Algebraic Number Theory - Assignment 11

Matteo Durante, 2303760, Leiden University

6th December 2018

Exercise 5

We see that we are asked to find the smallest unit > 1 and of norm 1 in $\mathbb{Z}[\sqrt{61}]$.

Let's consider the number field $\mathbb{K} \cong \mathbb{Q}(\sqrt{61}) \cong \mathbb{Q}[X]/(f)$, $f = X^2 - 61$, and the number ring $R = \mathbb{Z}[\sqrt{61}]$.

Noticing that $61 \equiv 1 \mod 4$, we have by [1, thm. 3.10] that $\mathcal{O}_\mathbb{K} \cong \mathbb{Z}[\frac{1+\sqrt{61}}{2}] \cong \mathbb{Z}[X]/(g)$, where $g = X^2 - X - 15$. It is an order of rank 2 and we shall set $\alpha := \frac{1+\sqrt{61}}{2}$.

Since $[\mathbb{K} : \mathbb{Q}] = 2$ and f has only real roots, $\mathcal{O}_\mathbb{K}$ has only two real embeddings, hence by [1, thm. 5.13] we have that $\mathcal{O}_\mathbb{K}^* \cong < -1 > \times < \eta_0 >$, where $\sigma(\eta_0) > 1$ for the embedding representing the ring of integers as $\mathbb{Z}[\alpha]$. Let's fix this embedding.

We will now compute $\mathrm{Pic}(\mathcal{O}_\mathbb{K})$.

Notice that $\Delta(g) = 61$, thus $M_\mathbb{K} = \sqrt{61}/2$. We only have to check the primes above 2 and 3.

Since g has no roots in $\mathbb{F}_2$, it is irreducible in $\mathbb{F}_2[X]$ and the only prime above 2 is precisely 2.

On the other hand, $g \equiv X^2 - X = X(X-1) \mod 3$, thus 3 splits and we have $\mathfrak{p}_3 = (3, \alpha), \mathfrak{q}_3 = (3, 1-\alpha)$, $\mathfrak{p}_3\mathfrak{q}_3 = (3)$.

If we can prove that one among $\mathfrak{p}_3$ and $\mathfrak{q}_3$ is principal, then we are done showing that $\mathrm{Pic}(\mathcal{O}_\mathbb{K}) = 0$ because $[\mathfrak{p}_3] = [\mathfrak{q}_3]^{-1}$.

However, noticing that $3 + \alpha = \frac{7+\sqrt{61}}{2} \in (3, \alpha)$ has norm 3 like $\mathfrak{p}_3$, we have $\mathfrak{p}_3 = (\frac{7+\sqrt{61}}{2})$.

In the same way, we get that $\mathfrak{q}_3 = (\frac{7-\sqrt{61}}{2})$.

It follows that, since $\mathcal{O}_\mathbb{K}$ is a Dedekind ring with trivial Picard group, it is a PID by [1, ex. 2.39].

$g(0) = -15$, thus $\mathfrak{p}_3\mathfrak{p}_5 = (\alpha)$, where $\mathfrak{p}_5 = (5, \alpha) = (\frac{9-\sqrt{61}}{2})$, for $5 = \frac{9-\sqrt{61}}{2}\frac{9+\sqrt{61}}{2}$ and $\alpha = \frac{9-\sqrt{61}}{2}\frac{7+\sqrt{61}}{2}$.

$g(6) = 15$, thus $\mathfrak{p}_3\mathfrak{q}_5 = (6-\alpha)$, where $\mathfrak{q}_5 = (5, 1-\alpha) = (\frac{9+\sqrt{61}}{2})$.

$g(10) = 75$, thus $\mathfrak{q}_3\mathfrak{p}_5^2 = (10-\alpha)$.

Remembering that $\mathfrak{q}_3 = 3\mathfrak{p}_3^{-1}$ and $\mathfrak{q}_5 = 5\mathfrak{p}_5^{-1}$, we have the following relations: $\mathfrak{p}_3\mathfrak{p}_5 = (\alpha)$, $\mathfrak{p}_3\mathfrak{p}_5^{-1} = \frac{(6-\alpha)}{5}$, $\mathfrak{p}_3^{-1}\mathfrak{p}_5^2 = \frac{(10-\alpha)}{3}$.

The ideal generated by $\eta = \alpha^a(\frac{6-\alpha}{5})^b(\frac{10-\alpha}{3})^c$ will be then factorized as $\mathfrak{p}_3^{a+b-c}\mathfrak{p}_5^{a-b+2c}$. Setting the exponents $= 0$, we consider a solution of the system of equations: $(1, -3, -2)$.

It follows that $\eta = \frac{39+5\sqrt{61}}{2} \in \mathcal{O}_\mathbb{K}^*$, $\eta > 1$. We still need to show that it is a fundamental unit of this ring.

Remember that $\eta_0 = t + u\alpha \in \mathcal{O}_\mathbb{K}^*$, $\eta_0 > 1$, is a fundamental unit. Then, $\eta_0^n = \eta$ for some $n \geq 1$, where $t, u > 0$ because η has positive coefficients w.r.t. the basis $\{1, \alpha\}$.

Now, $N(\eta_0) = t^2 + tu - 15u^2 = 1$. If $u = 1$, $t^2 + t - 16 = 0$ has no natural solutions, thus $u > 1$.

It follows that $\eta > 2\alpha$, thus, since $1 \leq n = \frac{\log(\eta)}{\log(\eta_0)} < \frac{\log(\eta)}{\log(2\alpha)} < 2$, $n = 1$ and η is a fundamental unit.

Now, to find the fundamental unit of this ring, we still have to find out which is the lowest $n > 0$ s.t. $\eta^n \in \mathbb{Z}[\sqrt{61}]$, for $\mathcal{O}_\mathbb{K}$ is integral over $\mathbb{Z}[\sqrt{61}]$ and, by [1, ex. 5.20], $\mathbb{Z}[\sqrt{61}]^* = \mathbb{Z}[\sqrt{61}] \cap \mathcal{O}_\mathbb{K}^*$.

First of all, notice that $n > 1$ because η doesn't lie in $\mathbb{Z}[\sqrt{61}] = \mathbb{Z} + 2\mathcal{O}_\mathbb{K}$. However, by [1, 5.16], the index of $\mathbb{Z}[\sqrt{61}]^*$ in $\mathcal{O}_\mathbb{K}^*$ divides the order of $(\mathcal{O}_\mathbb{K}/2\mathcal{O}_\mathbb{K})^* \cong \mathbb{F}_4^*$. From this we get that $n = 3$, thus $\mathbb{Z}[\sqrt{61}]^* \cong < -1 > \times < \eta^3 >$, where $\eta^3 = 29718 + 3805\sqrt{61}$.

We only have to check which ones are the elements of norm 1 in this latest unit group and s.t. $\sqrt{61}$ has a positive coefficient. Since $N(\eta^3) = -1$ and the norm is multiplicative, these are precisely the even powers of η^3, thus the smallest integral solution of our Pell equation s.t. $y > 0$ is given by the coefficients of $\eta^6 = 1766319049 + 226153980\sqrt{61}$.

Exercise 6

We see that we are asked to find the smallest unit > 1 and of norm 1 in $\mathbb{Z}[\sqrt{109}]$.

Let's consider the number field $\mathbb{K} \cong \mathbb{Q}(\sqrt{109}) \cong \mathbb{Q}[X]/(f)$, $f = X^2 - 109$, and remember the number ring $R = \mathbb{Z}[\sqrt{109}]$.

Noticing that $109 \equiv 1 \mod 4$, we have by [1, thm. 3.10] that $\mathcal{O}_\mathbb{K} \cong \mathbb{Z}[\frac{1+\sqrt{109}}{2}] \cong \mathbb{Z}[X]/(g)$, where $g = X^2 - X - 27$. It is an order of rank 2 and we shall set $\alpha := \frac{1+\sqrt{109}}{2}$.

Since $[\mathbb{K} : \mathbb{Q}] = 2$ and f has only 2 real roots, $\mathcal{O}_\mathbb{K}$ has only two real embeddings, hence by [1, thm. 5.13] we have that $\mathcal{O}_\mathbb{K}^* \cong < -1 > \times < \eta >$, where $\sigma(\eta) > 1$ for the embedding representing the ring of integers as $\mathbb{Z}[\alpha]$. Let's fix this embedding.

We will now compute $\mathrm{Pic}(\mathcal{O}_\mathbb{K})$.

Notice that $\Delta_\mathbb{K} = 109$, thus $M_\mathbb{K} = \sqrt{109}/2$. We only have to check the primes above 2, 3 and 5.

Since g has no root in $\mathbb{F}_2$, it is irreducible in $\mathbb{F}_2[X]$ and the only prime above 2 is precisely (2).

Furthermore, $g \equiv X^2 - X = X(X-1) \mod 3$, thus 3 splits and we have $\mathfrak{p}_3 = (3, \alpha), \mathfrak{q}_3 = (3, 1-\alpha)$.

In the same way, $g \equiv X^2 - 6X + 8 = (X-4)(X-2) \mod 5$, thus 5 splits and we have $\mathfrak{p}_5 = (5, 4-\alpha), \mathfrak{q}_5 = (5, 2-\alpha)$.

If we can show that one ideal above 3 and one above 5 is principal, then we are done showing that $\mathrm{Pic}(\mathcal{O}_\mathbb{K}) = 0$ because $[\mathfrak{p}_p] = [\mathfrak{q}_p]^{-1}$.

Observe now that $2 \cdot 3 - \alpha = \frac{11-\sqrt{109}}{2} \in \mathfrak{p}_3$ has norm 3 like $\mathfrak{p}_3$, hence $\mathfrak{p}_3 = (\frac{11-\sqrt{109}}{2})$.

Furthermore, noticing that $7 \cdot 5 - 4(4-\alpha) = 21 + 2\sqrt{109} \in \mathfrak{p}_5$ has norm 5 like $\mathfrak{p}_5$, we have $\mathfrak{p}_5 = (21 + 2\sqrt{109})$.

It follows that, since $\mathcal{O}_\mathbb{K}$ is a Dedekind ring with trivial Picard group, it is a PID by [1, ex. 2.39].

$g(4) = -15$, thus $\mathfrak{q}_3\mathfrak{p}_5 = (4-\alpha)$.

$g(9) = 45$, thus $\mathfrak{p}_3^2\mathfrak{p}_5 = (9-\alpha)$.

$g(27) = 675$, thus $\mathfrak{p}_3^3\mathfrak{q}_5^2 = (27-\alpha)$.

Remembering that $\mathfrak{q}_p = p \cdot \mathfrak{p}_p^{-1}$, we have the following relations: $\mathfrak{p}_3^{-1}\mathfrak{p}_5 = \frac{(4-\alpha)}{3}, \mathfrak{p}_3^2\mathfrak{p}_5 = (9-\alpha), \mathfrak{p}_3^3\mathfrak{p}_5^{-2} = \frac{(27-\alpha)}{25}$.

The ideal generated by $\eta = (\frac{4-\alpha}{3})^a(9-\alpha)^b(\frac{27-\alpha}{25})^c$ will be then factorized as $\mathfrak{p}_3^{-a+2b+3c}\mathfrak{p}_5^{a+b-2c}$. Setting the exponents $= 0$, we consider a solution of the system of equations: $(-7, 1, -3)$.

It follows that $\eta = \frac{261+25\sqrt{109}}{2} \in \mathcal{O}_\mathbb{K}^*$, $\eta > 1$. We still need to show that it is a fundamental unit of this ring.

Remember that $\eta_0 = t + u\alpha \in \mathcal{O}_{\mathbb{K}}^*$, $\eta_0 > 1$, is our fundamental unit. Then, $\eta_0^n = \eta$ for some $n \geq 1$, where $t, u > 0$ because η has positive coefficients w.r.t. the basis $\{1, \alpha\}$.

Now, $N(\eta_0) = t^2 + tu - 27u^2 = 1$ and, looking at $t^2 + tu - (27u^2 + 1)$, we shall see this as a polynomial in t.

We can check that for $u \in \{1, 2, 3, 4\}$ there are no natural t satisfying the equation by finding the roots of our polynomial.

It follows that $u \geq 5$ and therefore $\eta_0 > 5\alpha$, thus, since $1 \leq n = \frac{\log(\eta)}{\log(\eta_0)} < \frac{\log(\eta)}{\log(5\alpha)} < 2$, $n = 1$ and η is a fundamental unit.

Now, to find the fundamental unit of this ring, we still have to find out which is the lowest $n > 0$ s.t. $\eta^n \in \mathbb{Z}[\sqrt{109}]$, for $\mathcal{O}_{\mathbb{K}}$ is integral over $\mathbb{Z}[\sqrt{109}]$ and, by [1, ex. 5.20], $\mathbb{Z}[\sqrt{109}]^* = \mathbb{Z}[\sqrt{109}] \cap \mathcal{O}_{\mathbb{K}}^*$.

First of all, notice that $n > 1$ because η doesn't lie in $\mathbb{Z}[\sqrt{109}] = \mathbb{Z} + 2\mathcal{O}_{\mathbb{K}}$. However, by [1, 5.16], the index of $\mathbb{Z}[\sqrt{109}]^*$ in $\mathcal{O}_{\mathbb{K}}^*$ divides the order of $(\mathcal{O}_{\mathbb{K}}/2\mathcal{O}_{\mathbb{K}})^* \cong \mathbb{F}_4^*$. From this we get that $n = 3$, thus $\mathbb{Z}[\sqrt{109}]^* \cong < -1 > \times < \eta^3 >$, where $\eta^3 = 8890182 + 851525\sqrt{109}$.

We only have to check which ones are the elements of norm 1 in this latest unit group and s.t. $\sqrt{109}$ has a positive coefficient. Since $N(\eta^3) = -1$ and the norm is multiplicative, these are precisely the even powers of η^3, thus the smallest integral solution of our Pell equation s.t. $y > 0$ is given by the coefficients of $\eta^6 = 158070671986249 + 15140424455100\sqrt{109}$.

References

[1] P. Stevenhagen, *Number Rings*, 2017.