Exercise 6.1

Consider $K := \mathbb{Q}(\sqrt{-10})$.

1. Show that $(2) = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ and find the generators of $\mathfrak{p}$ explicitly.

   Proof. Because $-10 \equiv 2 \mod 4$, the ring of integer of K is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-10}]$. The minimal polynomial of $\sqrt{-10}$ is $X^2 + 10$ and we have

   $$X^2 + 10 \equiv X^2 \mod 2.$$

   Thus, $(2) = (2, \sqrt{-10})^2$. □

2. Prove that the ideal $\mathfrak{p}$ you just found is prime, but not principal. Deduce the order of $[\mathfrak{p}] \in \mathrm{Cl}(K)$ is 2.

   Proof. $(2, \sqrt{-10})$ being prime arises from the theorem that gives the method of computation. Now assume $(2, \sqrt{-10})$ is principal, then there is an $\alpha \in \mathcal{O}_K$ that divides 2. Using the multiplicativity of the norm gives $N(\alpha)$ divides $N(2) = 4$, so $N(\alpha) = 2$, but this is impossible. So 2 is irreducible in $\mathcal{O}_K$ and clearly $\sqrt{-10}$ is not a multiple of 2. Hence the generators do not share a divisor and $(2, \sqrt{-10})$ is principal. Moreover, because $(2, \sqrt{-10})^2 = (2)$ is principal (and all principal ideals are equivalent to (1)), the order of $(2, \sqrt{-10})$ is 2. □

3. Prove that $(3) \subset \mathcal{O}_K$ is prime. Using Minkowski's bound, deduce that $\mathrm{Cl}(K) \simeq \mathbb{Z}/2\mathbb{Z}$.

   Proof. Similarly as in 1., we have

   $$X^2 + 10 \equiv X^2 + 1 \mod 3$$

   which is irreducible in $\mathbb{Z}/3\mathbb{Z}$, so (3) is prime. The Minkowski's bound for K is

   $$M_K = \sqrt{|D_K|}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n} = \sqrt{40}\frac{4}{\pi}\frac{2}{4} = \frac{4\sqrt{10}}{\pi} = 4.03.$$

   So the ideal class group is generated by the prime ideals with norm not exceeding M_K. For a prime ideal $\mathfrak{p}$ where $\mathrm{N}(\mathfrak{p}) < 4$, $\mathfrak{p}$ divides (2) or (3). While 3 is prime, (2) decomposes as $(2) = (2, \sqrt{-10})$. Thus, $\mathrm{Cl}(K)$ is generated by $[(1)]$ and $[(2, \sqrt{-10})]$ and we have $\mathrm{Cl}(K) \simeq \mathbb{Z}/3\mathbb{Z}$. □

6.2

Let K be a number field with ring of integers $\mathcal{O}_K$. Suppose $\mathfrak{p} \subset \mathcal{O}_K$ is nonzero prime ideal and $p \in \mathbb{N}$ a prime number. Denote the numerical norm of some ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ by $N_{K/\mathbb{Q}}$. Show that the following are equivalent.

1. $N_{K/\mathbb{Q}}(\mathfrak{p}) \equiv 0 \mod p$.
2. $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.
3. $\mathfrak{p}$ appears in the factorization of $(p) \subseteq \mathcal{O}_K$ into prime ideals.

Proof. 1. **3.** $\Rightarrow$ **1.** Let $(\mathfrak{p})$ decomposes into $\mathfrak{p}\mathfrak{a}$ where $\mathfrak{p}$ is a prime ideal and $\mathfrak{a}$ is an integral ideal. If $\mathfrak{a}^{-1}$ is a fractional ideal with $\mathfrak{a}\mathfrak{a}^{-1} = (1)$, we have

$$\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) = \mathrm{N}_{K/\mathbb{Q}}((p))\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) = |\mathcal{O}_K/(p)|\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}).$$

Now, $|\mathcal{O}_K/(p)|$ is divisible by p, we have that $N_{K/\mathbb{Q}}(\mathfrak{p}) \equiv 0 \mod p$.

□