Solutions 2

Dedekind Rings and Lattices

1. Consider the number field $K := \mathbb{Q}(\sqrt{-5})$ and its ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$.
   (a) Show that $(3) = \mathfrak{p}\mathfrak{p}'$ with prime ideals $\mathfrak{p} := (3, 1+\sqrt{-5})$ and $\mathfrak{p}' := (3, 1-\sqrt{-5})$.
   (b) Determine the structure of the ring $\mathcal{O}_K/(3)$.
   (c) Determine the inverse of $\mathfrak{p}$ as a fractional ideal.
   (d) Which powers of the ideal $\mathfrak{p}$ are principal?
   (e) Compute the factorization of (2) into prime ideals.
   (f) Compute the factorization of (5) into prime ideals.
   (g) Compute the factorization of (7) into prime ideals.

Solution:

(a) By definition the ideal $\mathfrak{p}\mathfrak{p}'$ is generated by $3 \cdot 3 = 9$ and $3 \cdot (1 \pm \sqrt{-5})$ and $(1+\sqrt{-5}) \cdot (1-\sqrt{-5}) = 6$. Thus it contains $9-6 = 3$, which in turn divides all other generators; hence $\mathfrak{p}\mathfrak{p}' = (3)$.
Since $1 \pm \sqrt{-5} \notin (3)$, both $\mathfrak{p}$ and $\mathfrak{p}'$ properly contain (3). Therefore the formula $\mathfrak{p}\mathfrak{p}' = (3)$ also implies that both $\mathfrak{p}$ and $\mathfrak{p}'$ are properly contained in $\mathcal{O}_K$. Since $\mathcal{O}_K/(3)$ has order 9, it follows that the factor rings $\mathcal{O}_K/\mathfrak{p}$ and $\mathcal{O}_K/\mathfrak{p}'$ both have order 3. But any ring of order 3 is isomorphic to $\mathbb{F}_3$ and hence a field; which implies that $\mathfrak{p}$ and $\mathfrak{p}'$ are prime ideals.

(b) Since $2 \cdot (1+\sqrt{-5}) + 2 \cdot (1-\sqrt{-5}) - 3 = 1$ lies in $\mathfrak{p} + \mathfrak{p}'$, the ideals $\mathfrak{p}$ and $\mathfrak{p}'$ are coprime. By part (a) and the Chinese Remainder Theorem it follows that $\mathcal{O}_K/(3) \cong \mathcal{O}_K/\mathfrak{p} \times \mathcal{O}_K/\mathfrak{p}' \cong \mathbb{F}_3 \times \mathbb{F}_3$.

(c) The inverse fractional ideal of (3) is $(\frac{1}{3})$; hence (a) implies that $\mathfrak{p}^{-1} = (\frac{1}{3}) \cdot \mathfrak{p}' = (1, \frac{1-\sqrt{-5}}{3})$.

(d) For any principal ideal $\mathfrak{a} = (a + b\sqrt{-5}) \subseteq \mathcal{O}_K$ we have $[\mathcal{O}_K : \mathfrak{a}] = \mathrm{Nm}(\mathfrak{a}) = |\mathrm{Nm}_{K/\mathbb{Q}}(a + b\sqrt{-5})| = a^2 + 5b^2$. For all $a, b \in \mathbb{Z}$ this number is $\neq 3$. Since $[\mathcal{O}_K : \mathfrak{p}] = 3$, it follows that $\mathfrak{p}$ is not principal.
Next, the ideal $\mathfrak{p}^2$ is generated by the elements $3 \cdot 3 = 9$ and $3 \cdot (1+\sqrt{-5})$ and $(1+\sqrt{-5})^2 = -4 + 2\sqrt{-5}$. Thus it also contains the smaller element

$$9 - 3 \cdot (1+\sqrt{-5}) + (-4 + 2\sqrt{-5}) \;=\; 2 - \sqrt{-5}.$$

This obviously divides the third generator, and since $\mathrm{Nm}_{K/\mathbb{Q}}(2-\sqrt{-5}) = (2-\sqrt{-5})\cdot(2+\sqrt{-5}) = 2^2+5 = 9$, it also divides the first generator. Since $3\cdot(1+\sqrt{-5})+3\cdot(2-\sqrt{-5}) = 9$, it therefore also divides the second generator; hence $\mathfrak{p}^2 = (2-\sqrt{-5})$ is principal.

Together this shows that the ideal class of $\mathfrak{p}$ in the class group $\mathrm{Cl}(\mathcal{O}_K)$ has order 2. Therefore $\mathfrak{p}^n$ is principal if and only if n is even.

(e) Since $\mathcal{O}_K \cong \mathbb{Z}[X]/(X^2+5)$ with $\sqrt{-5}$ corresponding to the residue class of X, we have $\mathcal{O}_K/(2) \cong \mathbb{F}_2[X]/(X^2+5)$. Since $X^2+5 = (1+X)^2$ in $\mathbb{F}_2[X]$, it follows that $\mathcal{O}_K/(2) \cong \mathbb{F}_2[X]/(1+X)^2$. This ring has the unique maximal ideal $(1+X)/(1+X)^2$, and the factor ring is $\mathbb{F}_2 \cong \mathbb{F}_2[X]/(1+X) \cong \mathcal{O}_K/\mathfrak{q}$ for $\mathfrak{q} := (2, 1+\sqrt{-5})$. Thus $\mathfrak{q}$ is a prime ideal. The isomorphism $\mathcal{O}_K/(2) \cong \mathbb{F}_2[X]/(1+X)^2$ also shows that $\mathfrak{q}^2$ maps to zero in $\mathcal{O}_K/(2)$; hence $\mathfrak{q}^2 \subseteq (2)$. Since $[\mathcal{O}_K : \mathfrak{q}^2] = [\mathcal{O}_K : \mathfrak{q}]^2 = 2^2 = [\mathcal{O}_K : (2)]$, it follows that $\mathfrak{q}^2 = (2)$.

Note: In the same way as in (d) one can show that $\mathfrak{q}$ is not a principal ideal.

Aliter (using divisibility only): Trial computation shows that $(1+\sqrt{-5})^2 = 2(2-\sqrt{-5})$ is divisible by 2. Thus $1+\sqrt{-5}$ must be divisible by some prime ideal dividing (2), i.e., containing 2, and so the ideal $\mathfrak{q} := (2, 1+\sqrt{-5})$ is also divisible by that prime ideal. On the other hand we have $1+\sqrt{-5} \notin 2\mathbb{Z} \oplus 2\mathbb{Z}\sqrt{-5} = (2)$. Together this implies that $(2) \subsetneqq \mathfrak{q} \subsetneqq \mathcal{O}_K$. Since $[\mathcal{O}_K : (2)] = 4$, it follows that $[\mathcal{O}_K : \mathfrak{q}] = 2$ and that $\mathfrak{q}$ is a maximal ideal. In particular $\mathfrak{q}$ is a prime ideal. Finally, the ideal $\mathfrak{q}^2$ is generated by the elements $2\cdot 2 = 4$ and $2\cdot(1+\sqrt{-5})$ and $(1+\sqrt{-5})^2 = -4+2\sqrt{-5}$. Thus it also contains the element $-4+2\cdot(1+\sqrt{-5})-(-4+2\sqrt{-5}) = 2$. Since that in turn divides all other generators, it follows that $\mathfrak{q}^2 = (2)$.

(f) Since $\sqrt{-5}^2 = -5$, we have $(\sqrt{-5}) = \mathbb{Z}\sqrt{-5} \oplus \mathbb{Z}5$ and so $\mathcal{O}_K/(\sqrt{-5}) \cong \mathbb{F}_5$. As that is a field, the ideal $(\sqrt{-5})$ is a prime ideal. Moreover $(\sqrt{-5})^2 = (-5) = (5)$, and we are done.

(g) Since $\mathcal{O}_K \cong \mathbb{Z}[X]/(X^2+5)$, we have $\mathcal{O}_K/(7) \cong \mathbb{F}_7[X]/(X^2+5) \cong \mathbb{F}_7[X]/((X+3)(X-3))$. This ring has the maximal ideals $\bar{\mathfrak{p}}_1 := (X-3)/(X^2+5)$ and $\bar{\mathfrak{p}}_2 := (X+3)/(X^2+5)$. Therefore $\mathfrak{p}_1|(7)$ and $\mathfrak{p}_2|(7)$ for the prime ideals $\mathfrak{p}_1 := (7, 3-\sqrt{-5})$ and $\mathfrak{p}_2 := (7, 3+\sqrt{-5})$. Since $\bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2 = 0$, it follows that $(7)|\mathfrak{p}_1\mathfrak{p}_2$ and hence $(7) = \mathfrak{p}_1\mathfrak{p}_2$.

2. Let A be a Dedekind domain.

   (a) Show that for any non-zero ideal $\mathfrak{a} \subseteq A$, any ideal of $A/\mathfrak{a}$ is principal.

   (b) Show that every ideal of A is generated by two elements.

Solution: (a) As a preparation write $\mathfrak{a} = \mathfrak{p}_1^{\nu_1}\cdots\mathfrak{p}_n^{\nu_n}$ with distinct prime ideals $\mathfrak{p}_1,\ldots,\mathfrak{p}_n$. Then for each i we have $\mathfrak{p}_i^2 \subsetneqq \mathfrak{p}_i$, so we can choose an element $p_i \in \mathfrak{p}_i^2 \smallsetminus \mathfrak{p}_i$. Also, by the Chinese Remainder Theorem we have

$$A/\mathfrak{p}_1^2\cdots\mathfrak{p}_n^2 \xrightarrow{\sim} A/\mathfrak{p}_1^2 \times \ldots \times A/\mathfrak{p}_n^2.$$

Thus there exists an element $\pi_i \in A$ whose residue class $\pi_i + \mathfrak{p}_1^2 \cdots \mathfrak{p}_n^2$ corresponds to the tuple with entries $1+\mathfrak{p}_j^2$ for $j \neq i$ and entry $p_i+\mathfrak{p}_i^2$ for $j = i$. By construction this element satisfies $\mathrm{ord}_{\mathfrak{p}_j}(\pi_i) = \delta_{ij}$ for each j.

Now consider any ideal of $A/\mathfrak{a}$. We know that this has the form $\mathfrak{b}/\mathfrak{a}$ for an ideal $\mathfrak{b}$ with $\mathfrak{a} \subseteq \mathfrak{b} \subseteq A$. Thus $\mathfrak{b} = \mathfrak{p}_1^{\mu_1} \cdots \mathfrak{p}_n^{\mu_n}$ with exponents $0 \leqslant \mu_i \leqslant \nu_i$. The element $b := \pi_1^{\mu_1} \cdots \pi_n^{\mu_n}$ then satisfies $\mathrm{ord}_{\mathfrak{p}_j}(b) = \mu_j$ for each j. Also, any prime ideal dividing the ideal $\mathfrak{a} + (b)$ also divides $\mathfrak{a}$ and is therefore one of the $\mathfrak{p}_j$, and $\mathrm{ord}_{\mathfrak{p}_j}(\mathfrak{a} + (b)) = \min\{\mathrm{ord}_{\mathfrak{p}_j}(\mathfrak{a}), \mathrm{ord}_{\mathfrak{p}_j}(b)\} = \mu_j$. Thus $\mathfrak{a} + (b) = \mathfrak{p}_1^{\mu_1} \cdots \mathfrak{p}_n^{\mu_n} = \mathfrak{b}$, and so $\mathfrak{b}/\mathfrak{a}$ is generated by the residue class of b, as desired.

(b) Obviously the assertion holds for the zero ideal. For any non-zero ideal $\mathfrak{b} \subseteq A$ choose an element $a \in \mathfrak{b} \smallsetminus \{0\}$; then by part (a) for the ring $A/(a)$ there exists an element $b \in A$ with $\mathfrak{b}/(a) = (b) + (a)/(a)$ and hence $\mathfrak{b} = (b, a)$, as desired.

3. Show that a subgroup Γ of a finite-dimensional $\mathbb{R}$-vector space V is a complete lattice if and only if Γ is discrete and V/Γ is compact.

   Solution: Suppose that Γ is a complete lattice, i.e., that $\Gamma = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_n$ for an $\mathbb{R}$-basis $v_1, \ldots, v_n$ of V. Then we can identify V with $\mathbb{R}^n$ such that $\Gamma = \mathbb{Z}^n$. Then Γ is discrete and we get homeomorphisms $V/\Gamma \cong \mathbb{R}^n/\mathbb{Z}^n \cong (\mathbb{R}/\mathbb{Z})^n \cong (S^1)^n$, which is compact (and Hausdorff).

   Aliter: Then Γ is discrete by definition of the topology of V. Next we have $V = \Phi + \Gamma$ for $\Phi := \{\sum x_i v_i \mid \forall i : 0 \leqslant x_i \leqslant 1\}$. Thus we obtain a continuous surjective map $\Phi \twoheadrightarrow V/\Gamma$. Since Φ is bounded and closed, it is compact; hence its image V/Γ is compact, too.

   Conversely, suppose that Γ is discrete and V/Γ is compact. By a proposition from the lecture, the first condition implies that $\Gamma = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_m$ for $\mathbb{R}$-linearly independent $v_1, \ldots, v_m \in V$. Let $V_1 := \mathrm{span}(v_1, \ldots, v_m)$ and write $V = V_1 \oplus V_2$ for some subspace $V_2 \subseteq V$. Then we obtain a homeomorphism $V/\Gamma \cong V_1/\Gamma \times V_2$, and it follows that $\dim V_2 = 0$, because V/Γ is compact. In conclusion, the lattice Γ is complete.

4. *(Minkowski's theorem on linear forms)* Let

$$L_i(x_1, \ldots, x_n) = \sum_{j=1}^{n} a_{ij} x_j, \qquad i = 1, \ldots, n,$$

   be real linear forms such that $\det(a_{ij}) \neq 0$, and let $c_1, \ldots, c_n$ be positive real numbers such that $c_1 \cdots c_n > |\det(a_{ij})|$. Show that there exist integers $m_1, \ldots, m_n \in \mathbb{Z}$, not all zero, such that for all $i \in \{1, \ldots, n\}$

$$|L_i(m_1, \ldots, m_n)| < c_i.$$

   Hint: Use Minkowski's lattice point theorem.

Solution: Let

$$X := \{\underline{x} \in \mathbb{R}^n \mid \forall i \in \{1, \dots, n\} : |L_i(\underline{x})| < c_i\}.$$

Then X is centrally symmetric, because the L_i are linear. We want to show that $\mathrm{vol}(X) > 2^n$. Consider the matrix $T := (a_{ij})$. Then

$$\begin{aligned} TX &= \{\underline{x} \in \mathbb{R}^n \mid \forall i \in \{1, \dots, n\} : |L_i(T^{-1}\underline{x})| < c_i\} \\ &= \{\underline{x} \in \mathbb{R}^n \mid \forall i \in \{1, \dots, n\} : |x_i| < c_i\} \end{aligned}$$

and thus $\mathrm{vol}(TX) = 2^n c_1 \cdots c_n$. Also $\mathrm{vol}(TX) = |\det(T)| \cdot \mathrm{vol}(X)$ and therefore

$$\mathrm{vol}(X) = 2^n c_1 \cdots c_n \cdot |\det(T)|^{-1},$$

which by assumption is $> 2^n$, as desired. The conclusion then follows using Minkowski's lattice point theorem with the lattice $\mathbb{Z}^n$.

*5. Consider a line $\ell := \mathbb{R} \cdot (1, \alpha)$ in the plane $\mathbb{R}^2$ with an irrational slope $\alpha \in \mathbb{R} \smallsetminus \mathbb{Q}$. Show that for any $\varepsilon > 0$, there are infinitely many lattice points $P \in \mathbb{Z}^2$ of distance $d(P, \ell) < \varepsilon$.

Solution: Consider the linear form $L_1(x_1, x_2) := \frac{1}{\sqrt{1+\alpha^2}} \cdot (x_1 + \alpha x_2)$. Then for any point $P \in \mathbb{R}^2$ we have $|L_1(P)| = d(P, \ell)$. Consider the second linear form $L_2(x_1, x_2) := x_2$. Then L_1 and L_2 are linearly independent, so we can apply Minkowski's theorem on linear forms. For any $c_1 > 0$ choose $c_2 \gg 0$ such that the inequality in Exercise 4 is satisfied. Thus there exists a lattice point $P = (x_1, x_2) \in \mathbb{Z}^2 \smallsetminus \{(0,0)\}$ with $|L_1(P)| < c_1$. Since $\alpha \notin \mathbb{Q}$, we then have $x_1 + \alpha x_2 \neq 0$ and hence $L_1(P) \neq 0$. Therefore $0 < d(P, \ell) < c_1$. Repeating the calculation with $d(P, \ell)$ in place of c_1 yields a second lattice point $P' \in \mathbb{Z}^2 \smallsetminus \{(0,0)\}$ which satisfies $0 < d(P', \ell) < d(P, \ell)$. Iterating this we can thus produce lattice points $P, P', P'', \ldots \in \mathbb{Z}^2 \smallsetminus \{(0,0)\}$ with $c_1 > d(P, \ell) > d(P', \ell) > d(P'', \ell) > \ldots > 0$. The strict inequalities imply that these points are all distinct. Thus there exist infinitely many points $P \in \mathbb{Z}^2 \smallsetminus \{(0,0)\}$ with $d(P, \ell) < c_1$.