Exercise 1

Rationalizing the denominator, one calculates

$$\alpha = \frac{3+2\sqrt{6}}{1-\sqrt{6}} = \frac{(3+2\sqrt{6})(1+\sqrt{6})}{(1-\sqrt{6})(1+\sqrt{6})} = \frac{15+5\sqrt{6}}{-5} = -3-\sqrt{6}.$$

According to exercise 2, one has $\mathcal{O}_{\mathbb{Q}(\sqrt{6})} = \mathbb{Z}[\sqrt{6}]$, which α clearly belongs to.

Alternatively, note that $(\alpha+3)^2 = 6$, so α is a root of the normalized integer polynomial $(X+3)^2 - 6$.

Exercise 2

Let

$$\omega := \omega_d := \begin{cases} \sqrt{d} & \text{if } d \equiv 2,3 \bmod 4, \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \bmod 4 \end{cases},$$

so that we want to show $\mathcal{O}_K = \mathbb{Z}[\omega]$. By the lecture (theorem 2.3 in my notes), for "$\supseteq$" one only needs to check that $\omega \in \mathcal{O}_K$. For $d \equiv 2,3 \bmod 4$, ω is a root of $X^2 - d$, for $d \equiv 1 \bmod 4$ one has

$$2\omega = 1+\sqrt{d} \quad \Longleftrightarrow \quad 4\omega^2 = 1+d+2\sqrt{d} = d-1+4\omega,$$

so ω is a root of $X^2 - X - \frac{d-1}{4}$, which has integral coefficients precisely because $d \equiv 1 \bmod 4$.

Now let $\alpha = a+b\sqrt{d}$ be integral over $\mathbb{Z}$, which according to the lecture (2.11) is equivalent to its minimal polynomial μ having integral coefficients. One has

$$\mu = X^2 - \mathrm{Tr}_{K/\mathbb{Q}}(\alpha)X + \mathrm{N}_{K\mathbb{Q}}(\alpha) = X^2 - 2aX + a^2 - db^2.$$

In particular we see $2a \in \mathbb{Z}$. If $a \in \mathbb{Z}$, then $db^2 \in \mathbb{Z}$, which implies $b \in \mathbb{Z}$, for the squarefree d cannot cancel any squared denominator of b. So in this case $\alpha \in \mathbb{Z}[\omega]$.

Now assume $a \notin \mathbb{Z}$, i.e. $a = \frac{x}{2}$ with x odd. Then $b \notin \mathbb{Z}$, but $4(a^2 - db^2) = x^2 - d(2b)^2$ is an integer, and as before we conclude that $2b \in \mathbb{Z}$. So write $b = \frac{y}{2}$ with $y \in \mathbb{Z}$ odd. Now we see

$$0 \equiv 4(a^2 - db^2) = x^2 - dy^2 = 1 - d \bmod 4,$$

so this case can only happen if $d \equiv 1 \bmod 4$. And in this case,

$$\alpha = \frac{x+y\sqrt{d}}{2} = \frac{x-y}{2} + y\omega,$$

where $\frac{x-y}{2} \in \mathbb{Z}$ since both x, y are odd. Hence $\alpha \in \mathbb{Z}[\omega]$ and we are done.

Exercise 3

a) We start with the hint. Let K be a number field and $\varepsilon \in \mathcal{O}_K^\times$. Using the multiplicativity of the norm, we see that

$$1 = \mathrm{N}_{K/\mathbb{Q}}(\varepsilon\varepsilon^{-1}) = \mathrm{N}_{K/\mathbb{Q}}(\varepsilon)\,\mathrm{N}_{K/\mathbb{Q}}(\varepsilon^{-1}),$$

so $\mathrm{N}_{K/\mathbb{Q}}(\varepsilon) \in \mathbb{Z}^\times = \{\pm 1\}$. Conversely, assume that $\mathrm{N}_{K/\mathbb{Q}}(\varepsilon) =: a \in \{\pm 1\}$. Consider

$$1 = a\,\mathrm{N}_{K/\mathbb{Q}}(\varepsilon) = a \prod_{\sigma \in \mathrm{Hom}(K,\overline{\mathbb{Q}})} \sigma\varepsilon = \varepsilon a \prod_{\sigma \neq 1} \sigma\varepsilon.$$

This last product is in K because it equals $(\varepsilon a)^{-1}$, and is integral over $\mathbb{Z}$ because each $\sigma\varepsilon$ has the same minimal polynomial as ε (cf. 2.11). Since $\mathcal{O}_K$ is integrally closed, we have $\prod_{\sigma\neq 1}\sigma\varepsilon \in \mathcal{O}_K$. Hence ε has an inverse in $\mathcal{O}_K$, which is what we wanted to show.

Returning to the exercise, let's first consider the case $d \equiv 2, 3 \bmod 4$. Let $\alpha = a + b\sqrt{d} \in \mathcal{O}_K^\times$. Then $\pm 1 = \mathrm{N}_{K/\mathbb{Q}}(\alpha) = a^2 - db^2$ is a sum of squares, so must equal 1. This implies ($a^2 = 1$ and $bd^2 = 0$) or ($a^2 = 0$ and $bd^2 = 1$). The latter case can only happen if $d = -1$, in which case we see $\mathcal{O}_K^\times = \{\pm 1, \pm i\}$, for all other d we have $\mathcal{O}_K^\times = \{\pm 1\}$.

Now consider $d \equiv 1 \bmod 4$. As before, let $\alpha = a + b\sqrt{d} \in \mathcal{O}_K^\times$, where either $a, b \in \mathbb{Z}$ or $a, b \in \frac{1}{2} + \mathbb{Z}$. Again we have to consider the equation $1 = a^2 - db^2$. If $b = 0$ then $a = \pm 1$. Otherwise, we must have $1 \geq -db^2 \geq -\frac{d}{4}$, i.e. $d \geq -4$, hence $d = -3$. Still, $b^2 \leq \frac{1}{3}$ implies $b = \pm\frac{1}{2}$, which yields $a^2 = \frac{1}{4}$. Putting everything together, we conclude

$$\mathcal{O}_K^\times = \begin{cases} \{\pm 1, \pm i\} & \text{if } d = -1, \\ \{\omega_6^i \mid i = 0, \ldots, 5\} & \text{if } d = -3, \\ \{\pm 1\} & \text{otherwise.} \end{cases}$$

b) It suffices to provide infinitely many units in each case. For $d = 2$ consider $\alpha_n = (1 + \sqrt{2})^n$ for $n \geq 1$. These are all units since $\alpha_1(\sqrt{2} - 1) = 1$, and are all different from each other since $1 + \sqrt{2} > 1$, so $(1 + \sqrt{2})^n$ diverges to ∞.

Analogously, consider $(\frac{1+\sqrt{5}}{2})^n$ for $d = 5$, with $\frac{1+\sqrt{5}}{2}\frac{\sqrt{5}-1}{2} = 1$.

Exercise 1

$1, \alpha, \alpha^2$ is clearly a bais of $K/\mathbb{Q}$ consisting of integral elements. Thus it suffices to show that $\mathcal{O}_K \subseteq \mathbb{Z}[\alpha]$. In the lecture we calculated $d(1, \alpha, \alpha^2) = -108 = -2^2 \cdot 3^3$ and saw $(\mathcal{O}_K : Z[\alpha])^2 d_K = d(1, \alpha, \alpha^2)$, so $i := (\mathcal{O}_K : Z[\alpha]) \mid 6$. But $i = 2$ or 6 would violate exercise 2, so assume $i = 3$, i.e. $\mathcal{O}_K \subseteq \frac{1}{3}\mathbb{Z}[\alpha]$.

Further note

$$\mathrm{N}_{K/\mathbb{Q}}(a + b\alpha + c\alpha^2) = \det \begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix} = a^3 + 2b^3 + 4c^3 - 6abc.$$

Let $\xi = \frac{1}{3}(a + b\alpha + c\alpha^2) \in \mathcal{O}_K$, with $a, b, c \in \mathbb{Z}$. Subtracting a suitable element of $\mathbb{Z}[\alpha]$, we may assume $a, b, c \in \{0, \pm 1\}$. But then

$$|\mathrm{N}_{K/\mathbb{Q}}(\xi)| \leq \frac{1}{27}(1 + 2 + 4 + 6) < 1,$$

so $\mathrm{N}_{K/\mathbb{Q}}(\xi) = 0$. But this implies $\xi = 0$, since otherwise multiplication with ξ is invertible, so the determinant cannot vanish. Thus $\xi \in \mathbb{Z}[\alpha]$.

Exercise 2

$\det(\sigma_i \alpha_j)$ is a sum of products of the $\sigma_i \alpha_j$, with a sign corresponding to the sign of the corresponding permutation. Write P, N for the sum of terms with positive and negative sign, respectively. Then $d_K = (P - N)^2 = (P + N)^2 - 4PN$. We show that $P + N, PN \in \mathbb{Q}$.

Let G be the Galois group of the normal closure of $K/\mathbb{Q}$. Then for every $\tau \in G$, $\tau\sigma_1, \ldots, \tau\sigma_n$ is a permutation of the σ_i, since $\tau|_K$ is one of them. Therefore, if this permutation is even, we have $\tau P = P$ and $\tau N = N$, or else $\tau P = N$ and $\tau N = P$. In either case, $\tau(P + N) = P + N$ and $\tau(PN) = PN$. By Galois theory, $P + N, PN \in \mathbb{Q}$.

But then $d_K = (P + N)^2 - 4PN \equiv (P + N)^2 \equiv 0, 1 \bmod 4$ is clear.

Exercise 3

We proceed as in the lecture: First note that $x^2 - 3y^2 \equiv 1 \bmod 3$, so $x^2 - 3y^2 \equiv 1, 4, 7, 10 \bmod 12$. Of course there are no primes $\equiv 4, 10 \bmod 12$, and $7 \bmod 12$ is ruled out by $x^2 - 3y^2 \equiv x^2 + y^2 \equiv 0, 1, 2 \bmod 4$. This proves one direction.

For the other, let $p \equiv 1 \bmod 12$ and note (as always) that

$$p = x^2 - 3y^2 = (x - \sqrt{3}y)(x + \sqrt{3}y) = \mathrm{N}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}(x + \sqrt{3}y).$$

From the lecture we know $\mathcal{O}_{\mathbb{Q}(\sqrt{3})} = \mathbb{Z}[\sqrt{3}]$, which we know[1] is an euclidean ring with height function $|\mathrm{N}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}(-)|$, hence factorial. Now we claim that 3 is a square $\bmod p$, since $(\frac{3}{p}) \overset{QR}{=} (\frac{p}{3}) = (\frac{1}{3}) = 1$. So there exists x with $x^2 \equiv 3 \bmod p$, i.e. $p \mid x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$. But p divides neither factor: If, say, $p \mid x - \sqrt{3}$, then applying the algebraic conjugate would yield $p \mid x + \sqrt{3}$, so p would also divide their sum $2x$. Then $12 \equiv 4x^2 \equiv 0 \bmod p$, which contradicts the assumption $p \neq 2, 3$. Therefore p is not a prime element in $\mathbb{Z}[\sqrt{3}]$, hence also not irreducible. Thus there exist nonunits $\alpha, \beta \in \mathbb{Z}[\sqrt{3}]$ with $p = \alpha\beta$, which implies $\mathrm{N}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}(\alpha) = \mathrm{N}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}(\beta) = p$. (Note that the norm cannot be $-p$, because then we had integers with $x^2 - 3y^2 \equiv 11 \bmod 12$, which we ruled out.)

[1] Use division in $\mathbb{Q}(\sqrt{3})$ and round the resulting coefficients to the nearest integers, then the difference (measured in the norm) between the rounded and the "true" quotient is at most $3(\frac{1}{2})^2 < 1$.

Exercise 4

First note that f is irreducible, since it is of degree 3 and $f(\pm 1), f(\pm 2), f(\pm 4) \neq 0$, so f has no roots. Therefore $K/\mathbb{Q}$ has degree 3, and $1, \theta, \theta^2$ is a basis of $K/\mathbb{Q}$. Now we calculate, using $\theta^3 = \theta + 4$

$$\xi \begin{pmatrix} 1 \\ \theta \\ \theta^2 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} \theta + \theta^2 \\ \theta^2 + \theta + 4 \\ \theta^2 + 5\theta + 4 \end{pmatrix} = \underbrace{\frac{1}{2} \begin{pmatrix} 0 & 1 & 1 \\ 4 & 1 & 1 \\ 4 & 5 & 1 \end{pmatrix}}_{=:A} \begin{pmatrix} 1 \\ \theta \\ \theta^2 \end{pmatrix},$$

hence

$$\begin{aligned} \chi_\xi(T) = \det(TE - A) &= \frac{1}{8} \det \begin{pmatrix} 2T & -1 & -1 \\ -4 & 2T-1 & -1 \\ -4 & -5 & 2T-1 \end{pmatrix} \\ &= \frac{1}{8} \Big(2T(2T-1)^2 - 20 - 4 - 8(2T-1) - 5(2T) \Big) \\ &= T^3 - T^2 - 3T - 2. \end{aligned}$$

We know $\chi_\xi(\xi) = 0$, and the minimal polynomial of ξ must have degree 3, since $\xi \in \mathbb{Q}(\theta) \setminus \mathbb{Q}$ must generate an intermediate extension other than $\mathbb{Q}$. But the degree 3 is prime, so $\mathbb{Q}(\xi) = \mathbb{Q}(\theta)$. Hence χ_ξ is the minimal polynomial of ξ.

Now note $\operatorname{Tr}(\theta) = 0$ and $\operatorname{Tr}(2\xi) = 2\operatorname{Tr}(A) = 2 = \operatorname{Tr}(\theta) + \operatorname{Tr}(\theta^2) = \operatorname{Tr}(\theta^2)$, so

$$d(1, \theta, \theta^2) = \det \begin{pmatrix} \operatorname{Tr}(1) & \operatorname{Tr}(\theta) & \operatorname{Tr}(\theta^2) \\ \operatorname{Tr}(\theta) & \operatorname{Tr}(\theta^2) & \operatorname{Tr}(\theta + 4) \\ \operatorname{Tr}(\theta^2) & \operatorname{Tr}(\theta + 4) & \operatorname{Tr}(\theta^2 + 4\theta) \end{pmatrix} = \det \begin{pmatrix} 3 & 0 & 2 \\ 0 & 2 & 12 \\ 2 & 12 & 2 \end{pmatrix} = -428.$$

Now let $M = \langle 1, \theta, \xi \rangle_\mathbb{Z}$, then we have the inclusions $\mathbb{Z}[\theta] \subsetneq M \subseteq \mathcal{O}_K$ (the last one follows from χ_ξ having integral coefficients). From the lecture we know

$$(\mathcal{O}_K : \mathbb{Z}[\theta])^2 d_K \mid d(1, \theta, \theta^2) = -2^2 \cdot 107,$$

so $(\mathcal{O}_K : \mathbb{Z}[\theta]) \leq 2$. Since $(M : \mathbb{Z}[\theta]) \geq 2$, it follows that

$$(\mathcal{O}_K : M) = \frac{(\mathcal{O}_K : \mathbb{Z}[\theta])}{(M : \mathbb{Z}[\theta])} \leq \frac{2}{2} = 1,$$

i.e. $\mathcal{O}_K = M$.

Exercise 1

(i) We have $\mathfrak{b} \subseteq \mathfrak{a}$ if and only if $\mathcal{O} \supseteq \mathfrak{b}\mathfrak{a}^{-1} = \prod \mathfrak{p}^{\mu_\mathfrak{p} - \nu_\mathfrak{p}}$ iff $\mu_\mathfrak{p} - \nu_\mathfrak{p} \geq 0$ iff $\mu_\mathfrak{p} \geq \nu_\mathfrak{p}$.

(ii) Let $\mathfrak{c} := \prod \mathfrak{p}^{\min(\mu_\mathfrak{p}, \nu_\mathfrak{p})}$. By (i) we have $\mathfrak{c} \mid \mathfrak{a}, \mathfrak{b}$. Let $\mathfrak{c}' = \prod \mathfrak{p}^{\upsilon_\mathfrak{p}}$ be any ideal such that $\mathfrak{c}' \mid \mathfrak{a}, \mathfrak{b}$. Again by (i) we have $\upsilon_\mathfrak{p} \leq \mu_\mathfrak{p}, \nu_\mathfrak{p}$, so $\upsilon_\mathfrak{p} \leq \min(\mu_\mathfrak{p}, \nu_\mathfrak{p})$ and $\mathfrak{c}' \mid \mathfrak{c}$. Therefore, $\mathfrak{c}$ is the smallest ideal containing both $\mathfrak{a}, \mathfrak{b}$, i.e. their sum.

(iii) Switch "$\min$" to "$\max$", "$\leq$" to "$\geq$", "smallest" to "biggest" and the order of all divisions in (ii).

Exercise 2

First note that

$$33 + 11\sqrt{-7} = 11(3 + \sqrt{-7}) = (2 + \sqrt{-7})(2 - \sqrt{-7})2(\frac{3 + \sqrt{-7}}{2}) = -\alpha\overline{\alpha}\beta\overline{\beta}^3$$

with $\alpha = 2 + \sqrt{-7}$ and $\beta = \frac{1}{2}(1 + \sqrt{-7})$. One easily checks that these elements are irreducible since they have prime norms 11 and 2, respectively. We claim that this is also the factorization of ideals, i.e. all the principal ideals $(\alpha), (\overline{\alpha}), (\beta), (\overline{\beta})$ are prime.

More generally, if $a \in \mathcal{O}_K$ has prime norm, then $(a) \subseteq \mathcal{O}_K$ is prime. Indeed, let $T_a : \mathcal{O}_K \to \mathcal{O}_K$. We know that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$, so let M_a be a matrix representation of T_a w.r.t. some integral basis of $\mathcal{O}_K$. Then $\mathcal{O}_K/(a) = \operatorname{coker} T_a$, and from linear algebra we know that $|\mathcal{O}_K/(a)| = |\det(M_a)| = |\det(T_a)| = |\operatorname{N}_{K/\mathbb{Q}}(a)|$. A ring with prime many elements is necessarily a field, so (a) is prime, even maximal.

(Alternatively, calculate

$$\mathbb{Z}[\tfrac{1+\sqrt{-7}}{2}]/(\tfrac{1+\sqrt{-7}}{2}) \cong \mathbb{Z}[X]/(X^2 - X + 2, X) \cong \mathbb{Z}/(2^2 - 2 + 2) = \mathbb{F}_2$$

and similarly for the others.)

Exercise 3

The ideals of R correspond bijectively to ideals of $\mathcal{O}$ containing $\mathfrak{a}$. By exercise 1, these are exactly the ideals $\mathfrak{p}^i$ for $i \leq n$. Let $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Then for $i = 0, \ldots, n$, the ideal $\pi^i\mathcal{O} + \mathfrak{p}^n$ contains $\mathfrak{p}^n$, so again it must be of the form $\mathfrak{p}^j$ for some $j \leq n$. We have $\pi^i \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$ (look at the factorization of (a)), so $i = j$. But then $\mathfrak{p}^i/\mathfrak{p}^n = (\pi^i)/\mathfrak{p}^n$ is principal.

Exercise 4

(i) $S^{-1}(\mathfrak{ab})$ is (as a module) generated by elements of the form $\frac{ab}{s}$ with $a \in \mathfrak{a}, b \in \mathfrak{b}, s \in S$. Since $\frac{ab}{s} = \frac{a}{1}\frac{b}{s} \in S^{-1}(\mathfrak{a})S^{-1}(\mathfrak{b})$, this shows one inclusion.

Conversely, for generators $\frac{a}{s}\frac{b}{t} \in S^{-1}(\mathfrak{a})S^{-1}(\mathfrak{b})$ we see $\frac{a}{s}\frac{b}{t} = \frac{ab}{st} \in S^{-1}(\mathfrak{ab})$, since $st \in S$ using the multiplicativity of S.

(ii) Let $\frac{b}{s} \in S^{-1}(R : \mathfrak{a})$ and $\frac{a}{t} \in \mathfrak{a}$. Then $\frac{b}{s}\frac{a}{t} = \frac{ab}{st} \in S^{-1}R$, since $ab \in R$ by definition of $(R : \mathfrak{a})$. Thus $\frac{b}{s} \in (S^{-1}R : S^{-1}\mathfrak{a})$.

Conversely, suppose that $\mathfrak{a} = (\alpha_1, \ldots, \alpha_n)$ is finitely generated[2], and let $y \in (S^{-1}R : S^{-1}\mathfrak{a})$. Then $y \cdot \frac{\alpha_i}{1} \in S^{-1}R$, say $y\alpha_i = \frac{r_i}{s_i}$. Let $s = \prod_{i=1}^n s_i$, then $sy\alpha_i = r_i \prod_{j \neq i} s_j \in R$, i.e. $sy \in (R : \mathfrak{a})$. But then $y = \frac{sy}{s} \in S^{-1}(R : \mathfrak{a})$, as desired.

(iii) Clear.

(iv) Equality is a local property, so we may check

$$\mathfrak{a}_\mathfrak{p}^{-1} = S_\mathfrak{p}^{-1}(\mathfrak{a}^{-1}) \overset{!}{=} S_\mathfrak{p}^{-1}(\mathcal{O} : \mathfrak{a}) = (\mathcal{O}_\mathfrak{p} : \mathfrak{a}_\mathfrak{p})$$

for all maximal ideals $\mathfrak{p}$, where the first equality follows from (i) and the third from (ii). Now $\mathcal{O}_\mathfrak{p}$ is a DVR, in particular a PID, so we may write $\mathfrak{a}_\mathfrak{p} = a_\mathfrak{p}\mathcal{O}_\mathfrak{p}$ for some $a_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}$. Applying (iii) yields

$$(\mathcal{O}_\mathfrak{p} : a_\mathfrak{p}\mathcal{O}_\mathfrak{p}) = \frac{1}{a_\mathfrak{p}}\mathcal{O}_\mathfrak{p}.$$

It only remains to check that $\mathcal{O}_\mathfrak{p} = \mathfrak{a}(\mathcal{O}_\mathfrak{p} : \mathfrak{a}\mathcal{O}_\mathfrak{p}) = a_\mathfrak{p}\mathcal{O}_\mathfrak{p} \cdot \frac{1}{a_\mathfrak{p}}\mathcal{O}_\mathfrak{p}$, which is clear.

[2]Otherwise, the claim is false: Let $R = \mathbb{Z}[s, t, x_n, y_n \mid n \in \mathbb{N}]/(s^n x_n - t y_n)_{n\in\mathbb{N}}$, $S = \langle s \rangle$ and $\mathfrak{a} = (x_1, x_2, \ldots)$. Then $\frac{1}{t} \in (S^{-1}R : S^{-1}\mathfrak{a})$, for $\frac{x_n}{t} = \frac{y}{s^n} \in S^{-1}R$. Suppose $\frac{1}{t} \in S^{-1}(R : \mathfrak{a})$, then there exists n with $\frac{s^n x_i}{t} \in R$ for all i, but this is wrong for $i > n$. Hence $(S^{-1}R : S^{-1}\mathfrak{a}) \not\subseteq S^{-1}(R : \mathfrak{a})$.

Exercise 1

a) Consider the ring morphism $\mathbb{Z} \to \mathrm{End}_{\mathbf{Grp}}(\mathcal{O}_K/\mathfrak{p})$ that sends $n \in \mathbb{Z}$ to the "multiplication by n" map $T_n : \mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_K/\mathfrak{p}$, $a \mapsto na$. Since $p \in \mathfrak{p}$, the image of p under this map is trivial, so it descends to a morphism $\mathbb{F}_p \to \mathrm{End}(\mathcal{O}_K/\mathfrak{p})$. This exactly means that $\mathcal{O}_K/\mathfrak{p}$ is a $\mathbb{F}_p$-vector space. It is finite, since $\mathfrak{p}$ and $\mathcal{O}_K$ are free over $\mathbb{Z}$ of the same rank, hence $\mathrm{N}(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ is a p-power.

b) Applying the multiplicativity of the index to the chain $\mathcal{O}_K \supseteq \mathfrak{p} \supseteq \ldots \supseteq \mathfrak{p}^n$, we have

$$\mathrm{N}(\mathfrak{p}^n) = (\mathcal{O}_K : \mathfrak{p}^n) = (\mathcal{O}_K : \mathfrak{p}) \cdots (\mathfrak{p}^{n-1} : \mathfrak{p}^n).$$

It thus suffices to show that each $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ is a $\mathcal{O}_K/\mathfrak{p}$-vector space of dimension 1, then each of the n factors have cardinality $|\mathcal{O}_K/\mathfrak{p}| = \mathrm{N}(\mathfrak{p})$.

One shows that it is a vector space as in (a), and in the lecture we have seen that $\mathfrak{p}^i/\mathfrak{p}^{i+1} = (\overline{a})$ is a principal ideal of $\mathcal{O}/\mathfrak{p}^{i+1}$, which means that $\overline{a}$ is a basis of $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ as a $\mathcal{O}_K/\mathfrak{p}$-vector space.

c) By the Chinese Remainder Theorem, $\mathrm{N}(\mathfrak{ab}) = \mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{b})$ for coprime ideals $\mathfrak{a}, \mathfrak{b}$. Hence for any ideal $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, we have

$$\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{p}_1^{e_1}) \cdots \mathrm{N}(\mathfrak{p}_r^{e_r}) \overset{(b)}{=} \mathrm{N}(\mathfrak{p}_1)^{e_1} \cdots \mathrm{N}(\mathfrak{p}_r)^{e_r}.$$

From this formula, multiplicativity of the ideal norm is clear.

Exercise 2

$$(\mathfrak{a} + d_1\mathcal{O}_K)(\mathfrak{a} + d_2\mathcal{O}_K) = \underbrace{\mathfrak{a}^2}_{\subseteq \mathfrak{a}} + \mathfrak{a} \cdot \underbrace{(d_1\mathcal{O}_K + d_2\mathcal{O}_K)}_{=\mathcal{O}_k \text{ since } (d_1,d_2)=1} + \underbrace{d_1d_2\mathcal{O}_K}_{\subseteq \mathfrak{a}} = \mathfrak{a}$$

For the counterexample, take $K = \mathbb{Q}$, $d_1, d_2 = 2 \in \mathbb{Z}$ and $\mathfrak{a} = (2)$. Then $d_1d_2 = 4 \in \mathfrak{a}$, but $\mathfrak{a}_i = (2) + (2) = (2)$, so that $\mathfrak{a}_1\mathfrak{a}_2 = (2)(2) = (4) \neq (2) = \mathfrak{a}$.

Exercise 3

a) Let h be the order of $[\mathfrak{a}] \in \mathrm{cl}_K$. Since the class group is finite, one has $h < \infty$. Therefore $0 = [\mathfrak{a}]^h = [\mathfrak{a}^h]$ in cl_K, i.e. $\mathfrak{a}^h$ is a principal ideal.

b) Say $\mathfrak{a}^h = (a)$. In $\mathcal{O}_L$, one still has

$$(\mathfrak{a}\mathcal{O}_L)^h = \mathfrak{a}^h\mathcal{O}_L = a\mathcal{O}_L = \sqrt[h]{a}^h\mathcal{O}_L = (\sqrt[h]{a}\mathcal{O}_L)^h.$$

By uniqueness of prime factorization, this already implies $\mathfrak{a}\mathcal{O}_L = \sqrt[h]{a}\mathcal{O}_L$.

c) Let $h = |\,\mathrm{cl}_K\,|$ and $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ be a system of representatives of cl_K. As in (a), $\mathfrak{a}_i^h$ is principal for all i, say $\mathfrak{a}_i^h = (a_i)$. Then by (b), all the $\mathfrak{a}_i$ become principal in $L = K(\sqrt[h]{a_1}, \ldots, \sqrt[h]{a_h})$.

Let $\mathfrak{b} \in [\mathfrak{a}_i]$ be any ideal of K, then $\mathfrak{b} = x\mathfrak{a}_i$ for some $x \in K^\times$, so that

$$\mathfrak{b}\mathcal{O}_L = x\mathfrak{a}_i\mathcal{O}_L = x\sqrt[h]{a_i}\mathcal{O}_L$$

is principal.

Exercise 4

$1 + \sqrt{-3} \in (2)$ would imply $\frac{1+\sqrt{-3}}{2} \in \mathbb{Z}[\sqrt{-3}]$, which is clearly wrong. So $I \neq (2)$. Now calculate

$$I^2 = (4, 2(1 + \sqrt{-3}), -2 + 2\sqrt{-3}) = (4, 2 + 2\sqrt{-3}) = 2I,$$

where the central equality follows from $-2 + 2\sqrt{-3} = 2(1 + \sqrt{-3}) - 4$.

If one could write I and (2) as products of prime ideals, then $I^2 = 2I$ would imply that $I = (2)$ by removing the prime factors corresponding to I from both sides of the factored equation.

Exercise 1

Let $\mathfrak{p} = \alpha\mathcal{O}_K = \langle 2, \alpha, \alpha^2\rangle_{\mathbb{Z}} \subseteq \mathcal{O}_K = \mathbb{Z}[\alpha]$. Then clearly $\mathfrak{p}^3 = (\alpha\mathcal{O}_K)^3 = \alpha^3\mathcal{O}_K = 2\mathcal{O}_K$, and $\mathfrak{p}$ is prime, since $\mathrm{N}(\mathfrak{p}) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)| = \alpha(\zeta\alpha)(\zeta^2\alpha) = 2$ is. Here, ζ is a primitive third root of unity, so that $\alpha \mapsto \zeta^j\alpha$ induce the embeddings $K \hookrightarrow \mathbb{C}$.

$2, \alpha, \alpha^2$ is clearly a $\mathbb{Z}$-Basis of $\mathfrak{p}$, so their images under $f \circ j$ is a $\mathbb{Z}$-Basis of $\Gamma = f \circ j(\mathfrak{p})$. One calculates

$$\begin{aligned} f(j(2)) &= f(2,2,2) = (2,2,0),\\ f(j(\alpha)) &= f(\alpha, \zeta\alpha, \zeta^2\alpha) = (\alpha, -\tfrac{1}{2}\alpha, \tfrac{\sqrt{3}}{2}\alpha),\\ f(j(\alpha^2)) &= f(\alpha^2, \zeta^2\alpha^2, \zeta\alpha^2) = (\alpha^2, -\tfrac{1}{2}\alpha^2, -\tfrac{\sqrt{3}}{2}\alpha^2). \end{aligned}$$

Hence, by the lecture,

$$\mathrm{Vol}(\Gamma) = 2^1 \det \begin{pmatrix} 2 & \alpha & \alpha^2 \\ 2 & -\frac{1}{2}\alpha & -\frac{1}{2}\alpha^2 \\ 0 & \frac{\sqrt{3}}{2}\alpha & -\frac{\sqrt{3}}{2}\alpha^2 \end{pmatrix} = 12\sqrt{3}.$$

Alternatively, $\mathrm{Vol}(\Gamma) = \sqrt{|d_K|}\,\mathrm{N}(\mathfrak{p}) = 12\sqrt{3}$. These calculations are w.r.t. the inner product $(-,-)$ as defined in the lecture. For the Lebesque measure, divide the result by $2^s = 2$.

Exercise 2

For example, take $\Gamma = \mathbb{Z}^n \subseteq \mathbb{R}^n$ and $X = (-1,1)^n$. Then $\mathrm{Vol}(X) = 2^n$, but X contains no nonzero lattice point.

Now assume that X is compact. For $n \geq 1$, the set $(1+\frac{1}{n})X$ is still centrally symmetric, convex, and of volume $(1+\frac{1}{n})\,\mathrm{Vol}(X) > 2^n\,\mathrm{Vol}(\Gamma)$, so there exists $\gamma_n \in \Gamma \cap (1+\frac{1}{n})X \subseteq \Gamma \cap 2X$. Since $2X$ is compact as well, the sequence $(x_n)_n$ must have a convergent subsequence $x_{n_k} \to x$. Then $x \in \Gamma$ because Γ is discrete, and the sequence (x_{n_k}) is eventually constant. Further, $x \in \bigcap_k (1+\frac{1}{n_k})X = \overline{X} = X$.

Exercise 3

Neukirch, III.2.15.

Exercise 4

Let $t = n(M\,\mathrm{N}(\mathfrak{a}))^{1/n}$ and consider

$$X = \left\{ (z_\tau) \in K_{\mathbb{R}} \,\middle|\, \sum_\tau |z_\tau| \leq t \right\}.$$

Then X is convex, centrally symmetric, compact, and is the closure of the set in exercise 3, so has the same volume

$$\mathrm{Vol}(X) = 2^r\pi^s\frac{n^n}{n!}M\,\mathrm{N}(\mathfrak{a}) = 2^n\sqrt{|d_K|}\,\mathrm{N}(\mathfrak{a}) = 2^n\,\mathrm{Vol}(j(\mathfrak{a})),$$

so by exercise 2 there exists $0 \neq a \in \mathfrak{a}$ such that $\sum_\tau |\tau(a)| \leq t$. Now

$$|\mathrm{N}_{K/\mathbb{Q}}(a)| = \prod_\tau |\tau(a)| \leq \left(\frac{1}{n}\sum_\tau |\tau(a)|\right)^n = \left(\frac{t}{n}\right)^n = M\,\mathrm{N}(\mathfrak{a}).$$

Exercise 1

a) There is no (quadratic) number field with discriminant 11, by the explicit formula, or by Stickelsberger's rule. We'll take 13 instead. For $d_K = 5, 8, 13, -3, -4, -7, -8, -11$ one computes the Minkowski constant

$$M = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|} = \begin{cases} \frac{1}{2}\sqrt{d_K} & \text{if } d_K > 0, \\ \frac{2}{\pi}\sqrt{|d_K|} & \text{otherwise} \end{cases}$$

In all cases but $d_K = -11$, one finds $M < 2$. Hence cl_K is generated by ideals of norm at most 1, but $\mathcal{O}_K$ is the only such ideal. Hence $\mathrm{cl}_K = 1$.

Now let $d_K = -11$, i.e. $K = \mathbb{Q}(\sqrt{-11})$. Then $M \approx 2.11$, so cl_K is generated by ideals of norm at most 2. Hence it suffices to show that no ideal $\mathfrak{a}$ with $\mathrm{N}(\mathfrak{a}) = 2$ exists, then we can conclude as above. Suppose otherwise, then $2 = 0 \in \mathcal{O}_K/\mathfrak{a}$, i.e. $2 \in \mathfrak{a}$. But

$$\mathcal{O}_K/(2) \cong \mathbb{Z}[X]/(X^2 - X + 3)/(2) \cong \mathbb{F}_2[X]/(X^2 + X + 1)$$

is a field, so (2) is maximal. Hence $\mathfrak{a} = (2)$ or $\mathcal{O}_K$, both of which have norm $\neq 2$.

b) As before, we have $M = \frac{2}{\pi}\sqrt{104} \approx 6.5$. By the lecture, it suffices to consider prime ideals in the factorization of $2\mathcal{O}_K, 3\mathcal{O}_K$ and $5\mathcal{O}_K$. Let $\mathfrak{p}_2 = (2, \sqrt{-26})$, $\mathfrak{p}_3 = (3, 1 + \sqrt{-26})$ and $\mathfrak{p}_5 = (5, 2 + \sqrt{-26})$. Then

$$\begin{aligned} \mathfrak{p}_2^2 &= (4, 2\sqrt{-26}, -26) = (2), \\ \mathfrak{p}_3\overline{\mathfrak{p}}_3 &= (9, 27, 3 \pm 3\sqrt{-26}) = (3), \\ \mathfrak{p}_5\overline{\mathfrak{p}}_5 &= (25, 30, 10 \pm 5\sqrt{-26}) = (5). \end{aligned}$$

Thus cl_K is generated by $[\mathfrak{p}_2]$, $[\mathfrak{p}_3] = [\overline{\mathfrak{p}}_3]^{-1}$ and $[\mathfrak{p}_5] = [\overline{\mathfrak{p}}_5]^{-1}$.

Furthermore, $\mathrm{N}_{K/\mathbb{Q}}(1 - \sqrt{26}) = 27$, so it factors as the product of three prime ideals of norm 3. Since $3 \nmid 1 - \sqrt{26}$, this factorization does not include $\mathfrak{p}_3\overline{\mathfrak{p}}_3$, so is either $\mathfrak{p}_3^3$ or $\overline{\mathfrak{p}}_3^3$. Either way, $[\mathfrak{p}_3]^3 = 1$ in cl_K. Similarly, $\mathrm{N}_{K/\mathbb{Q}}(2 + \sqrt{-26}) = 30$, so it factors as $\mathfrak{p}_2\widetilde{\mathfrak{p}}_3\widetilde{\mathfrak{p}}_5$ for some choices $\widetilde{\mathfrak{p}}_i \in \{\mathfrak{p}_i, \overline{\mathfrak{p}}_i\}$. Either way, $[\widetilde{\mathfrak{p}}_5] = [\mathfrak{p}_5]^{\pm 1} \in \langle [\mathfrak{p}_2], [\mathfrak{p}_3] \rangle$.

Therefore, cl_K is generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$, and for $i = 2, 3$, $\mathfrak{p}_i$ has order dividing i. Further they are not principal, because this would imply the existence of an element with norm i, but $x^2 + 26y^2 = i$ has no integral solutions. Hence the order of $\mathfrak{p}_i$ is i, and since those orders are coprime we can immediately conclude

$$\mathrm{cl}_K = \langle [\mathfrak{p}_2], [\mathfrak{p}_3] \rangle = \langle [\mathfrak{p}_2] \rangle \times \langle [\mathfrak{p}_3] \rangle \cong \mathbb{Z}/6\mathbb{Z}.$$

Exercise 2

a) Let $\lambda_0 = \frac{1}{\sqrt{r+s}}(1, \ldots, 1)^t$ and consider $M = (\lambda_0 \mid \Lambda)$ For any fixed i, adding all rows to the i-th row of M turns this row into $(\sqrt{r+s}, 0, \ldots, 0)$, so expanding along this row yields $|\det(M)| = \sqrt{r+s}|\det(\Lambda_{\widehat{i}})| = \sqrt{r+s}R(\eta_1, \ldots, \eta_t)$. Since $|\det(M)|$ does not depend on i, this shows that R is well-defined.

b) Since λ_0 is a unit vector orthogonal to H, by the computation in a) one has $\mathrm{Vol}(\lambda(\langle \eta_1, \ldots, \eta_t \rangle)) = \sqrt{r+s}R(\eta_1, \ldots, \eta_t)$. Thus the result follows from the lecture (full lattice iff volume $\neq 0$, and index = ratio of volumes).

Exercise 3

We have already determined $\mathcal{O}^\times_{\mathbb{Q}(\sqrt{-1})} = \langle i \rangle$ and $\mathcal{O}^\times_{\mathbb{Q}(\sqrt{-3}} = \langle \zeta_6 \rangle$ on sheet 1. For the others, Dirichlet's unit theorem implies $\mathcal{O}_K^\times = \{\pm\varepsilon^n \mid n \in \mathbb{Z}\}$ for a fundamental unit ε. We claim that the fundamental units are given as

d	2	3	5	6	7	29
ε	$1+\sqrt{2}$	$2+\sqrt{3}$	$\frac{1}{2}(1+\sqrt{5})$	$5+2\sqrt{6}$	$8+3\sqrt{7}$	$\frac{1}{2}(5+\sqrt{29})$

By the lecture, these are found as follows: Let (x, y) be the positive solution with smallest x of $x^2 - dy^2 = \pm 4$, preferring the negative solution if both are first solvable at the same time. Then $\frac{1}{2}(x + y\sqrt{d})$ is a fundamental unit. E.g. for $d = 3$, we see that $1^2 \cdot 3 \pm 4$ is not a square, but $2^2 \cdot 3 \pm 4$ is, for the $+$ case. So $(4, 2)$ is the smallest solution, and $\varepsilon = \frac{1}{2}(x + y\sqrt{d}) = 2 + \sqrt{3}$.

Exercise 4

Applying exercise 4, sheet 5 to $\mathfrak{a} = \mathcal{O}_K$ yields $1 \leq M$, i.e. $\sqrt{|d_K|} \geq \frac{n^n}{n!}(\frac{\pi}{4})^s \geq \frac{n^n}{n!}(\frac{\pi}{4})^{n/2} =: a_n$ This sequence satisfies $a_2 = \pi/2 > 1$ and

$$\frac{a_{n+1}}{a_n} = \left(\frac{\pi}{4}\right)^{1/2} \left(\frac{n+1}{n}\right)^n \geq \sqrt{\pi} > 1,$$

since $2 \leq (1 + \frac{1}{n})^n \nearrow e$. Hence a_n is increasing, in particular $a_n \geq a_2 > 1$, thus $d_K > 1$ for all $K/\mathbb{Q}$, $K \neq \mathbb{Q}$.

Exercise 1

For $\mathbb{Z}[\sqrt{d}] \subsetneq \mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \mathcal{O}_K$ we have $\mathfrak{f} = (2)$, so for every $p \neq 2$ we may apply the theorem directly (with $\theta = \sqrt{d}, f = X^2 - d$) and find, as in the $d \equiv 2, 3$ case, that $p\mathcal{O}_K = \mathfrak{p}^2$ is ramified iff $p \mid d$, $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ is split iff $p \nmid d$ and d is a square mod p, and $p\mathcal{O}_K$ is inert otherwise.

Finally, for $p = 2$ we apply the theorem with $\theta = \frac{1+\sqrt{d}}{2}$ and $f = X^2 - X + \frac{d-1}{4}$. Looking at $f \bmod 2$, we see that either f is irreducible, so $2\mathcal{O}_K$ is prime, iff $\frac{d-1}{4}$ is odd iff $d \equiv 5 \bmod 8$, or $f \equiv X(X+1)$ iff $\frac{d-1}{4}$ is even iff $d \equiv 1 \bmod 8$, in which case $2\mathcal{O}_K$ is split.

Exercise 2

Let $\mathfrak{p}\mathcal{O}_M = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ and $\mathfrak{P}_i\mathcal{O}_L = P_{i1}^{g_{i1}} \cdots P_{is_i}^{g_{is_i}}$ be the prime factorizations of $\mathfrak{p}$ and $\mathfrak{P}_i$. Then we have

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{p}\mathcal{O}_M)\mathcal{O}_L = \prod_i \mathfrak{P}_i^{e_i}\mathcal{O}_L = \prod_i (\mathfrak{P}_i\mathcal{O}_L)^{e_i} = \prod_{ij} P_{ij}^{e_i g_{ij}}.$$

Hence the ramification indices are multiplicative. Further

$$[\mathcal{O}_L/P_{ij} : \mathcal{O}_K/\mathfrak{p}] = [\mathcal{O}_L/P_{ij} : \mathcal{O}_M/\mathfrak{P}_i] \cdot [\mathcal{O}_M/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$$

from the degree formula for field extensions, so the intertia degrees are multiplicative as well.

Exercise 3

a) Clearly $\mu_K \supseteq \langle \zeta, -1 \rangle \supsetneq \langle \zeta \rangle$. Let ξ be a generator of μ_K, then ξ is a primitive n-th root of unity for some n with $p \mid n$. But then in partiular $\mathbb{Q}(\xi) \subseteq K$, so $\varphi(n) \mid \varphi(p) = p - 1$. Hence $\varphi(\frac{n}{p}) = 1$, so either $n = p$ or $n = 2p$. Since $\langle \zeta \rangle \neq \mu_K$, $n = 2k$ and μ_K is generated by a $2p$-th root of unity.

b) If $M \subseteq \mathbb{R} \cap K$, it is clearly fixed by τ, so $M \subseteq K^{\langle \tau \rangle}$. Hence $K^+ = K^{\langle \tau \rangle}$. Also $\tau(\zeta + \zeta^{-1}) = \zeta^{-1} + \zeta$, since $\zeta\tau(\zeta) = |\zeta|^2 = 1$. So $\mathbb{Q}(\zeta + \zeta^{-1}) \subseteq K^{\langle \tau \rangle}$. By Galois theory, $K^{\langle \tau \rangle}$ has index 2 in K, and the same is true for $\mathbb{Q}(\zeta + \zeta^{-1})$, since ζ is a root of $T^2 - (\zeta + \zeta^{-1})T + 1$.

c) For any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, we have

$$\left| \sigma\left(\frac{u}{\tau(u)}\right) \right|^2 = \frac{\sigma(u)}{\tau(\sigma(u))} \tau\left(\frac{\sigma(u)}{\tau(\sigma(u))}\right) = \frac{\sigma(u)\tau(\sigma(u))}{\tau(\sigma(u))\tau(\tau(\sigma(u)))} = 1.$$

Thus $\frac{u}{\tau(u)} \in \ker \lambda = \mu_K$.

f is clearly a group homomorphism, so it remains to compute the kernel.

For $u \in \mu_K$, one has $f(u) = u^2\mu_K^2 = \mu_K^2$, and for $u \in \mathcal{O}_{K^+}^\times$, we see $f(u) = \frac{u}{u}\mu_K^2 = \mu_K^2$, so $\mu_K\mathcal{O}_{K^+}^\times \subseteq \ker f$. Conversely, say $u \in \ker f$, i.e. $\frac{u}{\tau(u)} = \varepsilon^2$ for some $\varepsilon \in \mu_K$. But then

$$\frac{u\varepsilon^{-1}}{\tau(u\varepsilon^{-1})} = \varepsilon^2 \cdot \frac{\varepsilon^{-1}}{\varepsilon} = 1,$$

so $u\varepsilon^{-1} \in K^{\langle \tau \rangle} = K^+$, and $u = \varepsilon(u\varepsilon^{-1}) \in \mu_K\mathcal{O}_{K^+}^\times$. (Note that clearly $\mathcal{O}_{K^+}^\times = \mathcal{O}_K^\times \cap K^+$).

d) From c) we see $[\mathcal{O}_K^\times : \mu_K\mathcal{O}_{K^+}^\times] = |\operatorname{im} f| \leq |\mu_K/\mu_K^2|$. By a), the last group is isomorphic to $(\mathbb{Z}/2p\mathbb{Z})/(2\mathbb{Z}/2p\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

Exercise 4

By assumption we have $\mathfrak{P}^s \mid \mathfrak{p}\mathcal{O}_L$, i.e. $\mathfrak{p}\mathcal{O}_L \subseteq \mathfrak{P}^s$. But then $\mathfrak{p} \subseteq \mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K \subseteq \mathfrak{P}^s \cap \mathcal{O}_K \subseteq \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.

Exercise 1

By lemma 1.2.17 we have $d\mathcal{O}_L \subseteq \mathbb{Z}[\theta]$. But this means $d \in \mathfrak{f}$, i.e. $\mathfrak{f} \mid d$.

Exercise 2

$K/\mathbb{Q}$ is Galois with Galois group generated by $\sigma_i : \sqrt{i} \mapsto -\sqrt{i}$, $i = 2, 3$, i.e. $G = \{\mathrm{id}, \sigma_2, \sigma_3, \sigma_2\sigma_3\}$. By Dedekind's theorem, $\mathcal{O}_K^\times$ has rank 3. Further, K contains $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ as subfields, so let $\varepsilon_1 = 1 + \sqrt{2}$ and $\varepsilon_2 = 2 + \sqrt{3}$ be their respective fundamental units. Finally, let $\varepsilon_3 = \sqrt{2} + \sqrt{3}$, which is a unit since $\varepsilon_3(\sqrt{3} - \sqrt{2}) = 1$. We claim that $\langle \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle$ is a subgroup of $\mathcal{O}_K^\times$ of finite index. By a previous exercise, for this it suffices to show $R := R(\varepsilon_1, \varepsilon_2, \varepsilon_3) \neq 0$. We calculate

$$\Lambda = \begin{pmatrix} \lambda(\varepsilon_1) & \lambda(\varepsilon_2) & \lambda(\varepsilon_3) \end{pmatrix} = \begin{pmatrix} \log|1+\sqrt{2}| & \log|2+\sqrt{3}| & \log|\sqrt{2}+\sqrt{3}| \\ \log|1-\sqrt{2}| & \log|2+\sqrt{3}| & \log|\sqrt{3}-\sqrt{2}| \\ \log|1+\sqrt{2}| & \log|2-\sqrt{3}| & \log|\sqrt{2}-\sqrt{3}| \\ \log|1-\sqrt{2}| & \log|2-\sqrt{3}| & \log|\sqrt{2}+\sqrt{3}| \end{pmatrix}$$

Removing, say, the last row, we then obtain

$$\begin{aligned} \pm R &= \det \begin{pmatrix} \log(1+\sqrt{2}) & \log(2+\sqrt{3}) & \log(\sqrt{2}+\sqrt{3}) \\ \log(\sqrt{2}-1) & \log(2+\sqrt{3}) & \log(\sqrt{3}-\sqrt{2}) \\ \log(1+\sqrt{2}) & \log(2-\sqrt{3}) & \log(\sqrt{3}-\sqrt{2}) \end{pmatrix} \\ &\overset{\substack{r_2+r_1 \\ r_3-r_1}}{=} \det \begin{pmatrix} \log(1+\sqrt{2}) & \log(2+\sqrt{3}) & \log(\sqrt{2}+\sqrt{3}) \\ 0 & 2\log(2+\sqrt{3}) & 0 \\ 0 & -2\log(2+\sqrt{3}) & -2\log(\sqrt{2}+\sqrt{3}) \end{pmatrix} \\ &= -4\log(1+\sqrt{2})\log(2+\sqrt{3})\log(\sqrt{2}+\sqrt{3}) \neq 0 \end{aligned}$$

Exercise 4

a) The Minkowski bound is $\sqrt{10} \approx 3.2$. Further $2\mathcal{O}_K = \mathfrak{p}_2^2 = (2, \sqrt{10})^2$ and $3\mathcal{O}_K = \mathfrak{p}_3\overline{\mathfrak{p}}_3$ with $\mathfrak{p}_3 = (3, 1+\sqrt{10})$. Hence cl_K is generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3] = [\overline{\mathfrak{p}}_3]^{-1}$. Note that $\mathrm{N}(2+\sqrt{10}) = 6$, so $(2+\sqrt{10})\mathcal{O}_K = \mathfrak{p}_2\widetilde{\mathfrak{p}_3}$ for some $\widetilde{\mathfrak{p}_3} \in \{\mathfrak{p}_3, \overline{\mathfrak{p}}_3\}$, so $[\mathfrak{p}_3] \in \langle [\mathfrak{p}_2] \rangle$. Finally, $\mathfrak{p}_2$ is not principal, since $x^2 - 10y^2 = 2$ has no solution $\mathrm{mod}5$. Therefore $[\mathfrak{p}_2]$ has order 2, and $\mathrm{cl}_K = \langle [\mathfrak{p}_2] \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Thus $h_K = 2$.

b) The equation $x^2 - 10y^2 = 37$ has no solutions, which one again sees by reducing $\mathrm{mod}5$. For $x^2 - 10y^2 = 31$, a solution is given by $(x, y) = (11, 3)$, in other words $\mathrm{N}(11 + 3\sqrt{10}) = 31$. The normalized fundamental unit of K is $\varepsilon = 3 + \sqrt{10}$, so we see that $\mathrm{N}(\pm\varepsilon^{2n}(11 + 3\sqrt{10})) = 31$ for all n as well, i.e. writing $x + y\sqrt{10} = \pm\varepsilon^{2n}(11 + 3\sqrt{10})$, then (x, y) is a solution of the equation.

We claim that these are all solutions. Indeed, let $x^2 - 10y^2 = \pm 31$. Without loss we may assume $x, y > 0$. Then multiplying $z = (x + y\sqrt{10})$ with ε^{-1}, we obtain a new solution

$$z_1 = (-3x + 10y) + (x - 3y)\sqrt{10}.$$

Now if $y > 5$, then $6y^2 > 31 = x^2 - 10y^2$, i.e. $4y > x$ and $x - 3y < y$. Also $x - 3y > 0$, since $x^2 = 10y^2 \pm 31 > 9y^2$. Therefore repeating this procedure, we can continue until $0 < y \leq 5$, for which we can list all solutions: $(3, 2), (11, 3)$. But note $11 + 3\sqrt{31} = \varepsilon(3 + 2\sqrt{31})$. Therefore every solution of $x^2 - 10y^2 = \pm 31$ with $x, y > 0$ is of the form $(3 + 2\sqrt{31})\varepsilon^n$, $n > 0$, and $\mp$ corresponds exactly to the parity of n, by the multiplicativity of the norm.

Exercise 3

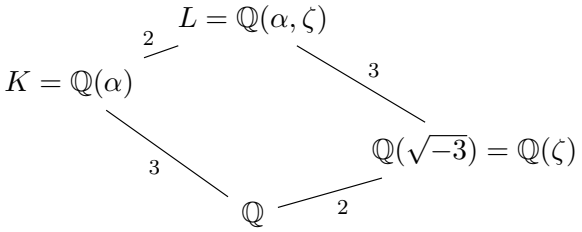
a) The Galois closure of $K = \mathbb{Q}(\alpha)$ is the splitting field of $X^3 - 2 = (X - \alpha)(X - \zeta\alpha)(X - \zeta^2\alpha)$, i.e. $\mathbb{Q}(\alpha, \zeta\alpha, \zeta^2\alpha)$. Since $\zeta = \frac{\zeta\alpha}{\alpha}$, it immediately follows that $\mathbb{Q}(\alpha, \zeta\alpha, \zeta^2\alpha) = \mathbb{Q}(\alpha, \zeta) = L$.

Any element of the Galois group must send α to a root of $X^3 - 2$, i.e. to $\zeta^i\alpha$ for $i = 0, 1, 2$, and ζ to a root of $X^2 + X + 1$, i.e. to ζ or ζ^2. This gives a total of $3 \cdot 2$ possibilities, which equals $[L : \mathbb{Q}]$. Hence $G = \langle \sigma_{i,j} \mid i = 0, 1, 2;\ j = 1, 2 \rangle$, where

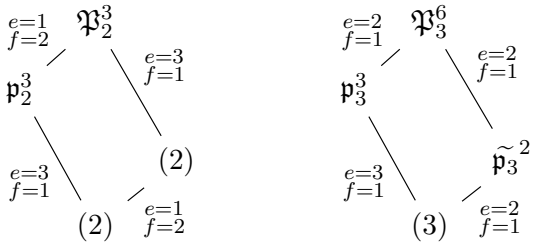
$$\sigma_{i,j} : L \to L, \qquad \alpha \mapsto \zeta^i\alpha, \quad \beta \mapsto \zeta^j.$$

b) First consider $q = 2$. In $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3})$, 2 stays prime since $-3 \equiv 5 \bmod 8$ by the splitting laws in quadratic fields (so $e = 1, f = 2$). In $\mathbb{Q}(\alpha)$ we apply the polynomial decomposition law and see that $X^3 - 2 \equiv X^3 \bmod 2$, so $2\mathcal{O}_K = \mathfrak{p}_2^3$ (i.e. $e = 3, f = 1$). Now if $\mathfrak{P} \mid 2\mathcal{O}_L$, we know $f \geq 2$ and $e \geq 3$, while $ref = 6$. So $r = 1, e = 3, f = 2$ and $2\mathcal{O}_L = \mathfrak{P}_2^3$ for some prime ideal $\mathfrak{P}_2 \subseteq \mathcal{O}_L$. (Explicitly, $\mathfrak{P}_2 = \alpha\mathcal{O}_L$).

For $p = 3$ we argue analogously: Since $X^3 - 2 \equiv (X + 1)^3 \bmod 3$, $3\mathcal{O}_K = \mathfrak{p}_3^3$, and $3 \mid -3$, so $3 = \widetilde{\mathfrak{p}_3}^2$ in $\mathbb{Q}(\sqrt{-3})$. Hence if $\mathfrak{P}_3 \mid 3\mathcal{O}_L$, then it satisfies $2, 3 \mid e$, so $e = 6$ and $3\mathcal{O}_L = \mathfrak{P}_3^6$ for some prime ideal $\mathfrak{P}_3 \subseteq \mathcal{O}_L$. (Explicitly, $\mathfrak{P}_3 = (3, \alpha + 1, \zeta + 2)$.) In diagram form: We consider the field extensions



and get



Furthermore, we have $G_{\mathfrak{P}_2} = G = G_{\mathfrak{P}_3}$, since there is only one prime ideal above 2 resp. 3. Since $f(\mathfrak{P}_3 \mid 3\mathbb{Z}) = 1$, we have $I_{\mathfrak{P}_3} = G_{\mathfrak{P}_3} = G$, and finally, $I_{\mathfrak{P}_2}$ is a subgroup of order $e(\mathfrak{P}_2 \mid 2\mathbb{Z}) = 3$, of which there is only one. Hence $I_{\mathfrak{P}_2} = \{\sigma_{0,1}, \sigma_{1,1}, \sigma_{2,1}\} \cong A_3$

Exercise 1

$K/\mathbb{Q}$ ist abelsch, sodass alle $G_\mathfrak{p}$ für $\mathfrak{p} \mid p$ gleich sind. Wir können diese Gruppe also gefahrlos G_p nennen.In der Vorlesung wurde gezeigt, dass G_p zyklisch ist, und (für $\mathfrak{p} \mid p$) erzeugt wird von dem eindeutigen Element φ mit $\varphi(\alpha) \equiv \alpha^q \bmod \mathfrak{p}$. σ_p erfüllt diese Bedingung (sogar $\bmod p$), also folgt direkt $G_p = \langle \varphi_p \rangle$.

Exercise 2

a) R ist ein euklidischer Ring, also auch ein Hauptidealring und faktoriell. Also kann jedes Element $\alpha \in R$ eindeutig geschrieben werden als $\alpha \sim \prod_f f^{v_f(\alpha)}$, wobei das Produkt über irreduzible normierte Polynome läuft, und $v_f(\alpha) \in \mathbb{Z}$ für fast alle f verschwindet. Für ein Primideal $0 \neq \mathfrak{p} = (f)$ setze nun $v_\mathfrak{p}(\alpha) := v_f(\alpha)$. Die Eigenschaften $v_\mathfrak{p}(\alpha\beta) = v_\mathfrak{p}(\alpha) + v_\mathfrak{p}(\beta)$ und $v_\mathfrak{p}(\alpha + \beta) \geq \min(v_\mathfrak{p}(\alpha), v_\mathfrak{p}(\beta))$ folgen dann wie in der Vorlesung.

Ist $f = X - a$ und $\alpha = \frac{g}{h}$ mit g, h teilerfremd, dann gilt $v_\mathfrak{p}(\alpha) > 0 \iff \alpha(a) = g(a) = 0$ und die Ordnung der Nullstelle ist genau $v_\mathfrak{p}(\alpha)$, und $v_\mathfrak{p}(\alpha) < 0 \iff h(a) = 0$ und die Ordnung des Pols ist genau $-v_\mathfrak{p}$.

b) Seien $\alpha = \frac{f}{g}$. $\beta = \frac{p}{q} \in K^\times$. Dann gilt

$$v_\infty(\tfrac{f}{g}\tfrac{p}{q}) = \deg(gq) - \deg(fp) = \deg(g) + \deg(q) - \deg(f) - \deg(p) = v_\infty(\tfrac{f}{g}) + v_\infty(\tfrac{p}{q}),$$

sowie $\frac{f}{g} + \frac{p}{q} = \frac{fq+gp}{gq}$, also

$$\begin{aligned} v_\infty(\alpha + \beta) &= \deg(gq) - \deg(fq + gp) \\ &\geq \deg(g) + \deg(q) - \max(\deg(f) + \deg(q), \deg(g) + \deg(p)) \\ &= \min(\deg(g) - \deg(f), \deg(q) - \deg(p)) = \min(v_\infty(\alpha), v_\infty(\beta)). \end{aligned}$$

Betrachte $R' = \mathbb{F}_p[\frac{1}{T}] \subseteq K$ und $v_{(1/T)}$ die zu dem Primideal $(\frac{1}{T})$ assoziierte Bewertung wie in (a). Man sieht direkt $v_\infty = v_{(1/T)}$, also entspricht $v_\infty(\alpha)$ der Ordnung der Entwicklung von α "bei ∞".

c) Aufgrund der Multiplikativität der Beträge können wir o.E. $h \in R$ annehmen. Nach Vergleich der Exponenten ist

$$0 = v_\infty(h) + \sum_\mathfrak{p} f_\mathfrak{p} v_\mathfrak{p}(h) \iff \deg(h) = \sum_\mathfrak{p} f_\mathfrak{p} v_\mathfrak{p}$$

zu zeigen, aber das folgt direkt aus der eindeutigen Primfaktorzerlegung.

Exercise 3

$f(x) = x^2 - 2$ erfüllt $f(3) \equiv 0 \bmod p = 7$ und $f'(3) \not\equiv 0 \bmod 7$, also gibt es nach Hensel's Lemma eine Nullstelle in $\mathbb{Z}_7$. Explizit:

Wir konstruieren induktiv eine Lösung in $\mathbb{Z}/p^n\mathbb{Z}$. Angenommen, $x^2 \equiv 2 \bmod p^n$, dann gilt $x^2 \equiv 2 + kp^n \bmod p^{n+1}$ für ein k. Es folgt$(ap^n + x)^2 \equiv 2xap^n + x^2 \equiv 2 + (2xa + k)p^n \bmod p^{n+1}$. Die Gleichung $2xa + k \equiv 0 \bmod p$ ist lösbar, da $2x \neq 0 \bmod p$. Für solches a folgt dann sofort, dass $x' := ap^n + x$ eine Lösung der Gleichung in $\mathbb{Z}/p^n\mathbb{Z}$ ist, und dass $x' \bmod p^n = x$.

Beginnend mit $x = 3$ konstruieren wir so eine Folge $y = (x, x', x'', \ldots)$, die offenbar ein Element von $\mathbb{Z}_p$ ist. Um $y^2 = 2$ zu zeigen, müssen wir dies nur in jedem Faktor überprüfen, wo diese Gleichheit aber nach Konstruktion gilt.

Exercise 4

a) Nach Konstruktion des projektiven Limes genügt es, Gleichheit in jedem Faktor zu überprüfen. Es gilt $\pi_n(p^m a) = p^m \pi_n(a) = p^m a_n + p^n\mathbb{Z}$, also $\pi_n(p^m a) = 0$ für $n \leq m$ und für $n > m$ ist

$$p^m a_n \equiv p^m (a_n \bmod p^{n-m}) \equiv p^m a_{n-m} \mod p^n.$$

b) Aus (a) folgt, dass p^m kein Nullteiler ist. Wie in der Vorlesung zeigt man, dass jedes Element von $\mathbb{Z}_p \setminus \{0\}$ zu einem p^m assoziiert ist. Da Einheiten keine Nullteiler sind, und Produkte von Nicht-Nullteilern wieder Nicht-Nullteiler sind, folgt daraus schon die Behauptung.

Exercise 1

Let $\alpha\mathcal{O}_K = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ be the prime ideal factorization. Then

$$\prod_{\mathfrak{p}\in\mathcal{P}} |\alpha|_\mathfrak{p} = \prod_{i=1}^{r} \mathrm{N}(\mathfrak{q}_i)^{-e_i} = \mathrm{N}(\alpha\mathcal{O}_K)^{-1} = |\,\mathrm{N}_{K/\mathbb{Q}}(\alpha)|^{-1},$$

while

$$\prod_{\mathfrak{p}\in\mathcal{P}_\infty} |\alpha|_\mathfrak{p} = \left|\prod_\rho \rho(\alpha) \prod_\sigma \sigma(\alpha)\overline{\sigma}(\alpha)\right| = \left|\prod_\tau \tau(\alpha)\right| = |\,\mathrm{N}_{K/\mathbb{Q}}(\alpha)|.$$

Hence in total $\prod_{\mathfrak{p}\in\mathcal{P}\cup\mathcal{P}_\infty} |\alpha|_\mathfrak{p} = 1$.

Exercise 2

We first find z_i s.t. $|z_i|_i \approx 1$, and $|z_i|_j \approx 0$ for $i \neq j$, with $i, j \in \{5, 11, \infty\}$. We may take $z_5 = \frac{1}{11^2}$, $z_{11} = \frac{1}{5^2}$ and $z_\infty = 1$. Then by the lecture,

$$x = \sum_i z_i a_i = \frac{1}{11^2} \cdot 1 + \frac{1}{5^2} \cdot 2 + 1 = \frac{3292}{3025}$$

does the trick: Indeed, $|x-1|_5 = |\frac{267}{3025}|_5 = |\frac{3\cdot 89}{5^2\cdot 11^2}|_5 = \frac{1}{25} < \frac{1}{10}$, $|x-2|_{11} = |\frac{-2758}{3025}|_{11} = |\frac{-2\cdot 7\cdot 197}{5^2\cdot 11^2}|_{11} = \frac{1}{121} < \frac{1}{10}$ and $|x-1|_\infty = |\frac{267}{3025}|_\infty < \frac{1}{10}$.

Exercise 3

Let $\alpha \in \mathbb{Z}$. Since n and p are coprime, for any $k \geq 0$ there exists a solution $a > 0$ to $a \equiv 1 \bmod n$ and $a \equiv \alpha \bmod p^k$. Then a is of the desired form, and $|\alpha - a|_p \leq \frac{1}{p^k}$.

Exercise 4

a) Note that in

$$\binom{bp^n}{i} = \frac{bp^n(bp^n-1)\cdots(bp^n-i+1)}{1\cdot 2\cdots i}$$

we have $v_p(bp^n - k) = \min(v_p(bp^n), v_p(k)) = v_p(k)$ for $1 \leq k \leq i-1$. Hence the p-contribution of all these terms cancel out, and we are left with $v_p(bp^n) - v_p(i) = n - v_p(i)$.

b) It suffices to show that $(\varepsilon^{s_n})_n$ is Cauchy. Then the series converges in $\mathbb{Q}_p$, since $\mathbb{Q}_p$ is complete. Moreover, $1 + p\mathbb{Z}_p$ is a closed multiplicative subgroup, so with ε, all its powers and hence also the limit lie in $1 + p\mathbb{Z}_p$.

Let $\varepsilon = 1 + p\beta$. Then for $n \geq m$

$$|\varepsilon^{s_n} - \varepsilon^{s_m}| = |\varepsilon^{s_m}| \left|\sum_{i=1}^{s_n - s_m} \binom{s_n - s_m}{i} (p\beta)^i\right| = |s_n - s_m||p\beta| \leq \frac{1}{p^{m+1}}.$$

c) Let $\varepsilon, \eta \in 1 + p\mathbb{Z}_p$ and $\alpha, \beta \in \mathbb{Z}_p$. We have to show $\varepsilon^1 = \varepsilon$, $(\varepsilon\eta)^\alpha = \varepsilon^\alpha\eta^\alpha$, $\varepsilon^{\alpha+\beta} = \varepsilon^\alpha\varepsilon^\beta$ and $\varepsilon^{\alpha\beta} = (\varepsilon^\alpha)^\beta$. The first is clear, for the second and third note that the sequences in the definition agree. For the final one, note that by the calculation in b) $\varepsilon^\alpha \bmod p^n$ is already determined by $\varepsilon, \alpha \bmod p^n$. Hence for checking that $\varepsilon^{\alpha\beta} = (\varepsilon^\alpha)^\beta \bmod p^n$, we may reduce everything mod p^n, at which point the result clearly holds.

Exercise 5

a) The equation $x^2 - 3y^2 = 11$ has no solution $\mathrm{mod} 3$, since $11 \equiv 2$ is not a square. However, the mentioned theorem would imply that $x^2 - 3y^2 = 11$ has solutions, since $(\frac{3}{11}) = -(\frac{11}{3}) = 1$ and $\mathbb{Q}(\sqrt{3})$ has class number 1.

b) Let p be an odd prime and $p \nmid d$ be squarefree. Then $|x^2 - dy^2| = p$ is solvable if and only if $(\frac{d}{p}) = 1$ and p splits into principal ideals in $K = \mathbb{Q}(\sqrt{d})$. (Moreover, if $d > 0$ and the fundamental unit of $\mathbb{Q}(\sqrt{d})$ has norm -1, then both $x^2 - dy^2 = \pm 1$ are solvable).

Proof: $|x^2 - dy^2| = p$ iff $\mathrm{N}((x \pm y\sqrt{d})\mathcal{O}_K) = p$. But then these ideals lie above p, so p is split, i.e. $(\frac{d}{p}) = 1$. Conversely, if p splits in K into principal ideals, then generators of these ideals have the correct norm.

Exercise 1

Let L, L' be two extensions of K containing α. Then $\alpha \in LL'$, hence it suffices to check the well-definedness for $L \subseteq L'$. In this case, everything follows immediately from $\mathrm{N}_{L'/K}(\alpha) = \mathrm{N}_{L/K}(\alpha)^{[L':L]}$.

Exercise 2

For $\alpha = \sqrt[m]{p}$ we may take $L = \mathbb{Q}_p(\sqrt[m]{p})$, which is an extension of degree m since $X^m - p \in \mathbb{Z}_p[X]$ is irreducible (Eisenstein). Therefore, $|\sqrt[m]{p}|_p = |\mathrm{N}_{L/\mathbb{Q}_p}(\sqrt[m]{p})|_p^{1/m} = \frac{1}{p}^{1/m}$.

Let $K/\mathbb{Q}_p$ be a finite extension and $\eta \in \mathcal{O}_K^\times$. Then $\mathrm{N}_{K/\mathbb{Q}_p}(\eta) \in \mathbb{Z}_p^\times$, so $|\mathrm{N}_{K/\mathbb{Q}_p}(\eta)|_p = 1$, i.e. $|\eta|_p = 1$.

Let $\alpha = 1 - \zeta_{p^n}$. The minimal polynomial of ζ_{p^n} over $\mathbb{Q}_p$ is Φ_{p^n}, since it is irreducible $\mathrm{mod} p$. We have $\mathrm{N}_{\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p} = \Phi_{p^n}(1) = p$ by induction, hence $|\alpha|_p = \frac{1}{p}^{1/\varphi(p)}$

Exercise 3

By assumption, $g = (X - a)$ is a factor of $\overline{f}$; write $\overline{f} = \overline{g}\overline{h}$. Further, a is not a double root of $\overline{f}$, so $\overline{g}, \overline{h}$ are coprime. Hence by Hensel's lemma we have $f = gh$ with g of degree 1, i.e. $g(X) = X - \alpha$. It satisfies $f(\alpha) = g(\alpha)h(\alpha) = 0$ and $\overline{\alpha} = \overline{-g(0)} = -\overline{g}(0) = a$.

Exercise 4

Let $0 \neq H \subseteq \mathbb{Z}_p$ be a closed subgroup, and let $x \in H$ with $n := v_p(x)$ minimal. Write $x = up^n$ with $u \in \mathbb{Z}_p^\times$. Since multiplication with x is continuous, the inverse image of H under this map is a closed subgroup as well. But this subgroup contains 1, hence $\mathbb{Z}$, hence $\overline{\mathbb{Z}} = \mathbb{Z}_p$. Hence $H = x\mathbb{Z}_p = p^n\mathbb{Z}_p$.