Solutions 6

Ideal Class Group

1. (a) Show that the number fields $\mathbb{Q}(\sqrt{11})$ and $\mathbb{Q}(\sqrt{-11})$ have class number 1.
   (b) Show that the class group of $\mathbb{Q}(\sqrt{-14}\,)$ is cyclic of order 4.

Solution: See also Chapter 12.6 in Alaca, Williams [1] to compute the class group.

(a) **Case** $K := \mathbb{Q}(\sqrt{11})$**:** Since $11 \equiv 3 \mod 4$, we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{11}] \cong \mathbb{Z}[X]/(X^2-11)$ and $\operatorname{disc}(\mathcal{O}_K) = 4\cdot 11 = 44$. Since $11 > 0$, the field is real quadratic with $r = 2$ and $s = 0$. By Proposition 4.3.2 from the lecture, every ideal class in $\mathrm{Cl}(\mathcal{O}_K)$ contains an ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ with

$$\operatorname{Norm}(\mathfrak{a}) \;\leqslant\; \left(\frac{2}{\pi}\right)^s \sqrt{|\operatorname{disc}(\mathcal{O}_K)|} \;=\; \sqrt{44} \;=\; 6.6332...$$

Therefore, it suffices to show that all ideals $\mathfrak{a}$ of $\mathcal{O}_K$ of norm $\leqslant 6$ are principal. Recall that for any non-zero ideal $\mathfrak{a} \subset \mathcal{O}_K$ we have $\operatorname{Norm}(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]$. In particular $\operatorname{Norm}(\mathfrak{a}) = 1$ if and only if $\mathfrak{a} = (1)$, which is principal. Moreover, any prime divisor $\mathfrak{p}|\mathfrak{a}$ satisfies $\operatorname{Norm}(\mathfrak{p})|\operatorname{Norm}(\mathfrak{a})$. As any non-zero ideal is a product of prime ideals, it thus suffices to show that every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ of norm $\leqslant 6$ is principal. For any such $\mathfrak{p}$, the norm is the order of the residue field and therefore a prime power.

If $\operatorname{Norm}(\mathfrak{p}) = 2$, then $(2) \subseteq \mathfrak{p}$, and $\mathfrak{p}/(2)$ is an ideal of index 2 of the factor ring $\mathcal{O}_K/(2) \cong \mathbb{F}_2[X]/(X^2+1) = \mathbb{F}_2[X]/(1+X)^2$. Thus $\mathfrak{p}/(2)$ corresponds to the unique maximal ideal $(1+X)$, and so $\mathfrak{p} = (2, 1+\sqrt{11})$. We must show that $\mathfrak{p} = (\alpha)$ for some $\alpha = a + b\sqrt{11} \in \mathcal{O}_K$. Any such α must satisfy $|a^2 - 11b^2| = |\operatorname{Norm}_{K/\mathbb{Q}}(\alpha)| = \operatorname{Norm}((\alpha)) = 2$. A little experimentation shows that the equality $|a^2 - 11b^2| = 2$ holds for $\alpha := 3 + \sqrt{11}$. For this we then in fact have $\operatorname{Norm}((\alpha)) = 2$ and hence $(\alpha) = \mathfrak{p}$. Thus the only ideal of $\mathcal{O}_K$ of norm 2 is principal.

If $\operatorname{Norm}(\mathfrak{p}) = 3$, then likewise $\mathfrak{p}/(3)$ is an ideal of index 3 of $\mathcal{O}_K/(3) \cong \mathbb{F}_3[X]/(X^2+1)$. But since X^2+1 is irreducible in $\mathbb{F}_3[X]$, this factor ring is a field of order 9 and does not possess an ideal of index 3. Thus there exists no ideal of $\mathcal{O}_K$ of norm 3.

If $\operatorname{Norm}(\mathfrak{p}) = 4$, then $(4) \subseteq \mathfrak{p}$. For $\mathfrak{p}$ prime this implies that $(2) \subset \mathfrak{p}$, which by comparing indices implies that $(2) = \mathfrak{p}$. But we have seen above that $\mathcal{O}_K/(2)$ is not a field; hence (2) is not a prime ideal. Thus there is no prime ideal of norm 4.

If $\mathrm{Norm}(\mathfrak{p}) = 5$, then likewise $\mathfrak{p}/(5)$ is an ideal of index 5 of $\mathcal{O}_K/(5) \cong \mathbb{F}_5[X]/(X^2-1) = \mathbb{F}_5[X]/((1+X)(1-X))$. Thus $\mathfrak{p}/(5)$ corresponds to the maximal ideal $(1\pm X)$ and so $\mathfrak{p} = (5, 1\pm\sqrt{11})$ for some choice of sign. We must show that $\mathfrak{p} = (\alpha)$ for some $\alpha = a + b\sqrt{11} \in \mathcal{O}_K$. Any such α must satisfy $|a^2 - 11b^2| = |\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)| = \mathrm{Norm}((\alpha)) = 5$. A little experimentation shows that the equality $|a^2 - 11b^2| = 5$ holds for $\alpha := 4 \mp \sqrt{11} = 5 - (1 \pm \sqrt{11}) \in \mathfrak{p}$. For this we then have $\mathrm{Norm}((\alpha)) = 5$, and comparing indices shows that $(\alpha) = \mathfrak{p}$. Thus every ideal of $\mathcal{O}_K$ of norm 5 is principal.

Finally, there is no prime ideal with $\mathrm{Norm}(\mathfrak{p}) = 6$, because 6 is not a prime power.

Case $K := \mathbb{Q}(\sqrt{-11})$**:** Since $-11 \equiv 1 \mod 4$, we have $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-11}}{2}] \cong \mathbb{Z}[X]/(X^2 - X + 3)$ and $\mathrm{disc}(\mathcal{O}_K) = -11$. Since $\mathbb{Q}(\sqrt{-11})$ does not have any embeddings into $\mathbb{R}$, we have $r = 0$ and $s = 1$. By Proposition 4.3.2 from the lecture, every ideal class in $\mathrm{Cl}(\mathcal{O}_K)$ contains an ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ with

$$\mathrm{Norm}(\mathfrak{a}) \;\leqslant\; \left(\frac{2}{\pi}\right)^s \sqrt{|\,\mathrm{disc}(\mathcal{O}_K)|} \;=\; \frac{2}{\pi} \cdot \sqrt{11} \;=\; 2.1114...$$

Therefore, it suffices to show that all ideals $\mathfrak{a}$ of $\mathcal{O}_K$ of norm $\leqslant 2$ are principal.

Again $\mathrm{Norm}(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}] = 1$ if and only if $\mathfrak{a} = (1)$, which is principal.

If $\mathrm{Norm}(\mathfrak{a}) = 2$, then $(2) \subseteq \mathfrak{a}$, and $\mathfrak{a}/(2)$ is an ideal of index 2 of the factor ring $\mathcal{O}_K/(2) \cong \mathbb{F}_2[X]/(X^2 - X + 3)$. Since $X^2 - X + 3 = X^2 + X + 1$ in $\mathbb{F}_2[X]$ is irreducible, this factor ring is a field of order 4 and does not possess an ideal of index 2. Thus there exists no ideal of $\mathcal{O}_K$ of norm 2, and we are done.

(b) See Example 12.6.4 in [1]. To factor the ideals (2) and (3), instead of using the Legendre symbol, one can do the following: We have $\mathcal{O}_K/(2) \cong \mathbb{F}_2[X]/(X^2)$ with (X) the only prime ideal and hence $(2) = (2, \sqrt{-14})^2$. Similarly, we have $\mathcal{O}_K/(3) \cong \mathbb{F}_3[X]/(X^2 + 2)$ which has the prime ideals $(1 - X)$ and $(1 + X)$. Hence $(3) = (3, 1 + \sqrt{-14}) \cdot (3, 1 - \sqrt{-14})$.

2. (a) Let K be a number field. Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$ and $m \geqslant 1$ an integer such that $\mathfrak{a}^m = (\alpha)$. Let L/K be a finite extension containing an element $\sqrt[m]{\alpha}$ such that $\sqrt[m]{\alpha}^{\,m} = \alpha$. Show that $\mathfrak{a}\mathcal{O}_L = \sqrt[m]{\alpha}\,\mathcal{O}_L$.

(b) Deduce that there is a finite field extension L/K such that for every fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ the ideal $\mathfrak{a}\mathcal{O}_L$ is principal.

Solution:

(a) Since $\mathfrak{a}^m = \alpha\mathcal{O}_K$, it follows that $(\mathfrak{a}\mathcal{O}_L)^m = \mathfrak{a}^m\mathcal{O}_L = \alpha\mathcal{O}_L = \sqrt[m]{\alpha}^{\,m}\mathcal{O}_L = (\sqrt[m]{\alpha}\,\mathcal{O}_L)^m$. Unique factorization of fractional ideals in L now implies that $\mathfrak{a}\mathcal{O}_L = \sqrt[m]{\alpha}\,\mathcal{O}_L$.

(b) Let h be the class number of K and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ denote a system of representatives of the elements of the class group. For each i choose $\alpha_i \in K^\times$ such that $\mathfrak{a}_i^h = (\alpha_i)$ and an element $\sqrt[h]{\alpha_i} \in \bar{K}$ such that $\sqrt[h]{\alpha_i}^{\,h} = \alpha_i$. Set $L := K(\sqrt[h]{\alpha_1}, \ldots, \sqrt[h]{\alpha_h}) \subset \bar{K}$. Then for any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ we have $\mathfrak{a} = \alpha\mathfrak{a}_j$ for some $\alpha \in K^\times$ and some j; hence by (a) we have $\mathfrak{a}\mathcal{O}_L = \alpha\mathfrak{a}_j\mathcal{O}_L = \alpha\sqrt[h]{\alpha_i}\,\mathcal{O}_L$, which is a principal ideal.

3. Consider a prime $p \equiv 3 \bmod (4)$. It is known that the class number of $K := \mathbb{Q}(\sqrt{p}\,)$ is odd. Use this fact to prove that there exist $a, b \in \mathbb{Z}$ such that

$$|a^2 - pb^2| = 2.$$

Hint: Study the ideal $\mathfrak{p} := (2, 1 + \sqrt{p}\,)$.

Solution: We compute

$$\mathfrak{p}^2 = \big(4, 2(1+\sqrt{d}\,), (1+\sqrt{d}\,)^2\big) = \big(4, 2+2\sqrt{d}\,, 1+d+2\sqrt{d}\,\big) = \big(4, 2+2\sqrt{d}\,, d-1\big).$$

Since $d - 1 \equiv 2 \bmod (4)$, this ideal contains the element $\gcd(4, d-1) = 2$. As every generator is divisible by 2, it follows that $\mathfrak{p}^2 = (2)$.

On the one hand this implies that $\mathrm{Nm}(\mathfrak{p})^2 = \mathrm{Nm}((2)) = 4$ and hence $\mathrm{Nm}(\mathfrak{p}) = 2$. On the other hand it implies that the corresponding element $[\mathfrak{p}]$ of the class group $\mathrm{Cl}(\mathcal{O}_K)$ has order dividing 2. As the class number is odd, it follows that this element is trivial. Therefore $\mathfrak{p}$ is a principal ideal.

Now $p \equiv 3 \bmod (4)$ implies that $\mathcal{O}_K = \mathbb{Z}[\sqrt{p}\,]$. Thus there exist integers a, b with $\mathfrak{p} = (a + b\sqrt{p}\,)$. Computing the norm yields

$$2 \;=\; \mathrm{Nm}(\mathfrak{p}) \;=\; |\,\mathrm{Nm}_{K/\mathbb{Q}}(a + b\sqrt{p}\,)| \;=\; |(a + b\sqrt{p}\,)(a - b\sqrt{p}\,)| \;=\; |a^2 - pb^2|.$$

4. Suppose that the equation $y^2 = x^5 - 2$ has a solution with $x, y \in \mathbb{Z}$.

   (a) Determine the ring of integers and the class number of $K := \mathbb{Q}(\sqrt{-2})$.

   (b) Show that y is odd and that the two ideals $(y \pm \sqrt{-2})$ of $\mathcal{O}_K$ are coprime.

   (c) Prove that $y + \sqrt{-2}$ is a 5-th power in $\mathcal{O}_K$.

   (d) Deduce a contradiction, proving that the equation has no integer solution.

Solution: (a) Since $-2 \not\equiv 1 \mod 4$, we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$ and $\mathrm{disc}(\mathcal{O}_K) = -8$. Furthermore, we have $r = 0$ and $s = 1$. To compute the class number of K, we use Minkowski's bound: Every ideal class in $\mathrm{Cl}(\mathcal{O}_K)$ contains an ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ with

$$\mathrm{Norm}(\mathfrak{a}) \leqslant \frac{2}{\pi}\sqrt{8} = 1.8\ldots < 2.$$

Since the only ideal in $\mathcal{O}_K$ with norm 1 is the unit ideal, it follows that the class group is trivial and the class number is 1.

(b) Assume, for contradiction, that y is even. Then $x^5 - 2 = y^2 \equiv 0 \mod 4$. By checking all residue classes in $\mathbb{Z}/4\mathbb{Z}$, the equation $x^5 - 2 \equiv 0 \mod 4$ has no solutions. We obtain a contradiction and hence y is odd.

Next the ideal $(y + \sqrt{-2}) + (y - \sqrt{-2})$ contains the element $2\sqrt{-2}$ and hence its square -8. But it also contains the integer $(y + \sqrt{-2})(y - \sqrt{-2}) = y^2 + 2$, which is odd, because y is odd. Thus it contains 1, and so the ideals $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$ are coprime.

(c) Since the class number is 1, the ring $\mathcal{O}_K$ is a unique factorization domain. Since $x^5 = (y + \sqrt{-2})(y - \sqrt{-2})$, where the factors are coprime, it follows that $y + \sqrt{-2} = u\alpha^5$ for some $\alpha \in \mathcal{O}_K$ and some unit $u \in \mathcal{O}_K^\times$. But here $\mathcal{O}_K^\times = \{\pm 1\}$ has order 2, so we have $u = u^5$ and hence $y + \sqrt{-2} = u^5\alpha^5 = (u\alpha)^5$.

(d) By (c), we can write $y + \sqrt{-2} = (a + b\sqrt{-2})^5$ for some $a, b \in \mathbb{Z}$. The binomial expansion yields

$$y + \sqrt{-2} = (a + b\sqrt{-2})^5 = \big(a^5 - 20a^3b^2 + 20ab^4\big) + \big(5a^4b - 20a^2b^3 + 4b^5\big)\sqrt{-2}.$$

Comparing coefficients shows that $b(5a^4 - 20a^2b^2 + 4b^4) = 1$. This implies that $b = \pm 1$ and hence $5a^4 - 20a^2 + 4 = b$.

If $b = 1$, we have $5a^4 - 20a^2 + 3 = 0$. Thus a^2 is a rational root of the quadratic polynomial $5X^2 - 20X + 3$. But this polynomial has discriminant $(-20)^2 - 4 \cdot 5 \cdot 3 = 20 \cdot 17$, which is not a square in $\mathbb{Q}$, hence it does not possess any rational root.

If $b = -1$, we have $5a^4 - 20a^2 + 5 = 0$. Dividing by 5, we obtain $a^4 - 4a^2 + 1 = 0$. Thus a^2 is a rational root of the quadratic polynomial $X^2 - 4X + 1$. But this polynomial has discriminant 12, which is not a square in $\mathbb{Q}$, hence it does not possess any rational root.

In either case we have obtained a contradiction, proving that $y^2 = x^5 - 2$ has no solutions in $\mathbb{Z}$.

P.S.: Is there a direct proof that does not use algebraic number theory?

*5. Let $d := -p_1 \cdots p_r$ with distinct primes p_i and $K := \mathbb{Q}(\sqrt{d}\,)$. For any $1 \leqslant i \leqslant r$ consider the ideal $\mathfrak{p}_i := (p_i, \sqrt{d}\,)$ of $\mathcal{O}_K$, and for any subset $I \subset \{1, \ldots, r\}$ consider the ideal $\mathfrak{a}_I := \prod_{i \in I} \mathfrak{p}_i$.

(a) Show that $\mathfrak{p}_i^2 = (p_i)$.

(b) Deduce that $\mathfrak{p}_i$ is a maximal ideal above p_i with norm $\mathrm{Nm}(\mathfrak{p}_i) = p_i$.

(c) Show that $\mathfrak{a}_I$ is principal for $I = \{1, \ldots, r\}$.

(d) Show that $\mathfrak{a}_I$ is not principal for any $I \neq \varnothing, \{1, \ldots, r\}$.

(e) Conclude that the class group $\mathrm{Cl}(\mathcal{O}_K)$ contains a subgroup isomorphic to $\mathbb{F}_2^{r-1}$.

Solution:

(a) By definition we have $\mathfrak{p}_i^2 = (p_i, \sqrt{d}\,)^2 = (p_i^2, p_i\sqrt{d}, d)$. Here p_i^2 and d lie in $\mathbb{Z}$ and have greatest common divisor p_i. Thus p_i is a $\mathbb{Z}$-linear combination of p_i^2 and d, so in particular it lies in $\mathfrak{p}_i^2$. Conversely each of the stated generators of $\mathfrak{p}_i^2$ is an $\mathcal{O}_K$-multiple of p_i. Therefore $\mathfrak{p}_i^2 = (p_i)$.

(b) The multiplicativity of the norm and the fact that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank 2 show that

$$\mathrm{Nm}(\mathfrak{p}_i)^2 \;=\; \mathrm{Nm}(\mathfrak{p}_i^2) \;\overset{(a)}{=}\; \mathrm{Nm}((p_i)) \;=\; [\mathcal{O}_K : p_i\mathcal{O}_K] \;=\; p_i^2.$$

Therefore

$$|\mathcal{O}_K/\mathfrak{p}_i| \;=\; [\mathcal{O}_K : \mathfrak{p}_i] \;=\; \mathrm{Nm}(\mathfrak{p}_i) \;=\; p_i.$$

Thus $\mathcal{O}_K/\mathfrak{p}_i$ is a finite ring of prime order p_i and therefore isomorphic to $\mathbb{F}_{p_i}$. As this is a field, the ideal $\mathfrak{p}_i$ is a maximal ideal. Since $p_i = 0$ in $\mathbb{F}_{p_i}$, we must have $p_i\mathbb{Z} \subset \mathfrak{p}_i \cap \mathbb{Z}$. As both are non-zero prime ideals of $\mathbb{Z}$, we have equality, and so $\mathfrak{p}_i$ is a prime ideal above p_i.

For the rest observe that by the multiplicativity of the norm we have

$$\mathrm{Nm}(\mathfrak{a}_I) \;=\; \prod_{i\in I} \mathrm{Nm}(\mathfrak{p}_i) \;\overset{(b)}{=}\; \prod_{i\in I} p_i \;=:\; a_I. \qquad (*)$$

(c) For $I = \{1, \ldots, r\}$ observe first that by construction we have $\sqrt{d} \in \bigcap_{i=1}^r \mathfrak{p}_i$. Here the ideals $\mathfrak{p}_i$ are pairwise coprime by (b); hence $\bigcap_{i=1}^r \mathfrak{p}_i = \prod_{i=1}^r \mathfrak{p}_i = \mathfrak{a}_I$. Therefore $(\sqrt{d}\,) \subset \mathfrak{a}_I$. On the other hand we have $\mathrm{Nm}(\mathfrak{a}_I) = \prod_{i=1}^r p_i = |d|$ by $(*)$ and $\mathrm{Nm}((\sqrt{d}\,)) = |\,\mathrm{Nm}_{K/\mathbb{Q}}(\sqrt{d}\,)| = |d|$. Since moreover we have $\mathrm{Nm}((\sqrt{d}\,)) = [\mathfrak{a}_I : (\sqrt{d}\,)] \cdot \mathrm{Nm}(\mathfrak{a}_I)$, it follows that $\mathfrak{a}_I = (\sqrt{d}\,)$.

(d) Suppose that $I \neq \varnothing, \{1, \ldots, r\}$ and that $\mathfrak{a}_I$ is principal. We distinguish cases.

i. If $d \equiv 2, 3 \bmod (4)$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}\,]$; hence $\mathfrak{a}_I = (a + b\sqrt{d}\,)$ for some $a, b \in \mathbb{Z}$. Then by $(*)$ we have

$$a_I \;=\; \mathrm{Nm}(\mathfrak{a}_I) \;=\; |\,\mathrm{Nm}_{K/\mathbb{Q}}(a + b\sqrt{d}\,)| \;=\; |a^2 - b^2 d| \;=\; a^2 + b^2|d|.$$

Here the right hand side is $\geqslant |d|$ if $b \neq 0$. But $I \neq \{1, \ldots, r\}$ implies that $a_I < |d|$. Thus we must have $b = 0$ and therefore $a_I = a^2$. But by assumption a_I is squarefree and > 1, so we have a contradiction.

ii. If $d \equiv 1 \bmod (4)$, then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$; hence $\mathfrak{a}_I = (a + b\frac{1+\sqrt{d}}{2})$ for some $a, b \in \mathbb{Z}$. Then by $(*)$ we have

$$a_I \;=\; \mathrm{Nm}(\mathfrak{a}_I) \;=\; |\,\mathrm{Nm}_{K/\mathbb{Q}}(a + b\tfrac{1+\sqrt{d}}{2})| \;=\; (a + \tfrac{b}{2})^2 + |d| \cdot (\tfrac{b}{2})^2.$$

Multiplying by 4 yields an equation in integers:

$$4a_I \;=\; (2a+b)^2 + |d| \cdot b^2.$$

Since a_I is squarefree and divides $|d|$, this equation implies that $a_I | 2a+b$. Dividing by a_I thus yields the equation

$$4 \;=\; a_I \cdot (\tfrac{2a+b}{a_I})^2 + \tfrac{|d|}{a_I} \cdot b^2$$

where each factor is an integer. Here by assumption a_I and $\frac{|d|}{a_I}$ are coprime integers > 1; hence their sum is $\geqslant 5$. The equality therefore requires that one of the summands on the right hand side vanishes. As neither a_I nor $\frac{|d|}{a_I}$ is a square, this yields a contradiction in both cases.

(e) The equality in (a) implies that we have a well-defined group homomorphism

$$\mathbb{F}_2^{r-1} \to \mathrm{Cl}(\mathcal{O}_K), \quad (m_i)_i \mapsto \left[\prod_{i=1}^{r-1} \mathfrak{p}_i^{m_i}\right].$$

By (d) its kernel is zero; hence it is injective.

References

[1] S. Alaca, K. S. Williams, *Introductory to Algebraic Number Theory.* Cambridge University Press. 2004.