ALGEBRAIC NUMBER THEORY

HOMEWORK 2

(1) Show that the ideal $(2, 1+\sqrt{-5}\,)$ equals the $\mathbb{Z}$-module $[2, 1+\sqrt{-5}\,]$.

We have $(2, 1+\sqrt{-5}\,) = 2\mathcal{O}_K + (1+\sqrt{-5}\,)\mathcal{O}_K \supseteq 2\mathbb{Z} + (1+\sqrt{-5}\,)\mathbb{Z} = [2, 1+\sqrt{-5}\,]$. Thus it remains to show that $(2, 1+\sqrt{-5}\,) \subseteq [2, 1+\sqrt{-5}\,]$. In other words: we have to show that the element $2(a+b\sqrt{-5}\,) + (1+\sqrt{-5}\,)(c+d\sqrt{-5}\,)$ can be written in the form $2r + (1+\sqrt{-5}\,)s$ for $r, s \in \mathbb{Z}$. But we find

$$\begin{aligned}
&2(a+b\sqrt{-5}\,) + (1+\sqrt{-5}\,)(c+d\sqrt{-5}\,) \\
&\qquad = (2a+c-5d) + (2b+c+d)\sqrt{-5} \\
&\qquad = (2a+c-5d) - (2b+c+d) + (2b+c+d)(1+\sqrt{-5}\,) \\
&\qquad = 2(a-b-3d) + (2b+c+d)(1+\sqrt{-5}\,),
\end{aligned}$$

and this is exactly what we needed to show.

(2) Show that the $\mathbb{Z}$-module $M = [2, 1+3\sqrt{-5}\,]$ has norm 6, and that $MM' = 2[1, 3\sqrt{-5}\,]$.

We actually proved in class that M has norm 6; the reason is that every element in $\mathcal{O}_K$ can be reduced to one of $a+b\sqrt{-5}$ with $0 \le a \le 1$ and $0 \le b \le 2$, and that these elements generate pairwise distinct residue classes modulo M.

Now we compute the product

$$\begin{aligned}
MM' &= [2, 1+3\sqrt{-5}\,] \cdot [2, 1-3\sqrt{-5}\,] \\
&= [4, 2(1-3\sqrt{-5}\,), 2(1+3\sqrt{-5}\,), 46] \\
&= 2[2, 1-3\sqrt{-5}, 1+3\sqrt{-5}, 23] \\
&= 2[1, 1-3\sqrt{-5}, 1+3\sqrt{-5}\,] \\
&= 2[1, 3\sqrt{-5}\,].
\end{aligned}$$

Here we have used that $1 = 23 - 2 \cdot 11$. Note that $\mathcal{O} = [1, 3\sqrt{-5}\,]$ is an order (a full $\mathbb{Z}$-module containing 1), but not the full maximal order $\mathcal{O}_K$ since e.g. $\sqrt{-5} \notin \mathcal{O}$.

(3) Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$. Prove Fermat's little theorem: $\alpha^{N\mathfrak{p}} \equiv \alpha \bmod \mathfrak{p}$ for all $\alpha \in \mathcal{O}_K$. (Hint: transfer the proof from elementary number theory to $\mathcal{O}_K$.)

One possible proof is by imitating the proof from elementary number theory, where you observe that multiplication by α permutes the nonzero residue classes modulo $\mathfrak{p}$.

Another option is to use the binomial theorem. We have $\alpha = a + b\omega$ for integers a, b, hence $\alpha^p = (a + b\omega)^p \equiv a^p + b^p\omega^p \equiv a + b\omega^p \bmod p$, where we have used the fact that $\binom{k}{p} \equiv 0 \bmod p$ for $1 \leq k \leq p-1$, as well as Fermat's little theorem. Now assume that $m \equiv 2, 3 \bmod 4$; then $\omega = \sqrt{m}$, and $\omega^p = m^{(p-1)/2}\omega \equiv (\frac{m}{p})\omega \bmod p$ if p is an odd prime.

Next observe that we have $(\frac{m}{p}) = +1, 0, -1$ according as $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, $p\mathcal{O}_K = \mathfrak{p}^2$ and $p\mathcal{O}_K = \mathfrak{p}$ are the factorizations of $p\mathcal{O}_K$ into prime ideals. Since $p \in \mathfrak{p}$ in every case, every congruence modulo p also holds modulo $\mathfrak{p}$.

If $(\frac{m}{p}) = +1$, we have thus proved $\alpha^{N\mathfrak{p}} = \alpha^p \equiv \alpha \bmod \mathfrak{p}$. Similarly, if $(\frac{m}{p}) = 0$ for some odd prime p, then $p \mid m$ and $\alpha^{N\mathfrak{p}} = \alpha^p \equiv a \equiv \alpha \bmod \mathfrak{p}$. If $p = 2$, then $m \equiv 2, 3 \bmod 4$ and $p\mathcal{O}_K = \mathfrak{p}^2$, and it is easily checked that $a + bm \equiv \alpha \bmod \mathfrak{p}$ since we have in fact $m \equiv \sqrt{m} \bmod \mathfrak{p}$ in this case. Finally, if $(\frac{m}{p}) = -1$, then we have proved that $\alpha^p \equiv \alpha' \bmod p$; raising this to the p-th power then shows that $\alpha^{N(p)} = \alpha^{p^2} \equiv \alpha \bmod p$.

(4) Let m be a squarefree integer and p a prime number with $(\frac{m}{p}) = -1$. Derive the congruence $(a + b\sqrt{m})^p \equiv a - b\sqrt{m}$ for $a, b \in \mathbb{Z}$. What happens if $(\frac{m}{p}) = +1$?

We have already proved this in Exercise 3.

(5) 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.