Problem sheet 7 Solutions

Problem 1

(a) By linearlity one can easily check that $(a+a', b+b'), (ka, kb) \in \Lambda$ for any $(a,b), (a',b') \in \Lambda$ and $k \in \mathbb{Z}$. It shows that Λ is a subgroup of $\mathbb{Z}^2$. We also observe that Λ is a lattice with a basis $(1,u), (0,p)$. Then the index of Λ in $\mathbb{Z}^2$ is computed by

$$\left| \det \begin{pmatrix} 1 & u \\ 0 & p \end{pmatrix} \right| = p.$$

(b) Similar to (a), Λ is a sublattice of $\mathbb{Z}^4$ by the linearlity of the equations. Any element of Λ can be written in a form of $(a, b, ua+vb+pc', -va+ub+pd') \in \mathbb{Z}^4$, where $a, b, c', d' \in \mathbb{Z}$. Hence, $(1,0,u,-v), (0,1,v,u), (0,0,p,0), (0,0,0,p)$ is a basis of Λ. It follows that the index of Λ in $\mathbb{Z}^2$ is

$$\left| \det \begin{pmatrix} 1 & 0 & u & -v \\ 0 & 1 & v & u \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{pmatrix} \right| = p^2.$$

Problem 2

Let $I_1 = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ be the factorization of I_1, where $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ are distinct maximal ideals and $e_1, \cdots, e_r \geq 1$. We also factorize $I_2 = \mathfrak{q}_1^{f_1} \cdots \mathfrak{q}_s^{f_s}$, where $\mathfrak{q}_1, \cdots, \mathfrak{q}_s$ are distinct maximal ideals and $f_1, \cdots, f_s \geq 1$. Since I_1 and I_2 are coprime, the maximal ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_r, \mathfrak{q}_1, \cdots, \mathfrak{q}_s$ are all distinct. It follows that $J^k = I_1 I_2$ is factorized as $J^k = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \mathfrak{q}_1^{f_1} \cdots \mathfrak{q}_s^{f_s}$, hence $e_1, \cdots, e_r, f_1, \cdots, f_s$ are divided by k. Let $e_i = ke_i'$ and $f_j = kf_j'$ for $1 \leq i \leq r$ and $1 \leq j \leq s$. Then we have $I_1 = J_1^k$ and $I_2 = J_2^k$ for $J_1 = \mathfrak{p}_1^{e_1'} \cdots \mathfrak{p}_r^{e_r'}$ and $J_2 = \mathfrak{q}_1^{f_1'} \cdots \mathfrak{q}_s^{f_s'}$.

Problem 3

(a) Let $K = \mathbb{Q}(\sqrt{3})$. Then $d = 2, r = 1$, and $s = 0$. Note that $1, \sqrt{3}$ is an integral basis of K, and $\Delta[1, \sqrt{3}] = 4 \cdot 3 = 12$. We calculate the Minkowski bound:

$$c = \frac{2!}{4}\sqrt{12} \approx 1.732.$$

By Theorem 6.41, every ideal class contains an ideal with norm 1, i.e, $h(K) = 1$.

Let $K = \mathbb{Q}(\sqrt{-3})$. Then $d = 2, r = 0$, and $s = 1$. Note that $1, \tau$ is an integral basis of K, where $\tau = \frac{1+\sqrt{-3}}{2}$, and $\Delta[1, \tau] = 3$. We calculate the Minkowski bound:

$$c = \frac{4}{\pi}\frac{2!}{4}\sqrt{3} \approx 1.102.$$

By Theorem 6.41, every ideal class contains an ideal with norm 1, i.e, $h(K) = 1$.

(b) Let $K = \mathbb{Q}(\sqrt{-11})$. Then $d = 2, r = 0$, and $s = 1$. Note that $1, \tau$ is an integral basis of K, where $\tau = \frac{1+\sqrt{-11}}{2}$, and $\Delta[1, \tau] = 11$. We calculate the Minkowski bound:

$$c = \frac{4}{\pi}\frac{2!}{4}\sqrt{11} \approx 2.111.$$

By Theorem 6.41, every ideal class contains an ideal with norm ≤ 2. Suppose now that $\mathfrak{a}$ has norm 2. Then $\mathfrak{a} | \langle 2 \rangle$, so we shall factorize $\langle 2 \rangle$. Recall that τ is a root of the polynomial $f(t) = t^2 - t + 3$. Applying Dedekind's criterion (Theorem 4.73), $\langle 2 \rangle$ is prime as $f(t) \equiv t^2 + t + 1 (\text{mod } 2)$ is irreducible. Moreover, we have $N(\langle 2 \rangle) = 2^2$, so there are no ideals of norm 2. Thus $h(K) = 1$.

(c) Let $K = \mathbb{Q}(\sqrt{-13})$. Then $d = 2, r = 0$, and $s = 1$. Note that $1, \sqrt{-13}$ is an integral basis of K, $f(t) = t^2 + 13$ is the minimal polynomial of $\sqrt{13}$, and $\Delta[1, \sqrt{-13}] = 4 \cdot 13$. We calculate the Minkowski bound:

$$c = \frac{4}{\pi}\frac{2!}{4}\sqrt{4 \cdot 13} \approx 4.591.$$

The only rational primes $\leq c$ are $2, 3$. We shall factorize $\langle 2 \rangle$ and $\langle 3 \rangle$. Applying Dedekind's criterion (Theorem 4.73), $\langle 3 \rangle$ is prime as $f(t) \equiv t^2 + 1 (\text{mod } 3)$ is irreducible. As $f(t) \equiv t^2 + 2t + 1 = (t+1)^2 (\text{mod } 2)$, we have $\langle 2 \rangle = \mathfrak{p}_2^2$, where $\mathfrak{p}_2 = \langle 2, 1 + \sqrt{-13} \rangle$. Moreover, we have $N(\mathfrak{p}_2) = 2$ and $N(\langle 3 \rangle) = 3^2 > 4$, so $\text{Cl}(K)$ is generated by $\mathfrak{p}_2$. We also know that $\mathfrak{p}_2^2$ is a principal ideal $\langle 2 \rangle$. Therefore $\text{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, which is generated by the class of $\mathfrak{p}_2$.

(d) See Example 6.50.

(e) Let $K = \mathbb{Q}(\sqrt{-65})$. Then $d = 2, r = 0$, and $s = 1$. Note that $1, \sqrt{-65}$ is an integral basis of K, $f(t) = t^2 + 65$ is the minimal polynomial of $\sqrt{-65}$, and $\Delta[1, \sqrt{-65}] = 4 \cdot 65$. We calculate the Minkowski bound:

$$c = \frac{4}{\pi}\frac{2!}{4}\sqrt{4 \cdot 65} \approx 10.265.$$

The only rational primes $\leq c$ are $2, 3, 5, 7$. We shall factorize $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 5 \rangle$, and $\langle 7 \rangle$. We first factorize the minimal polynomial $f(t)$ as follows:

$$f(t) \equiv t^2 + 2t + 1 = (t + 1)^2 (\text{mod } 2),$$

$$f(t) \equiv t^2 - 1 = (t+1)(t-1)(\text{mod } 3),$$
$$f(t) \equiv t^2(\text{mod } 5),$$
$$f(t) \equiv t^2 + 2(\text{mod } 7).$$

Applying Dedekind's criterion (Theorem 4.73), $\langle 7 \rangle$ is prime as $f(t) \equiv t^2 + 2(\text{mod } 7)$ is irreducible, and

$$\langle 2 \rangle = \mathfrak{p}_2^2, \quad \mathfrak{p}_2 = \langle 2, 1 + \sqrt{-65} \rangle,$$
$$\langle 3 \rangle = \mathfrak{p}_3\mathfrak{p}_3', \quad \mathfrak{p}_3, \mathfrak{p}_3' = \langle 3, 1 + \sqrt{-65} \rangle, \langle 3, 1 - \sqrt{-65} \rangle,$$
$$\langle 5 \rangle = \mathfrak{p}_5^2, \quad \mathfrak{p}_5 = \langle 5, \sqrt{-65} \rangle.$$

Moreover, we have $N(\mathfrak{p}_2) = 2$, $N(\mathfrak{p}_3) = N(\mathfrak{p}_3') = 3$, $N(\mathfrak{p}_5) = 5^2$, and $N(\langle 7 \rangle) = 7^2 > c$. As $\mathfrak{p}_3 \sim \mathfrak{p}_3'$, $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$ and $[\mathfrak{p}_5]$.

Now we look for small $a \in \mathbb{Z}$ such that $N(a+\sqrt{-65}) = a^2+65$ only factors of $2, 3$, and 5. By straightforward calculation, we find $N(4 + \sqrt{-65}) = 3^4$ and $N(5+\sqrt{-65}) = 2 \cdot 3^2 \cdot 5$. Since 3 does not divide $\langle 4+\sqrt{-65} \rangle$, $\langle 4+\sqrt{-65} \rangle$ is only divisible by only one of $\mathfrak{p}_3$ or $\mathfrak{p}_3'$. Without loss of generality, let $\mathfrak{p}_3'$ be the factor of $\langle 4 + \sqrt{-65} \rangle$. As $\langle 4 + \sqrt{-65} \rangle$ and $\langle 5 + \sqrt{-65} \rangle$ are coprime, we get the factorization $\langle 5 + \sqrt{-65} \rangle = \mathfrak{p}_2\mathfrak{p}_3^2\mathfrak{p}_5$. It follows that $[\mathfrak{p}_2\mathfrak{p}_3^2\mathfrak{p}_5] = 1$, i.e. $[\mathfrak{p}_5] = [\mathfrak{p}_5^{-1}] = [\mathfrak{p}_2\mathfrak{p}_3^2]$, hence $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$.

Recall $[\mathfrak{p}_2]^2 = [\langle 2 \rangle] = 1$ and $[\mathfrak{p}_3]^4 = [\langle 4 + \sqrt{-65} \rangle] = 1$. As there is no integral solution of $x^2 + 65y^2 = 2$, $\mathfrak{p}_2$ is not principal. As $(\pm 3, 0)$ are the only integral solutions of $x^2 + 65y^2 = 9$, one can also check that $\mathfrak{p}_3^2$ is not principal. Thus, $[\mathfrak{p}_2]$ has order 2 and $[\mathfrak{p}_3]$ has order 4.

We still need to check if $\mathfrak{p}_2\mathfrak{p}_3^2$ is principal. Since there is no integral solution of $x^2 + 65y^2 = 18$, $\mathfrak{p}_2\mathfrak{p}_3^2$ is not principal. Therefore,

$$\mathrm{Cl}(K) \cong \langle [\mathfrak{p}_2] \rangle \times \langle [\mathfrak{p}_3] \rangle \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Problem 4

(a) We saw above (c) of Problem 3 that $h_K = 2$ for $K = \mathbb{Q}(\sqrt{-13})$. Since h_K is not divisible by 3, we may apply Proposition 7.1: if $y^3 = x^2 + 13$ then there exists $n \in \mathbb{Z}$ such that $x = n(n^2 - 3 \cdot 13)$ and $3n^2 = 13 \pm 1$. The only integral solution to these equations are $n = \pm 2$, hence $(x, y) = (\mp 70, \pm 17)$.

(b) One can show that $h_K = 4$ for $K = \mathbb{Q}(\sqrt{-30})$. Again applying Proposition 7.1, if $y^3 = x^2+30$ then there exists $n \in \mathbb{Z}$ such that $3n^2 = 30\pm 1$, which is impossible. Thus there is no integral solution to $y^3 = x^2 + 30$.