We fix a field k, and a field extension ℓ/k.

Let V be a k-vector space. Consider the ℓ-vector space $\tilde{V}$ on the basis $(e_v, v \in V)$. Let $V \otimes_k \ell$ be the quotient of $\tilde{V}$ by the ℓ-subspace generated by the elements

$$\begin{cases} \lambda e_v - e_{\lambda v} & \text{for } \lambda \in k, v \in V, \\ e_{u+v} - e_u - e_v & \text{for } u, v \in V. \end{cases}$$

For $\mu \in \ell$ and $v \in V$, we denote by $v \otimes \mu \in V \otimes_k \ell$ the image of μe_v.

Exercise 1. Let V be a k-vector space and W an ℓ-vector space. Let $f \colon V \to W$ a k-linear map. Show that there exists a unique ℓ-linear map

$$g \colon V \otimes_k \ell \to W$$

such that $g(v \otimes 1) = f(v)$ for all $v \in V$.

Exercise 2. Let V be a k-vector space. Show that the map $V \to V \otimes_k \ell$ given by $v \mapsto v \otimes 1$ is k-linear and injective. (Hint: injectivity is more subtle point.)

Exercise 3. Let V be a k-vector space, and assume that $e_1, \dots, e_n$ is a k-basis of V. Show that $e_1 \otimes 1, \dots, e_n \otimes 1$ is an ℓ-basis of $V \otimes_k \ell$, and deduce that $\dim_k V = \dim_\ell(V \otimes_k \ell)$.

Exercise 4. Let V, W be a k-vector spaces, and $f \colon V \to W$ a k-linear map.

(i) Show that f induces an ℓ-linear map $g \colon V \otimes_k \ell \to W \otimes_k \ell$.

(ii) If f is surjective, show that g is surjective.

(iii) If f is injective, show that g is injective.

Exercise 5. Let A be a k-algebra.

(i) Show that $A \otimes_k \ell$ is a naturally an ℓ-algebra.

(ii) Let B be an ℓ-algebra, and $f \colon A \to B$ be a morphism of k-algebras. Show that the induced ℓ-linear map $A \otimes_k \ell \to B$ is a morphism of ℓ-algebras.

Exercise 6. (i) Let V, W be k-vector spaces. Show that

$$(V \oplus W) \otimes_k \ell \simeq (V \otimes_k \ell) \oplus (W \otimes_k \ell)$$

as ℓ-vector spaces.

(ii) Let A, B be k-algebras. Show that

$$(A \times B) \otimes_k \ell \simeq (A \otimes_k \ell) \times (B \otimes_k \ell)$$

as ℓ-algebras.

Exercise 7. (i) Show that $(k[X]) \otimes_k \ell \simeq \ell[X]$ as ℓ-algebra.

(ii) Let A be a k-algebra and I an ideal of A. Show that $I \otimes_k \ell$ may be viewed as an ideal of $A \otimes_k \ell$, and that $(A/I) \otimes_k \ell \simeq (A \otimes_k \ell)/(I \otimes_k \ell)$.

(iii) Let $P \in k[X]$, and $A = k[X]/P$. Show that the ℓ-algebra $A \otimes_k \ell$ is naturally isomorphic to $\ell[X]/P$.

Exercise 8. Let A be a k-algebra.

(i) If A is an integral domain, is $A \otimes_k \ell$ an integral domain? Give a proof or a counterexample.

(ii) If A is reduced, is $A \otimes_k \ell$ reduced? Give a proof or a counterexample.

Recall that an element x in a (commutative) ring A is called *irreducible* if $x \notin A^\times$, $x \neq 0$, and for all $a, b \in A$

$$x = ab \implies a \in A^\times \text{ or } b \in A^\times.$$

Exercise 1. When A is a (commutative) ring, we say that an element $p \in A$ is *prime* if pA is a nonzero prime ideal of A.

(i) Assume that A is a domain. Show that every prime element of A is irreducible.

(ii) Assume that A is a principal ideal domain. Show that every irreducible element of A is prime. (Hint: Show that the ideal generated by an irreducible is maximal.)

Exercise 2. Let A be a principal ideal domain. Let $a \in A$ be such that $a \neq 0$ and $a \notin A^\times$.

(i) Show that there exist irreducible elements $p_1, \dots, p_n$ in A such that

$$a = p_1 \dots p_n.$$

(Hint: Consider the set of ideals generated by elements $a \notin A^\times \cup \{0\}$ which admit no such decomposition, and use the fact that A is noetherian.)

(ii) Show that the elements $p_1, \dots, p_n$ are uniquely determined by a, up to their ordering and multiplication by units of A.

Exercise 3. We are going to solve the equation

$$y^3 = x^2 + 1, \quad \text{with } x, y \in \mathbb{Z}.$$

We consider the ring of Gaussian integers $\mathbb{Z}[i]$.

(i) Show that the element $1 + i$ is prime in $\mathbb{Z}[i]$.

(ii) Let $x \in \mathbb{Z}$. Let us pick $d \in \mathbb{Z}[i]$ such that $d\mathbb{Z}[i]$ is the ideal generated by $x - i$ and $x + i$. Show that $d = u(1+i)^n$, where $u \in \mathbb{Z}[i]^\times$, and $n \in \{0, 1, 2\}$.

(iii) Assume that $x, y \in \mathbb{Z}$ are such that $x^2 + 1 = y^3$. Show that the ideal generated by $x + i$ and $x - i$ in $\mathbb{Z}[i]$ is the whole ring $\mathbb{Z}[i]$.

(iv) Find all solutions to the equation

$$y^3 = x^2 + 1, \quad \text{with } x, y \in \mathbb{Z}.$$

Exercise 4. Let $\pi \in \mathbb{Z}[i]$ be a prime element. Show that there exists a prime number $p \in \mathbb{N}$ such that $\mathrm{N}(\pi) = p$ or $\mathrm{N}(\pi) = p^2$. (Here $\mathrm{N}\colon \mathbb{Z}[i] \to \mathbb{Z}$ is the norm function defined in the lectures.)

Exercise 5. Consider an integer $x \in \mathbb{N}$, and its prime decomposition in $\mathbb{Z}$

$$n = \prod_p p^{v_p(n)},$$

where p runs over the prime numbers, and $v_p(n) \in \mathbb{N}$.

Show that the following conditions are equivalent:

(a) there exist $a, b \in \mathbb{N}$ such that $n = a^2 + b^2$,

(b) for each prime number p congruent to 3 modulo 4, the integer $v_p(n)$ is even.

(Hint: Use the previous exercise.)

Exercise 6. Let $p \in \mathbb{N}$ be a prime number.

(i) If $p = 2$, show that $p \in \mathbb{Z}[i]$ can be written as $p = ab$ where $a, b \in \mathbb{Z}[i]$ are prime elements generating the same ideal in $\mathbb{Z}[i]$.

(ii) If $p = 3 \mod 4$, then $p \in \mathbb{Z}[i]$ is a prime element. (Hint: Use the results from the lectures.)

(iii) If $p = 1 \mod 4$, then $p \in \mathbb{Z}[i]$ can be written as $p = ab$, where $a, b \in \mathbb{Z}[i]$ are prime elements generating different ideals in $\mathbb{Z}[i]$.

Exercise 1. Show that the polynomial ring $\mathbb{Z}[X]$ is not a principal ideal domain.

Exercise 2. Let A be a nonzero noetherian ring, and M a free A-module of rank n. If m is an integer such that the A-module M is free of rank m, show that $m = n$. (Hint: consider a maximal ideal of A.)

Exercise 3. Let A be a domain, and $P \in A[X]$ a polynomial. Show that $A[X]/P$ is integral over A if and only if the leading coefficient of the polynomial P is a unit in A.

Exercise 4. Let A be a domain having only finitely many elements. Show that A is a field.

Exercise 5. Let A be a domain, with fraction field K. Let L be a field extension of K having finite degree, and B the integral closure of A in L. Show that L is the fraction field of B.

Exercise 6. Let $A \subset R$ be a ring extension. Consider the following conditions

(a) the extension $A \subset R$ is integral,

(b) the A-module R is finitely generated.

Does (a) implies (b)? Does (b) implies (a)? (Justify your answers, either with a proof, reference to the lecture, or counterexample). Same questions when the A-algebra R is additionally assumed to be finitely generated.

Exercise 7. (Time permitting) We let $\sqrt{-5} \in \mathbb{C}$ be one of the roots of the polynomial $X^2 + 5$, and consider the subset

$$R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

Show that R is a subring of $\mathbb{C}$, and that R is not a principal ideal domain. (Hint: Assuming that R is a principal ideal domain, consider a prime decomposition of $1 + \sqrt{-5}$.)

Exercise 8. (Time permitting) Let K be a quadratic field.

(i) Let $\sigma \colon K \to K$ the nontrivial morphism of $\mathbb{Q}$-algebras. Express the maps

$$\mathrm{Tr}_{K/\mathbb{Q}} \colon K \to \mathbb{Q} \quad \text{and} \quad \mathrm{N}_{K/\mathbb{Q}} \colon K \to \mathbb{Q}$$

in terms of σ.

(ii) Show that $\mathrm{N}_{K/\mathbb{Q}}(\mathcal{O}_K) \subset \mathbb{Z}$.

Exercise 1. Let A, B be rings. Show that every ideal of the ring $A \times B$ is of the form $I \times J$, where $I \subset A$ and $J \subset B$ are ideals.

Exercise 2. Let k be a field. A k-algebra is called *diagonalisable* if it is isomorphic to k^n, for some integer $n \in \mathbb{N}$.

(i) Show that a finite-dimensional k-algebra A is diagonalisable if and only if the k-vector space of linear forms $\mathrm{Hom}_k(A, k)$ is generated by morphisms of k-algebras.

(ii) Deduce that every k-subalgebra of a diagonalisable k-algebra is diagonalisable.

(iii) Show that every diagonalisable k-algebra is generated by idempotent elements as a k-vector space. (Recall that an element x in a ring R is called idempotent if $x^2 = x$.)

(iv) Let $(e_1, \dots, e_n)$ be the canonical k-basis of k^n. For $I \subset \{1, \dots, n\}$, set

$$e_I = \sum_{i \in I} e_i.$$

Show that every idempotent of k^n is of the form e_I for some $I \subset \{1, \dots, n\}$.

(v) Deduce that a diagonalisable k-algebra admits only finitely many k-subalgebras.

Exercise 3. Let A be a k-algebra. We assume that there exists a field extension ℓ/k such that the ℓ-algebra $A \otimes_k \ell$ is diagonalisable. Show that the k-algebra A is étale. (N.B.: the converse was established in the lectures).

Exercise 4. Let k be a field, and A an étale k-algebra. (Hint for the questions below: Use the two previous exercises.)

(i) Let $B \subset A$ be a k-subalgebra. Show that B is an étale k-algebra.

(ii) Let C be a quotient k-algebra of A (i.e. $C = A/I$ for some ideal I of A). Show that the k-algebra C is étale.

(iii) Show that the k-algebra A admits only finitely many subalgebras and quotient algebras.

(iv) Assume that k is infinite. Show that there exists a separable polynomial $P \in k[X]$ such that $A \simeq k[X]/P$. (Hint: to show that A is generated by a single element as a k-algebra, recall that no k-vector space is a finite union of proper subspaces.)

Exercise 5. Let L/K be a field extension of finite degree. We are going to prove that the following conditions are equivalent:

(a) The K-algebra L is generated by a single element,

(b) There exist only finitely many subextensions of L/K.

We proceed as follows:

(i) Show that (b) implies (a). (Hint: Treat the cases k finite and infinite using different arguments.)

(ii) Assume that $L = K(\alpha)$ for some $\alpha \in L$. Let E/K be a subextension of L/K, and let

$$P = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in E[X]$$

be the minimal polynomial of α over E. Show that $E = K(a_0, \ldots, a_{d-1})$.

(iii) Show that in (ii) the image of P in $L[X]$ can take only finitely many values, as E/K varies (the element α being fixed).

(iv) Deduce that (a) implies (b).

Exercise 1 (Gauss Lemma)**.** Let A be a principal ideal domain, and K its fraction field. When $P \in A[X]$ is a polynomial, we define its *content* $\operatorname{cont}(P)$ as the ideal generated in A by its coefficients.

(i) Let $R \in A[X]$. Show that there exists $\alpha \in A$ and $\widetilde{R} \in A[X]$ such that $\operatorname{cont}(R) = \alpha A$ and $R = \alpha \widetilde{R}$.

(ii) Let $P, Q \in A[X]$ be such that $\operatorname{cont}(P) = \operatorname{cont}(Q) = A$. Show that $\operatorname{cont}(PQ) = A$. (Hint: Consider a prime ideal $\mathfrak{p}$ of A, and show that $PQ \notin \mathfrak{p}A[X]$.)

(iii) Let $P, Q \in A[X]$. Show that $\operatorname{cont}(PQ) = \operatorname{cont}(P)\operatorname{cont}(Q)$.

(iv) Let K be the fraction field of A, and $P \in A[X]$ be such that $\operatorname{cont}(P) = A$. Deduce that P is irreducible in $A[X]$ if and only if it is irreducible in $K[X]$.

Exercise 2. Let A be an integrally closed domain with fraction field K. Let L/K be a finite field extension. Consider an element $\alpha \in L$, and let $P \in K[X]$ be its minimal polynomial over K. Show that α is integral over A if and only if $P \in A[X]$.

Exercise 3. Let $a, b \in \mathbb{Q}$ be such that the polynomial $P = X^n + aX + b$ is irreducible in $\mathbb{Q}[X]$. Let $\alpha \in \mathbb{C}$ be a root of P, and $K = \mathbb{Q}(\alpha)$. Show that

$$\mathrm{D}_{K/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} + a^n(1-n)^{n-1}).$$

Exercise 4. Let $P = X^3 + X + 1 \in \mathbb{Z}[X]$.

(i) Show that the polynomial P is irreducible in $\mathbb{Q}[X]$.

(ii) Let $\alpha \in \mathbb{C}$ be a root of P, and consider the subfield $K = \mathbb{Q}(\alpha) \subset \mathbb{C}$. Show that $[K : \mathbb{Q}] = 3$ and that $\alpha \in \mathcal{O}_K$.

(iii) Show that $(1, \alpha, \alpha^2)$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$. (Hint: Use the previous exercise.)

Exercise 5. (Optional) Let $n \geq 2$ be an integer, and $\xi \in \mathbb{C}$ a primitive n-th root of unity. Let $P \in \mathbb{Q}[X]$ be the minimal polynomial of ξ over $\mathbb{Q}$. Let

$$\Phi_n = \prod_{k \in S}(X - \xi^k),$$

where $S \subset \{1, \ldots, n\}$ is the set of elements k with $\gcd(k, n) = 1$. We are going to prove that $P = \Phi_n$

We let p be prime number, and denote $Q \mapsto \overline{Q}$ the reduction modulo p map $\mathbb{Z}[X] \to \mathbb{F}_p[X]$. Let $F \in \mathbb{Q}[X]$ be the minimal polynomial of ξ^p over $\mathbb{Q}$.

(i) Show that $P, F \in \mathbb{Z}[X]$.

(ii) Show that $\overline{F}$ and $\overline{P}$ have a common irreducible divisor in $\mathbb{F}_p[X]$. (Hint: consider the polynomial $G = P(X^p) \in \mathbb{Z}[X]$.)

(iii) Assume that the prime number p does not divide n. Show that $F = P$.

(iv) Deduce that $\Phi_n \mid P$ in $\mathbb{Q}[X]$.

(v) Show that

$$\Phi_n = \prod_{d|n} \Phi_d$$

and deduce that $\Phi_n \in \mathbb{Z}[X]$.

(vi) Conclude.

Exercise 1. Let k be a field. Show that $k[X,Y]$ is not a Dedekind domain.

Exercise 2. Let k be a field, and consider the subring $A = k[X^2, X^3]$ of the polynomial ring $k[X]$.

(i) Show that A is a noetherian domain, and that every nonzero prime ideal of A is maximal. (Hint: Use the inclusions $k[X^2] \subset A \subset k[X]$.)

(ii) Let $k(X)$ be the fraction field of $k[X]$. Show that $k(X)$ is the fraction field of A.

(iii) Show that A is not a Dedekind domain.

Exercise 3 (Approximation Lemma)**.** Let A be a Dedekind domain, with fraction field K. For a nonzero prime ideal $\mathfrak{q}$ of A, and a element $y \in K$, we define

$$v_{\mathfrak{q}}(y) = \sup\{n \in \mathbb{Z} | y \in \mathfrak{q}^n\} \in \mathbb{Z} \cup \{\infty\}.$$

(i) For $a, b \in A$ and $\mathfrak{q}$ a nonzero prime ideal of A, show that

$$v_{\mathfrak{q}}(a+b) \geq \min\{v_{\mathfrak{q}}(a), v_{\mathfrak{q}}(b)\} \quad \text{and} \quad v_{\mathfrak{q}}(ab) = v_{\mathfrak{q}}(a) + v_{\mathfrak{q}}(b).$$

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be pairwise distinct nonzero prime ideals of A. Let $x_1, \ldots, x_s \in K$ and $n_1, \ldots, n_s \in \mathbb{N}$. We are going to prove that we may find $x \in K$ such that

$$v_{\mathfrak{p}_i}(x - x_i) \geq n_i \quad \text{for } i \in \{1, \ldots, s\}, \quad \text{and} \quad v_{\mathfrak{q}}(x) \geq 0 \quad \text{for } \mathfrak{q} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}. \quad (*)$$

(ii) If $s \geq 2$, show that $\mathfrak{p}_1^{n_1} + \mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_s^{n_s} = A$.

(iii) Show that we may find $x \in A$ satisfying $(*)$ when $x_1 \in A$ and $x_2 = \cdots = x_s = 0$.

(iv) Show that we may find $x \in A$ satisfying $(*)$ when $x_1, \ldots, x_s \in A$.

(v) Show that we may find $x \in K$ satisfying $(*)$.

Exercise 4. (Optional) Let A be a Dedekind domain.

(i) Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be pairwise distinct nonzero prime ideals of A. Let $n_1, \ldots, n_s \in \mathbb{N}$. Show that we may find an element $x \in A$ such that $v_{\mathfrak{p}_i}(x) = n_i$ for all $i \in \{1, \ldots, s\}$. (Hint: Use the previous exercise.)

(ii) Show that every ideal of A is generated by at most two elements.

(iii) Assume that A has only finitely prime ideals. Reprove (using (i)) that A is a principal ideal domain.

Exercise 1. Let K be a number field, and $I \subset \mathcal{O}_K$ a nonzero ideal such that $\mathrm{N}(I) = \mathrm{card}(\mathcal{O}_K/I)$ is a prime number. Show that the ideal I is prime.

Exercise 2. Let K be a number field and $\mathfrak{p}$ a nonzero prime ideal of $\mathcal{O}_K$. Show that $\mathrm{N}(\mathfrak{p}) = \mathrm{card}(\mathcal{O}_K/\mathfrak{p}) \in \mathbb{N}$ is a power of a prime number.

Exercise 3. Let A be a local noetherian domain. Assume that the maximal ideal $\mathfrak{m}$ of A is principal. We assume that A is not a field.

(i) Show that $\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = 0$.

(ii) Let K be the fraction field of A, and $\pi \in A$ a generator of $\mathfrak{m}$. Show that every element $x \in K \smallsetminus \{0\}$ is of the form $x = \pi^n u$ for unique elements $u \in A^\times$ and $n \in \mathbb{Z}$.

(iii) Deduce that A is a discrete valuation ring.

Exercise 4. Let A be a discrete valuation ring with fraction field K. Let π be a uniformising parameter of A. Let $\mathfrak{m} = \pi A$ be the maximal ideal of A, and $k = A/\mathfrak{m}$. We denote by $P \mapsto \overline{P}$ the reduction map $A[X] \to k[X]$.

(i) Let $Q \in A[X]$ be such that $\overline{Q} \neq 0$ in $k[X]$. If $U \in K[X]$ is such that $QU \in A[X]$, show that $U \in A[X]$.

We now let $P \in A[X]$ be a monic polynomial such that $\overline{P} \in k[X]$ is irreducible, and consider the ring $B = A[X]/P$.

(ii) Show that the ring B is a domain. (Hint: use (i)).

(iii) Show that the ring B is a discrete valuation ring, with uniformising parameter π. (Hint: Use Exercise 3.)

(iv) Let
$$Q = X^n + a_{n-1}X^{n-1} + \cdots + a_0, \text{with } a_0, \dots, a_{n-1} \in A.$$
Assume that a_0 is a uniformising parameter of A, and that $a_0 \mid a_i$ for all $i = 1, \dots, n-1$. Show that $C = A[X]/Q$ is a discrete valuation ring, where the class of X is a uniformising parameter. (Hint: This is not a direct consequence of (iii).)

Exercise 1. Let A be a domain, and $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ prime ideals of A.

(i) Show that the set $S = A \smallsetminus (\mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_n)$ is multiplicatively closed.

(ii) Assume that $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ for all $i \neq j$. Show that the ring $S^{-1}A$ possesses n maximal ideals.

Exercise 2. Let A be a Dedekind domain. We are going to prove that every ideal of A is generated by at most two elements.

(i) Let $x \in A$ be a nonzero element. Show that x is contained in only finitely many prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ of A.

(ii) Let $S = A \smallsetminus (\mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_n)$. Show that the ring $S^{-1}A$ is a principal ideal domain. (Hint: use the previous exercise.)

(iii) Show that for any $s \in S$, we have $sA + xA = A$.

(iv) Show that we have a ring isomorphism $A/xA \xrightarrow{\sim} (S^{-1}A)/(xS^{-1}A)$.

(v) Deduce that every ideal of A/xA is principal.

(vi) Conclude that every ideal of A is generated by at most two elements.

Exercise 3. Let A be a Dedekind domain, and $S \subset A$ a multiplicatively closed subset. Show that mapping a nonzero fractional ideal I of A to $S^{-1}I$ induces a surjective group morphism $\mathcal{C}(A) \to \mathcal{C}(S^{-1}A)$ between the ideal class groups.

Exercise 4. Let A be a Dedekind domain, and $f \in A$ a nonzero element. Consider the multiplicatively closed subset $S = \{f^n | n \in \mathbb{N}\}$ in A, and let r be the number of prime ideals of A containing f (recall from Exercise 2 (i) that $r < \infty$).

(i) Let Q be the kernel of the natural morphism $\mathcal{F}(A) \to \mathcal{F}(S^{-1}A)$ (where $\mathcal{F}(A), \mathcal{F}(S^{-1}A)$ denote the respective groups of nonzero fractional ideals). Show that the $\mathbb{Z}$-module Q is free of rank r.

(ii) By considering the morphism

$$(S^{-1}A)^\times \to \mathcal{F}(A), \quad x \mapsto xA$$

show that the $\mathbb{Z}$-module $(S^{-1}A)^\times/A^\times$ is free of rank $\leq r$.

Exercise 5 (Optional)**.** Let B be a noetherian domain, and $A \subset B$ a subring such that B is integral over A. If $\mathfrak{p}$ is a prime ideal of A, show that there exists a prime ideal $\mathfrak{q}$ of B such that $\mathfrak{q} \cap A = \mathfrak{p}$. (This is called the "going-up" theorem.)

Exercise 1. Let K be an imaginary quadratic field. Show that the group $(\mathcal{O}_K)^\times$ is finite and cyclic. (A more precise answer is obtained in Exercise 5 below).

Exercise 2. Let K be a real quadratic field. We fix an embedding $K \subset \mathbb{R}$.

(i) Show that $(\mathcal{O}_K)^\times \simeq \mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})$.

(ii) Deduce that the subset of units in $\mathcal{O}_K$ which are > 0 is a free $\mathbb{Z}$-module of rank 1, which admits a unique generator u such that $u > 1$. This element u is called *the fundamental unit* of K.

Exercise 3. Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field, where $d \in \mathbb{N} \smallsetminus \{0, 1\}$ is square-free. We view K as a subfield of $\mathbb{R}$. In this exercise, we describe a procedure to determine explicitly the fundamental unit of K (see the previous exercise).

(i) Let $x \in (\mathcal{O}_K)^\times$, and write $x = a + b\sqrt{d}$, with $a, b \in \mathbb{Q}$. Show that $a^2 \geq b^2$. *(Hint: the number $a^2 - db^2$ can only take two values...)*

(ii) Let $x \in (\mathcal{O}_K)^\times$, and write $x = a + b\sqrt{d}$, with $a, b \in \mathbb{Q}$. Show that

$$(x > 1) \Longleftrightarrow (a > 0 \text{ and } b > 0).$$

(Hint: If $x > 1$, observe that x is the unique maximal element of the set $\{x, x^{-1}, -x, -x^{-1}\}$.)

(iii) Assume that $d = 2, 3 \mod 4$. Show that the fundamental unit of K can be written as $a_1 + b_1\sqrt{d}$ with $a_1, b_1 \in \mathbb{N} \smallsetminus \{0\}$. Let $x = a + b\sqrt{d} \in (\mathcal{O}_K)^\times$, with $a, b \in \mathbb{N} \smallsetminus \{0\}$. Show that $b \geq b_1$, and that $b = b_1$ implies $a = a_1$.

(Hint: consider the sequences $a_n, b_n \in \mathbb{N} \smallsetminus \{0\}$ defined by $(a_1 + b_1\sqrt{d})^n = a_n + b_n\sqrt{d}$.)

(iv) Assume that $d = 2, 3 \mod 4$. Let $b \in \mathbb{N} \smallsetminus \{0\}$ be the smallest integer such that $db^2 - 1$ or $db^2 + 1$ is of the form a^2 with $a \in \mathbb{N} \smallsetminus \{0\}$. Show that $a + b\sqrt{d}$ is the fundamental unit of K.

(v) Assume that $d = 1 \mod 4$. Show that the fundamental unit of K can be written as $\frac{1}{2}(a_1 + b_1\sqrt{d})$ with $a_1, b_1 \in \mathbb{N} \smallsetminus \{0\}$. Let $x = a + b\sqrt{d} \in (\mathcal{O}_K)^\times$, with $a, b \in \mathbb{N} \smallsetminus \{0\}$. Show that $b \geq b_1$. Assume that $b = b_1$ and $a \neq a_1$. Show that $d = 5$, that $a_1 = b_1 = 1$ and $a = 3$.

(Hint: consider the sequences $a_n, b_n \in \mathbb{N} \smallsetminus \{0\}$ defined by $(\frac{1}{2}(a_1 + b_1\sqrt{d}))^n = \frac{1}{2}(a_n + b_n\sqrt{d})$, and analyse the conditions under which $b_2 = b_1$.)

(vi) Assume that $d = 1 \mod 4$ with $d \neq 5$. Let $b \in \mathbb{N} \smallsetminus \{0\}$ be the smallest integer such that $db^2 - 4$ or $db^2 + 4$ is of the form a^2 with $a \in \mathbb{N} \smallsetminus \{0\}$. Show that $\frac{1}{2}(a + b\sqrt{d})$ is the fundamental unit of K.

(vii) Determine the fundamental units of the following quadratic fields:

$$\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{6}), \mathbb{Q}(\sqrt{17})$$

Exercise 4 (Pell's equation)**.** (i) Let $d \in \mathbb{N} \smallsetminus \{0, 1\}$ be square-free. Show that the set of solutions $x, y \in \mathbb{N}$ to the equation

$$x^2 - dy^2 = 1,$$

is $\{(x_n, y_n) | n \in \mathbb{N}\}$, where

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n.$$

(Hint: Use the previous exercise.)

(ii) Determine (x_1, y_1) when $d \in \{2, 5, 6, 17\}$.

Exercise 5. Let K be an imaginary quadratic number field. Show that

$$(\mathcal{O}_K)^\times = \begin{cases} \{1, -1, i, -i\} & \text{if } K = \mathbb{Q}(i), \\ \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}, \text{where } \alpha = \frac{1+\sqrt{-3}}{2} & \text{if } K = \mathbb{Q}(\sqrt{-3}) \\ \{1, -1\} & \text{otherwise.} \end{cases}$$

Exercise 1. Let K be a number field.

(i) Show that there exists a monic irreducible polynomial $P \in \mathbb{Z}[X]$ and a root $\alpha \in \mathbb{C}$ such that $K = \mathbb{Q}(\alpha)$.

For the rest of the exercise, we assume that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. For $a, b \in \mathcal{O}_K$, we will denote by (a, b) the ideal of $\mathcal{O}_K$ generated by a and b. We let $p \in \mathbb{Z}$ be a prime number, and denote by $R \mapsto \overline{R}$ the reduction map $\mathbb{Z}[X] \to \mathbb{F}_p[X]$. Let us fix a polynomial $Q \in \mathbb{Z}[X]$ such that $\overline{Q} \in \mathbb{F}_p[X]$ is irreducible.

(ii) Assume that $\overline{Q}$ divides $\overline{P}$ in $\mathbb{F}_p[X]$. Show that the ideal $(p, Q(\alpha)) \in \mathcal{O}_K$ is prime.

(iii) Let $m \in \mathbb{N} \smallsetminus \{0\}$ be such that $\overline{Q}^m$ divides $\overline{P}$ in $\mathbb{F}_p[X]$. Show that

$$(p, Q(\alpha))^m = (p, Q(\alpha)^m).$$

(iv) Write $\overline{P} = \overline{P_1}^{n_1} \cdots \overline{P_s}^{n_s}$ where $P_1, \ldots, P_s \in \mathbb{Z}[X]$ are such that $\overline{P_1}, \ldots, \overline{P_s}$ are monic irreducible in $\mathbb{F}_p[X]$ and pairwise distinct. Show that

$$p\mathcal{O}_K = \prod_{i=1}^{s} (p, P_i(\alpha))^{n_i},$$

is the decomposition of the ideal $p\mathcal{O}_K$ as a product of prime ideals in $\mathcal{O}_K$.

Exercise 2. Consider the polynomial $P = X^3 + X + 1 \in \mathbb{Z}[X]$, and let $\alpha \in \mathbb{C}$ be a root of P. We recall from Exercise 4, Sheet 5 that $K = \mathbb{Q}(\alpha)$ is a number field of degree 3 whose absolute discriminant is 31, and that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

(i) Which prime numbers p ramify in K?

(ii) For every prime number p which ramifies in K, give an explicit description of the decomposition of $p\mathcal{O}_K$ as a product of prime ideals in $\mathcal{O}_K$. (Hint: use the previous exercise; compute $P(3)$ and $P(14)$.)

Exercise 3. Let K be a number field, and I an ideal of $\mathcal{O}_K$.

(i) Show that there exists an integer $n > 0$ such that the ideal I^n of $\mathcal{O}_K$ is principal.

(ii) Let $n > 0$ be an integer such that I^n is principal. Show that there exists a field extension L/K with $[L : K] \leq n$, and such that the ideal $I\mathcal{O}_L$ of $\mathcal{O}_L$ is principal.

Exercise 1. Let $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z} \smallsetminus \{0,1\}$ is square-free.

(i) Let $q \in \mathbb{N} \smallsetminus \{0\}$. Show that $\mathcal{O}_K$ admits a nonzero principal ideal I such that $\mathrm{N}(I) = q$ if and only if there exist $a, b \in \mathbb{Z}$ such that

$$|a^2 - db^2| = \begin{cases} q & \text{if } d = 2,3 \mod 4, \\ 4q & \text{if } d = 1 \mod 4. \end{cases}$$

(ii) If $d \in \{7, -11\}$, show that $\mathcal{O}_K$ is principal.

(iii) If $d = -6$, show that the ideal class group $\mathcal{C}(\mathcal{O}_K)$ is isomorphic to $\mathbb{Z}/2$.