# ALGEBRAIC NUMBER THEORY

HOMEWORK 4

(1) Show that $\mathbb{Q}(\sqrt{-65}\,)$ has class group $\simeq (2,4)$ (this is short for $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$).

We first list the prime ideals below the Minkowski bound $\mu_K = \sqrt{-4\cdot 65/3} < 10$:

- $\mathfrak{p}_2 = (2, 1+\sqrt{-65}\,)$ with $\mathfrak{p}^2 = (2)$.
- $\mathfrak{p}_3 = (3, 1+\sqrt{-65}\,)$ and $\mathfrak{p}_3' = (3, 1-\sqrt{-65}\,)$ with $\mathfrak{p}_3\mathfrak{p}_3' = (3)$.
- $\mathfrak{p}_5 = (5, \sqrt{-65}\,)$ with $\mathfrak{p}_5^2 = (5)$.
- $(-65/7) = -1$ shows that there is no prime ideal of norm 7.

Thus every ideal class in $K$ contains one of the following ideals: $(1)$, $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_3'$, $\mathfrak{p}_5$, $\mathfrak{p}_2\mathfrak{p}_3$, $\mathfrak{p}_2\mathfrak{p}_3'$, $\mathfrak{p}_3^2$, $(\mathfrak{p}_3')^2$. We also observe that the ideal classes of $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\mathfrak{p}_5$ generate the class group (here we may omit $\mathfrak{p}_3'$ since $\mathfrak{p}_3' \in [\mathfrak{p}_3]^{-1}$).

Now we need relations. First, $\mathfrak{p}_q$ clearly is not principal for any $q = 2,3,5$, since the smallest nontrivial norm in $\mathcal{O}_K$ is $65 = N(\sqrt{-65}\,)$. This also shows that $\mathfrak{p}_3^2$ and $\mathfrak{p}_3^3$ cannot be principal. On the other hand, $(4+\sqrt{-65}\,) = \mathfrak{p}_3^4$ is principal, so the ideal class $[\mathfrak{p}_3]$ has order 4. Both $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3^2]$ have order 2, but they are different; thus together they generate a group $\langle[\mathfrak{p}_2],[\mathfrak{p}_3]\rangle \simeq \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$. We claim that this is the whole class group. Clearly $\mathfrak{p}_3' \in [\mathfrak{p}_3]^{-1} = [\mathfrak{p}_3]^3$. Moreover, $\mathfrak{p}_5$ generates a class of order 2 and therefore should be in one of the classes $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]^2$ or $[\mathfrak{p}_2][\mathfrak{p}_3]^2$. Since 10 and 45 are not norms, it must be the latter, and in fact $90 = N(5+\sqrt{-65}\,)$; thus $(5-\sqrt{-65}\,) = \mathfrak{p}_2\mathfrak{p}_3^2\mathfrak{p}_5$ shows that $\mathfrak{p}_2\mathfrak{p}_3^2\mathfrak{p}_5 \sim (1)$, i.e., that $\mathfrak{p}_2\mathfrak{p}_3^2 \sim \mathfrak{p}_2\mathfrak{p}_3^2\mathfrak{p}_5^2 \sim \mathfrak{p}_5$.

(2) Show that $\mathbb{Q}(\sqrt{79}\,)$ has class group $\simeq \mathbb{Z}/3\mathbb{Z}$. Here the Gauss bound is $\mu = \sqrt{4\cdot 79/5} < 8$. The list of prime ideals is

- $\mathfrak{p}_2 = (2, 1+\sqrt{79}\,) = (9+\sqrt{79}\,)$,
- $\mathfrak{p}_3 = (3, 1+\sqrt{79}\,)$ and $\mathfrak{p}_3' = (3, 1-\sqrt{79}\,)$,
- $\mathfrak{p}_5 = (5, 2+\sqrt{79}\,)$ and $\mathfrak{p}_5' = (5, 2-\sqrt{79}\,)$,
- $\mathfrak{p}_7 = (7, 3+\sqrt{79}\,)$ and $\mathfrak{p}_7' = (7, 3-\sqrt{79}\,)$.

We already know that $\mathfrak{p}_3$ is not principal. Since $(17+2\sqrt{79}\,) = \mathfrak{p}_1^3$, we find that $[\mathfrak{p}]$ has order 3. Moreover, $\mathfrak{p}_3\mathfrak{p}_3' \sim (1)$, hence $\mathfrak{p}_3' \sim \mathfrak{p}_3^2$.

Next $(8-\sqrt{79}\,) = \mathfrak{p}_3\mathfrak{p}_5$, so $\mathfrak{p}_5 \sim \mathfrak{p}_3^2$ and $\mathfrak{p}_5' \sim \mathfrak{p}_3$. Finally, $(10+\sqrt{79}\,) = \mathfrak{p}_3\mathfrak{p}_7$, hence $\mathfrak{p}_7 \sim \mathfrak{p}_3^2$. This shows that every prime ideal of norm $< 8$ is in one of the classes $[(1)]$, $[\mathfrak{p}_3]$ or $[\mathfrak{p}_3]^2$. Thus $\mathrm{Cl}(K) = \langle[\mathfrak{p}_3]\rangle \simeq \mathbb{Z}/3\mathbb{Z}$.

(3) Show that the class number of $K = \mathbb{Q}(\sqrt{-p}\,)$ for primes $p \equiv 1 \bmod 4$ is even. A group has even order if and only if it has an element of order 2.

We show that $\mathfrak{p} = (2, 1+\sqrt{-p}\,)$ generates an ideal class of order 2. Clearly $\mathfrak{p}$ is not principal since $\mathbb{Z}[\sqrt{-p}\,]$ does not have elements of order 2 for $p \geq 5$. On the other hand, $\mathfrak{p}^2 = (2)$ is principal, hence $[\mathfrak{p}]$ is indeed an element of order 2 in $\mathrm{Cl}(K)$.

(4) Show that the class group of $\mathbb{Q}(\sqrt{-p}\,)$ for primes $p \equiv 1 \bmod 8$ has elements of order 4. 1. There are odd integers $e, f$ with $p = 2e^2 - f^2$.

In fact, primes $p \equiv 1 \bmod 2$ split in $\mathbb{Q}(\sqrt{2}\,)$. Since this field has class number 1 (its Gauss bound is $< 2$), we must have $\pm p = N\pi$ for some $\pi \in \mathbb{Z}[\sqrt{2}\,]$. If $p = N\pi$, then $-p = N(\varepsilon\pi)$, where $\varepsilon = 1+\sqrt{2}$ is the fundamental unit of $Z[\sqrt{2}\,]$. Thus there exist $e, f \in \mathbb{N}$ such that $-p = f^2 - 2e^2$. The congruence $1 \equiv p = 2e^2 - f^2 \bmod 8$ immediately shows that $e$ and $f$ must be odd, and this is what we needed to prove.

2. Now put $\mathfrak{a} = (e, f+\sqrt{-p}\,)$. We claim:

- $\mathfrak{a}^2 = (e^2, f+\sqrt{-p}\,)$.
  In fact,
  $$\begin{aligned}\mathfrak{a}^2 &= (e^2, e(f+\sqrt{-p}\,), (f+\sqrt{-p}\,)^2)\\ &= (e^2, e(f+\sqrt{-p}\,), f^2 + 2f\sqrt{-p} - p)\\ &= (e^2, e(f+\sqrt{-p}\,), 2e^2 + 2f\sqrt{-p} - 2p)\\ &= (e^2, e(f+\sqrt{-p}\,), f\sqrt{-p} - p)\\ &= (e^2, e(f+\sqrt{-p}\,), \sqrt{-p}(f+\sqrt{-p}\,)),\end{aligned}$$
  where we have used that $(e^2, 2) = (1)$. But now $(e(f+\sqrt{-p}\,), \sqrt{-p}(f+\sqrt{-p}\,)) = (f+\sqrt{-p}\,)(e, \sqrt{-p}\,) = (f+\sqrt{-p}\,)$ since $(e,p) = 1$ and therefore $(e, \sqrt{-p}\,) = (1)$. This proves the claim.
- $\mathfrak{a}^2\mathfrak{p} = (f+\sqrt{-p}\,)$, where $\mathfrak{p} = (2, 1+\sqrt{-p}\,)$.
  In fact, since $f \equiv 1 \bmod 2$ we have $\mathfrak{p} = (2, f+\sqrt{-p}\,)$ and thus
  $$\begin{aligned}\mathfrak{a}^2\mathfrak{p} &= (e^2, f+\sqrt{-p}\,)(2, f+\sqrt{-p}\,)\\ &= (2e^2, 2(f+\sqrt{-p}\,), e^2(f+\sqrt{-p}\,), (f+\sqrt{-p}\,)^2)\\ &= (f^2+p, 2(f+\sqrt{-p}\,), e^2(f+\sqrt{-p}\,), (f+\sqrt{-p}\,)^2)\\ &= (f+\sqrt{-p}\,)(f-\sqrt{-p}, 2, e^2, f+\sqrt{-p}\,)\\ &= (f+\sqrt{-p}\,)\end{aligned}$$
  Since the second ideal contains $(e^2, 2) = 1$.

Since $[\mathfrak{p}]$ has order 2, $[\mathfrak{a}]$ has order 4: in fact, $\mathfrak{a}^2 \sim \mathfrak{a}^2\mathfrak{p}^2 \sim \mathfrak{p}$, hence $\mathfrak{a}^4 \sim \mathfrak{p}^2 \sim (1)$. But the order of any element divides the group order, hence $4 \mid h$.