## ALGEBRA: HOMEWORK 7

**Problem 1.** Let $K = \mathbb{Q}(\sqrt{-5})$ and $I := (4+\sqrt{-5}, 1+2\sqrt{-5}) \subset \mathcal{O}_K$. Show that $I$ is not a principle ideal and that it is a prime ideal.

*Proof.* Since $-5 \equiv 3 \pmod 4$, $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$.

(1) $I$ is not a principle ideal. Assume $I = (a)$ for some $a = a_1 + a_2\sqrt{-5} \in \mathcal{O}_K$. Since $4+\sqrt{-5}, 3-\sqrt{-5} = 4+\sqrt{-5}-(1+2\sqrt{-5}) \in I$,

$$N_{K/\mathbb{Q}}(a) | N_{K/\mathbb{Q}}(4+\sqrt{-5}) = 21$$
$$N_{K/\mathbb{Q}}(a) | N_{K/\mathbb{Q}}(3-\sqrt{-5}) = 14.$$

So $N(a) = 1$ or $7$, i.e., $a_1^2 + 5a_2^2 = 1$ or $7$. The only possible case is $a_1 = 1, a_2 = 0$, i.e., $a = 1$ and $I = \mathcal{O}_K$. Then there exists $p, q, r, s \in \mathbb{Z}$, such that

$$(4+\sqrt{-5})(p+q\sqrt{-5}) + (1+2\sqrt{-5})(r+s\sqrt{-5}) = 1,$$

i.e.,

$$4p - 5q + r - 10s = 1 \tag{1}$$
$$p + 4q + 2r + s = 0. \tag{2}$$

4*(2)-(1) we have $21q + 7r + 14s = 7(3q + r + 2s) = -1$, contradictory!

(2) $I$ is a prime ideal. Let $I_1 = (4+\sqrt{-5}), I_2 = (3-\sqrt{-5}) \subset I$. Then

$$21 = N(4+\sqrt{-5}) = [\mathcal{O}_K : I_1] = [\mathcal{O}_K : I][I : I_1]$$
$$14 = N(4+\sqrt{-5}) = [\mathcal{O}_K : I_2] = [\mathcal{O}_K : I][I : I_2].$$

So $[\mathcal{O}_K : I] | 7$. Since $I \neq \mathcal{O}_K$, $[\mathcal{O}_K : I] = 7$. For any ideal $I'$ containing $I$, we have $7 = [\mathcal{O}_K : I] = [\mathcal{O}_K : I'][I' : I]$, so $I = \mathcal{O}_k$ or $I' = I$. So $I$ is a maximal ideal, and thus a prime ideal.

□

**Problem 2.** Let $\alpha \in \mathcal{O}_K$ be an element such that $K = \mathbb{Q}(\alpha)$. Show that

$$disc(\alpha) = disc(K/\mathbb{Q}) \cdot t^2,$$

for some $t \in \mathbb{Z}$. This $t$ is called the *index* of $\alpha$.

*Proof.* Assume $\alpha_1, ..., \alpha_n$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$, and $\alpha^{i-1} = \sum_{j=1}^{n} a_{ij}\alpha_j$, where $a_{ij} \in \mathbb{Z}$. Assume $A = (a_{ij})_{i,j=1}^{n}$, then

$$\begin{aligned} disc(\alpha) &= disc(1, \alpha, ..., \alpha^{n-1}) = \det[(\sigma_j(\alpha^{i-1}))_{i,j=1}^{n}]^2 \\ &= \det[(\sigma_j(\sum_{k=1}^{n} a_{ik}\alpha_k))_{j,i=1}^{n}]^2 = \det[(\sum_{k=1}^{n} a_{ik}\sigma_j(\alpha_k))_{j,i=1}^{n}]^2 \\ &= \det[A(\sigma_j(\alpha_k))_{k,i=1}^{n}]^2 = \det A^2 \det[(\sigma_j(\alpha_k))_{k,i=1}^{n}]^2 \\ &= \det A^2 \cdot disc(K/\mathbb{Q}). \end{aligned}$$

Then $t = \det A \in \mathbb{Z}$ is what we want. □

**Problem 3.** Show that if $\alpha \in \mathcal{O}_K$ has index one then $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

*Proof.* Using the proof of problem 2, we have $\det A = \pm 1$, then $B = (b_{ij})_{i,j=1}^{n} := A^{-1} \in SL(n, \mathbb{Z})$, i.e., $b_{ij} \in \mathbb{Z}$. We have $\alpha_i = \sum_{j=1}^{n} b_{ij}\alpha^{j-1} \in \mathbb{Z}[\alpha]$, for any $i = 1, ..., n$. So $\mathcal{O}_K = \mathbb{Z}[\alpha]$. □

**Problem 4.** Given coprime integral ideals $A, B \subset \mathcal{O}_K$ and $\alpha, \beta \in \mathcal{O}_K$ show that there exists a $\lambda \in \mathcal{O}_K$ such that

$$\lambda \equiv \alpha \pmod{A}, \quad \lambda \equiv \beta \pmod{B}.$$

*Proof.* Since $A, B$ are coprime, there exists $a \in A, b \in B$, such that $a + b = 1$. Then we can check that $\lambda = b\alpha + a\beta$ satisfies the conditions. □

**Problem 5.** Let $K = \mathbb{Q}(\zeta_7)$. Find a unit of infinite order.

*Proof.* In class we have known that $N(1 - \zeta_7) = N(1 - \zeta_7^2)$. So $N(1 + \zeta_7) = N(1) = 1$ is a unit. But its complex norm $|(1 + \zeta_7)| > 1$, so there is no $k \in \mathbb{Z}_{>0}$ such that $(1 + \zeta_7)^k = 1$. □