ALGEBRAIC NUMBER THEORY

HOMEWORK 2

(1) Let $a \in \mathbb{N}$ be a natural number. Find a basis (as a $\mathbb{Z}$-module) for the ideal $\mathfrak{a} = (a)$ in $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{m}\,)$ is a quadratic number field. Hint: $\mathfrak{a} = [n, c + m\omega]$; make an educated guess what n, c, m might be, and prove your conjecture.

We claim that $\mathfrak{a} = [a, a\omega]$. To see this, observe that

$$\begin{aligned} (a) &= \{a\alpha : \alpha \in \mathcal{O}_K\} && \text{by definition of } (a) \\ &= \{a(r + s\omega) : r, s \in \mathbb{Z}\} && \text{since } \{1, \omega\} \text{ is an integral basis} \\ &= [a, a\omega] \end{aligned}$$

(2) Show directly that $(7, 1 + \sqrt{-6}\,) = [7, 1 + \sqrt{-6}\,]$ in $R = \mathbb{Z}[\sqrt{-6}\,]$, i.e., that every R-linear combination $3\alpha + (1 + \sqrt{-6}\,)\beta$ with $\alpha, \beta \in R$ can already be written in the form $7a + (1 + \sqrt{-6}\,)b$ with $a, b \in \mathbb{Z}$.

Clearly $[7, 1 + \sqrt{-6}\,] \subseteq (7, 1 + \sqrt{-6}\,)$. Let us prove the converse. We have

$$\begin{aligned} 7\alpha + (1 + \sqrt{-6}\,)\beta &= 7(a + b\sqrt{-6}\,) + (1 + \sqrt{-6}\,)(c + d\sqrt{-6}\,) \\ &= 7a + 7b\sqrt{-6} + c(1 + \sqrt{-6}\,) + d\sqrt{-6} - 6d \\ &= 7(a - b - d) + 7b + 7b\sqrt{-6} + c(1 + \sqrt{-6}\,) + +d\sqrt{-6}d \\ &= 7(a - b - d) + (1 + \sqrt{-6}\,)(7b + c + d), \end{aligned}$$

and this shows that every element of the ideal $(7, 1 + \sqrt{-6}\,)$ can be written as a $\mathbb{Z}$-linear (not just $\mathcal{O}_K$-linear, which follows from the definition of an ideal) combination of 7 and $1 + \sqrt{-6}$.

(3) Let $K = \mathbb{Q}(\sqrt{m}\,)$ be a quadratic number field, where m is squarefree. Prove the following:
- If $m \equiv 2 \bmod 4$ then $2\mathcal{O}_K = (2, \sqrt{m}\,)^2$.
- If $m \equiv 3 \bmod 4$ then $2\mathcal{O}_K = (2, 1 + \sqrt{m}\,)^2$.
- If $m \equiv 1 \bmod 8$ then $2\mathcal{O}_K = \mathfrak{a}\mathfrak{a}'$, where $\mathfrak{a} = (2, \frac{1+\sqrt{m}}{2}\,)$ and $\mathfrak{a} \neq \mathfrak{a}'$.
- If $m \equiv 5 \bmod 8$ then $2\mathcal{O}_K$ is prime.

These are straightforward calculations.
- $m \equiv 2 \bmod 4$: then

$$(2, \sqrt{m}\,)^2 = (4, 2\sqrt{m}, m) = (2)(2, \sqrt{m}, \tfrac{m}{2}) = (2)$$

since $\frac{m}{2}$ is odd.

- $m \equiv 3 \bmod 4$: then
$$\begin{aligned}(2, 1+\sqrt{m}\,)^2 &= (2, 1+\sqrt{m}\,)(2, 1-\sqrt{m}\,)\\ &= (2)(2, 1+\sqrt{m}, \tfrac{1-m}{4}) = (2)\end{aligned}$$
since $\frac{1-m}{2}$ is odd.
- $m \equiv 1 \bmod 8$: then
$$\mathfrak{a}\mathfrak{a}' = (2)(2, \omega, \omega', \tfrac{1-m}{2}) = (2)$$
since $\omega + \omega' = 1$.
- $m \equiv 5 \bmod 8$: if (2) is not prime, then $2 = \mathfrak{a}\mathfrak{a}'$ for $\mathfrak{a} = [a, b + c\omega]$. Since $ac = N\mathfrak{a} = 2$, we must have $a = 2$ and $c = 1$ (if $a = 1$, then $1 \in \mathfrak{a}$, which is impossible). Thus $\mathfrak{a} = [2, b+\omega]$ with $2 \mid N(b+\omega)$. The last relation yields $(2b+1)^2 - m \equiv 0 \bmod 8$, hence $m \equiv 1 \bmod 8$: contradiction.

(4) Let $R = \mathbb{Z}[X]$, and consider $\mathfrak{a} = (2, X)$. Show that there does not exist an ideal $\mathfrak{b} \neq (0)$ in R such that $\mathfrak{a}\mathfrak{b}$ is principal. (I haven't thought of a simple argument; I don't even know for sure that the result is true.)

Let $\mathfrak{a} = (2, X)$, and assume that there is an ideal $\mathfrak{b}$ and a polynomial $f \in \mathbb{Z}[X]$ such that $\mathfrak{a}\mathfrak{b} = (f)$. Let $b \in \mathfrak{b}$; we claim that $f \mid b$. In fact, we see that $(2, X)b \subseteq (f)$, hence $2b \in (f)$ and $Xb \in f$. Thus $f \mid 2b$ and $f \mid Xb$. But 2 and X are distinct prime elements in the UFD $\mathbb{Z}[X]$ (because $\mathbb{Z}[X]/(2) \simeq \mathbb{Z}/2\mathbb{Z}[X]$ and $\mathbb{Z}[X]/(X) \simeq \mathbb{Z}$ are integral domains), hence coprime, so $f \mid \gcd(2b, Xb) = b\gcd(2, X) = b$. (Warning: we have $\gcd(2, X) = 1$, but $(2, X) \neq (1)$; the gcd only generates the ideal in a PID.) Thus $\mathfrak{b} = (f)\mathfrak{c}$ for some ideal $\mathfrak{c}$ in $\mathbb{Z}[X]$. This gives $\mathfrak{a}\mathfrak{c}(f) = (f)$, hence $\mathfrak{a}\mathfrak{c} = (1)$ (we can cancel principal ideals in domains). But then $(1) = \mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}(1) = \mathfrak{a}$, hence $\mathfrak{a} = (1)$. This is false, however: if we had $1 = 2r + sX$ for ring elements r, s, then plugging in $X = 0$ shows $2r = 1$, which is nonsense since 2 is a prime, not a unit, in $\mathbb{Z}[X]$.