Solutions to Exercise Sheet 10

Solution 10.1. *Some computation of class numbers.*

(1) We have $d = 2$, hence $\Delta_K = 4d = 8$, and $M_K = \frac{1}{2}\sqrt{8} = \sqrt{2} < 2$. Therefore every ideal class contains an ideal of norm 1, which must be $\mathcal{O}_K$. It follows that $h_K = 1$.

(2) We have $d = 6$, hence $\Delta_K = 4d = 24$, and $M_K = \frac{1}{2}\sqrt{24} = \sqrt{6} < 3$. Therefore every ideal class contains an ideal of norm 1 or 2. An ideal of norm 1 must be $\mathcal{O}_K$. By Proposition 10.10, since $d \not\equiv 1 \pmod 4$, we have $(2) = \mathfrak{p}^2$ and $\mathfrak{p}$ is the only ideal of norm 2. Therefore every ideal class contains $\mathcal{O}_K$ or $\mathfrak{p}$.

It remains to determine whether $\mathcal{O}_K$ and $\mathfrak{p}$ belong to the same ideal class, or equivalently, whether $\mathfrak{p}$ is a principal ideal. Since $\mathfrak{p}$ is the only ideal of norm 2, if we can find a principal ideal (α) of norm 2, then $\mathfrak{p} = (\alpha)$ is a principal ideal. If we assume $\alpha = a + b\sqrt{6}$, then $N((\alpha)) = |N(\alpha)| = |a^2 - 6b^2|$. Hence $N((\alpha)) = 2$ if and only if $a^2 - 6b^2 = \pm 2$. We observe that $a = 2$ and $b = 1$ satisfy $a^2 - 6b^2 = -2$. Therefore the norm of the principal ideal $(2 + \sqrt{6})$ is 2. By the above analysis we know that $\mathfrak{p} = (2 + \sqrt{6})$ is a principal ideal, hence $\mathcal{O}_K$ and $\mathfrak{p}$ are in the same ideal class. It follows that $h_K = 1$.

(3) We have $d = -13$, hence $\Delta_K = 4d = -52$, and $M_K = \frac{2}{\pi}\sqrt{52} < 5$. Therefore every ideal class contains an ideal of norm 1, 2, 3 or 4. An ideal of norm 1 must be $\mathcal{O}_K$. By Proposition 10.10, since $d \not\equiv 1 \pmod 4$, we have $(2) = \mathfrak{p}^2$ where $\mathfrak{p}$ is the only ideal of norm 2. By Proposition 10.11, since $(\frac{-13}{3}) = (\frac{-1}{3}) = -1$, (3) itself is a prime ideal and there is no ideal of norm 3. By the proof of Theorem 10.7, every ideal of norm 4 must be the product of some prime factors of the principal ideal (4). We realise that $(4) = (2)(2) = \mathfrak{p}^4$, hence the only ideals which divide (4) are $\mathfrak{p}^i$ for $0 \leqslant i \leqslant 4$. Since $N(\mathfrak{p}) = 2$, by Lemma 10.2, the only one among them which has norm 4 is $\mathfrak{p}^2 = (2)$. In other words, the ideal of norm 4 is (2). So we conclude that every ideal class contains an ideal among $\mathcal{O}_K$, $\mathfrak{p}$ and (2).

It is clear that (2) is a principal ideal, hence is in the same ideal class as $\mathcal{O}_K$. We claim that $\mathfrak{p}$ is not a prime ideal. If $\mathfrak{p} = (\alpha)$ for some non-zero $\alpha \in \mathcal{O}_K$, we assume $\alpha = a + b\sqrt{-13}$, then $N((\alpha)) = |N(\alpha)| = |a^2 + 13b^2|$. On the other hand $N((\alpha)) = N(\mathfrak{p}) = 2$, hence $a^2 + 13b^2 = \pm 2$. It is clear that $a^2 + 13b^2 = -2$ has no integer solutions, as the left-hand side is non-negative. It is also easy to see that $a^2 + 13b^2 = 2$ has no integer solutions, since $a^2 \leqslant 2$ implies $a^2 = 0$ or 1, and $13b^2 \leqslant 2$ implies $b^2 = 0$, which cannot add up to 2. We conclude that $\mathfrak{p}$ is not a principal ideal, hence it is not in the same ideal class as $\mathcal{O}_K$. Therefore $h_K = 2$.

Solution 10.2. *Fermats two square problem (revisited).*

(1) Since $p \equiv 1 \pmod 4$, -1 is a quadratic residue modulo p. It follows that there exists some $u \in \mathbb{Z}$, such that $u^2 \equiv -1 \pmod p$; or equivalently, $u^2+1 \equiv 0 \pmod p$.

(2) Assume the fundamental domain is T, then

$$\mathrm{vol}(T) = \left|\det \begin{pmatrix} 1 & 0 \\ u & p \end{pmatrix}\right| = p.$$

(3) The volume of the disk is $\mathrm{vol}(D) = \pi \cdot \frac{3}{2}p = \frac{3}{2}\pi p > 4p = 4\,\mathrm{vol}(T)$. By Theorem 9.11, D contains at least one non-zero point in L, say $(a, b) \in L$. Since a and b are not simultaneously zero, we have $a^2 + b^2 > 0$. On the other hand $(a, b) \in D$ implies $a^2 + b^2 < \frac{3}{2}p < 2p$.

(4) Since $(a, b) \in L$, we have that $(a, b) = m_1(1, u) + m_2(0, p)$ for some $m_1, m_2 \in \mathbb{Z}$. Therefore $a = m_1$ and $b = m_1u + m_2p = ua + pm_2 \equiv ua \pmod p$. It follows that $a^2 + b^2 \equiv a^2 + u^2a^2 = a^2(u^2 + 1) \equiv 0 \pmod p$, where the last congruence is due to part (1).

(5) From part (4) we know that a^2+b^2 is a multiple of p, while within the range given in part (3), the only multiple of p is p itself. Hence $a^2 + b^2 = p$.

Solution 10.3. *Minkowski bound for real quadratic fields.*

(1) The inequality $|xy| \leqslant \frac{1}{4}(|x| + |y|)^2$ is equivalent to $4|xy| \leqslant (|x| + |y|)^2$, which is further equivalent to $(|x| + |y|)^2 - 4|xy| \geqslant 0$. However the left-hand side is $|x|^2 + 2|xy| + |y|^2 - 4|xy| = |x|^2 - 2|xy| + |y|^2 = (|x| - |y|)^2 \geqslant 0$. Hence the inequality holds.

(2) By Proposition 9.14, the volume of the fundamental domain is $\mathrm{vol}(T_I) = N(I)|\Delta_K|^{\frac{1}{2}}$. On the other hand, the volume of the square S is given by $\mathrm{vol}(S) = 2r^2 = 4N(I)|\Delta_K|^{\frac{1}{2}} = 4\,\mathrm{vol}(T_I)$. By Corollary 9.12, S contains at least one non-zero point in L_I.

(3) By part (2) and the definition of L_I in Proposition 9.14, S contains a non-zero point in L_I, which is given by $(a + b\sqrt{d}, a - b\sqrt{d})$ for some non-zero $\alpha = a + b\sqrt{d} \in I$. We write $x = a + b\sqrt{d}$ and $y = a - b\sqrt{d}$, then by the definition of S we have $|x| + |y| \leqslant r$.

(4) For the α chosen in part (3), we have $N(\alpha) = a^2 - b^2d = (a + b\sqrt{d})(a - b\sqrt{d}) = xy$. Hence $|N(\alpha)| = |xy| \leqslant \frac{1}{4}(|x| + |y|)^2 \leqslant \frac{1}{4}r^2 = \frac{1}{2}N(I)|\Delta_K|^{\frac{1}{2}}$, in which the first inequality follows from part (1) and the second inequality follows from part (3).

(5) By Theorem 9.2, the ideal class $\mathcal{C}$ has an inverse in the ideal class group. We denote this inverse ideal class by $\overline{J}$ where J is any representative. Then by part (4) (which is Proposition 10.4), there exists a non-zero element $\beta \in J$ such that $|N(\beta)| \leqslant \frac{1}{2}N(J)\,|\Delta_K|^{\frac{1}{2}}$. Since we have $(\beta) \subseteq J$, there exists some ideal I such that

$IJ = (\beta)$ by Corollary 8.15. Since the ideal class containing (β) is the identity element in the ideal class group, $\overline{I}$ and $\overline{J}$ are inverse of each other, hence I is an ideal in $\mathcal{C}$. It remains to show $N(I)$ satisfies the given bound.

By Lemma 10.2 and Proposition 8.9, we have the following calculation

$$N(I)N(J) = N(IJ) = N((\beta)) = |N(\beta)| \leqslant \frac{1}{2} N(J) \, |\Delta_K|^{\frac{1}{2}} .$$

Since $N(J)$ is a positive integer by Proposition 8.3, we cancel it to get $N(I) \leqslant \frac{1}{2} \, |\Delta_K|^{\frac{1}{2}}$ as required.