible, monic and of degree $d \geqslant 1$. Deduce that $\Delta(f) = (-1)^{d(d-1)/2}\mathrm{Res}(f, f')$.