Solutions to Sheet 11

Exercise 1

Let p be a prime number.

1. Show that there exist $a, b \in \mathbb{Z}$ such that $a^2 + b^2 = -1 \pmod{p}$.
2. For $a, b \in \mathbb{Z}$ as in 1, set
$$\Lambda = \cdots \subset \mathbb{R}^4.$$
Show that Λ is a lattice in R^4 and that $\det \Lambda = p^2$.
3. Show that $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \bmod p$ for all $(x_1, \dots, x_4)^t \in \Lambda$.
4. Use Minkowski's theorem to show that there exist $x_1, \dots, x_4 \in \mathbb{Z}$ such that
$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = p.$$
I.e. every prime number is a sum of four squares. (Hint: The volume of the 4-dimensional unit ball is $\pi^2/4$.)

Solution.

1. If $-1 \in \mathbb{Z}/p\mathbb{Z}$ is a quadratic residue, we are done (choose $a = \sqrt{-1}$ and $b = 0$). Otherwise, we have to show that there exists a solution to $a^2 + 1 \equiv b^2 \bmod p$. This is just a matter of counting. Let $S = \{a^2 | a \in (\mathbb{Z}/p\mathbb{Z})\}$ be the set of squares mod p. Note that $\#S = \frac{p+1}{2}$. Now the sets S and $1 + S$ must meet, as otherwise $p = \#(\mathbb{Z}/p\mathbb{Z}) \geq \#S + \#(1 + S) = p + 1$.

2. It is a lattice because the determinant of the basis vectors is invertible, and this determinant is readily seen to be p^2.

3. If $(x_1, \dots, x_4)^t \in \Lambda$, we can write

$$\begin{aligned} x_1 &= pz_1 + 0z_2 + az_3 + bz_4 \\ x_2 &= 0z_1 + pz_2 + bz_3 + (-a)z_4 \\ x_3 &= 0z_1 + 0z_2 + 1z_3 + 0z_4 \\ x_4 &= 0z_1 + 0z_2 + 0z_3 + 1z_4. \end{aligned}$$

For their squares mod p we obtain

$$\begin{aligned} x_1^2 &= (az_3 + bz_4)^2 = (az_3)^2 + 2abz_3z_4 + (bz_4)^2 \\ x_2^2 &= (bz_3 + (-a)z_4)^2 = (bz_3)^2 - 2abz_3z_4 + (az_4)^2 \\ x_3^2 &= z_3^2 \\ x_4^2 &= z_4^2. \end{aligned}$$

Hence we obtain (again mod p)

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = (z_3 + z_4)(a^2 + b^2 + 1) = 0.$$

4. Write $\|-\|$ fot the 2-norm on $\mathbb{R}^4$. Part 3 has shown that for every $x \in \Lambda$, $\|x\|^2 \in p\mathbb{Z}$. Look at the ball

$$B = \{x \in \mathbb{R}^4 \mid \|x\|^2 < 2p\}.$$

Using the hint one quickly verifies that $\mathrm{vol}(B) = \frac{\pi^2}{2}(2p)^2$. In our situation, Minkowski's bound states that every convex, point symmetric convex set around the origin with volume $> 2^4 \det(\Lambda)$ has non-trivial intersection with Λ. As B satisfies all these assumptions (note that $\mathrm{vol}(B) > 18p^2 > 2^4p^2$), we find some point $x \in \Lambda$ with $0 < \|x\|^2 < 2p$. As $p \mid \|x\|^2$, this implies $\|x\|^2 = p$, and we are done.

Exercise 2

[Continuation of sheet 10, exercise 2] Let $m < 0$ be squarefree and set $K = \mathbb{Q}(\sqrt{m})$.

2. Suppose that $|\Delta_K|$ is not a prime number and $\Delta_K \notin \{-4, -8\}$. Show that $\mathrm{Cl}(K)$ is not trivial.

Solution. The hint (I didn't copy the hint) suggested to look at the smallest prime divisor of Δ_K. So let's do that, and denote it by p. We know that p ramifies in K, i.e., we have $p\mathcal{O}_K = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$. Now assume for sake of contradiction that $\mathrm{Cl}(K)$ is trivial. Then $\mathfrak{p}$ is principal, i.e., $\mathfrak{p} = (a)$ for some $a \in \mathcal{O}_K$. Now $a^2 = p$ (up to a unit), and we find that $a \notin \mathbb{Z}$. Hence part 1 of the exercise (on sheet 10) implies that

$$p = \mathrm{N}_{K/\mathbb{Q}}(a) \geq \frac{\Delta_K}{4} \geq \frac{p^2}{4}.$$

This is only possible if $p \in \{2, 3\}$. In the case $p = 2$ we find $|\Delta_K| \leq 8$, in the case $p = 3$ we find $|\Delta_K| \leq 12$. Now let us look at discriminants in this range. The discriminant values are

$$\{-4, -8, -3, -7, -11\}.$$

The cases $\Delta_K = \{-4, -8\}$ are excluded, the other cases are excluded because they arise from $\mathbb{Q}(\sqrt{m})$ when m is (a negative) prime. So there are simply no possibilities left.

Exercise 3

Compute $\mathrm{Cl}(\mathbb{Q}(10))$. **Solution.** We use Minkowski's bound. It states that every ideal class $C \in \mathrm{Cl}(K)$ contains a prime ideal with norm $\leq M_K$, where

$$M_K = \sqrt{|\Delta|_K}\left(\frac{4}{\pi}\right)^{r_2}\frac{n^n}{n!},$$

where $n = [K : \mathbb{Q}]$ and r_2 is the number of complex embeddings (up to conjugation). In our situation, one quickly verifies $M_{\mathbb{Q}(\sqrt{10})} = \sqrt{10} = 3.1\ldots$. So we only have to understand the primes up until norm 3. All of these prime ideals have to lie above (2) or (3), so we can use Dedekind-Kummer to find them. Note that the minimal polynomial of $\sqrt{10}$ over $\mathbb{Q}$ is $f(T) = T^2 - 10$. This reduces mod 2 to T^2 and mod 3 to $(T+1)(T-1)$. Hence the decompositions are given by

$$2 = \mathfrak{p}_2^2, \quad 3 = \mathfrak{p}_3\mathfrak{p}_3'$$

for prime ideals $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_3' \subset \mathcal{O}_K$. Note that $\mathrm{N}(\mathfrak{p}_2) = 2$, $\mathrm{N}(\mathfrak{p}_3) = \mathrm{N}(\mathfrak{p}_3') = 3$. With Dedekind-Kummer we can also explicitely describe all of those prime ideals, and find that (perhaps after interchanging $\mathfrak{p}_3$ and $\mathfrak{p}_3'$)

$$(1+\sqrt{10}) = \mathfrak{p}_3^2, \quad (2+\sqrt{10}) = \mathfrak{p}_2\mathfrak{p}_3.$$

But now, in $\mathrm{Cl}(K)$ we have the equalities

$$1 = [\mathfrak{p}_2]^2 = [\mathfrak{p}_3][\mathfrak{p}_3'] = [\mathfrak{p}_3]^2,$$

and in particular we find $\#\,\mathrm{Cl}(K) \leq 2$. But one quickly finds that $\mathfrak{p}_2$ is not principal: The equation $2 = \alpha^2$ is not solvable in $\mathcal{O}_K$, as $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \pm 2$ is impossible. Indeed, $\mathrm{N}_{K/\mathbb{Q}}(x + y\sqrt{10}) = x^2 - 10y^2 \not\equiv \pm 2 \bmod 5$ for $x, y \in \mathbb{Z}$ (the only quadratic residues mod 5 are ± 1). So $\#\,\mathrm{Cl}(K) > 1$, this implies $\mathrm{Cl}(K) = \mathbb{Z}/2\mathbb{Z}$, and we are done.

Exercise 4

We denote by $\sqrt{2}$ the positive square root of 2 in $\mathbb{R}$.

1. Supose that $u \in \mathbb{Z}[\sqrt{2}]^\times$ and $1 < u < 1 + \sqrt{2}$. Show that $u = 1$.
2. Deduce that $\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1+\sqrt{2})^k \mid k \in \mathbb{Z}\}$.

Solution.

1. Suppose for sake of contradiction that $(a + b\sqrt{2})(a - b\sqrt{2}) = 1$, with $1 < a + b\sqrt{2} < 1 + \sqrt{2}$. Then we find (using the triangle inequality)

$$2\,|a| \leq \underbrace{\left|a + b\sqrt{2}\right|}_{\leq 1+\sqrt{2}} + \underbrace{\left|a - b\sqrt{2}\right|}_{\leq 1} \leq 2 + \sqrt{2},$$

hence $|a| \leq 1 + \frac{1}{\sqrt{2}}$. One readily verifies that this results in a contradiction.

2. By multiplying with $(1+\sqrt{2})$ suitably often, any positive unit can be reduced to a unit with absolute value in the range $[1, 1+\sqrt{2})$. But the only unit in this range is 1, hence any positive unit is of the form $(1+\sqrt{2})^k$ for $k \in \mathbb{Z}$. The same can be done for negative units, and we find $\mathcal{O}_K^\times = \{\pm(1+\sqrt{2})^k \mid k \in \mathbb{Z}\}$.