Algebraic Number Theory - Assignment 10

Matteo Durante, 2303760, Leiden University

30th November 2018

Exercise 21

Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial s.t. $\mathbb{K} = \mathbb{Q}(\alpha) \cong \mathbb{Q}[X]/(f)$. It will have degree 3 and only one real root.

We know that the only roots of unity are ± 1 because $r > 0$ and, by [1, thm. 5.13], $\mathcal{O}_{\mathbb{K}}^*$ has rank $1 + 1 - 1 = 1$. We will call σ our real embedding, while $\sigma_\pm$ the complex ones.

Since $\mathcal{O}_{\mathbb{K}}^* \cong < -1 > \times < \mu >$, where $\mu \in \mathbb{K} \setminus \mathbb{Q}$ is a fundamental unit s.t. $\sigma(\mu) > 1$, setting for future reference $u = x^2 = \sigma(\mu)$, $x > 1$, being $< \mu >$ the infinite cyclic subgroup of all units with positive image under σ, we get that $< \mu > \cong \mathbb{Z}$.

The minimum polynomial of μ will have degree 3, for $1 < [\mathbb{Q}(\mu) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(\mu) : \mathbb{Q}] | [\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Remember that $\Delta(1, \mu, \mu^2) = \Delta(f_{\mathbb{Q}}^{\mu}) = [\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\mu]]^2 \cdot \Delta_{\mathbb{K}}$, hence $|\Delta(1, \mu, \mu^2)| \geq |\Delta_{\mathbb{K}}|$.

Since μ is a unit, $N_{\mathbb{K}/\mathbb{Q}}(\mu) = \pm 1$, which will be the opposite of the constant term of $f_{\mathbb{Q}}^{\mu}$. It follows that the product of the images of μ under the embeddings is $\pm 1 = x^2 a^2 > 0$, where $\sigma_\pm(\mu) = a e^{\pm iy}$, thus $a = x^{-1}$.

Now, considering $\sigma_\pm(\mu) = x^{-1} e^{\pm iy}$, we get:

$$
\begin{aligned}
|\Delta(1, \mu, \mu^2)| &= \left| \det \begin{bmatrix} 1 & x^2 & x^4 \\ 1 & x^{-1}e^{iy} & (x^{-1}e^{iy})^2 \\ 1 & x^{-1}e^{-iy} & (x^{-1}e^{-iy})^2 \end{bmatrix} \right|^2 \\
&= (2\sin(y)(x^3 + x^{-3} - 2\cos(y)))^2 \\
&= 4((x^3 + x^{-3})\sin(y) - \sin(2y))^2
\end{aligned}
$$

Let's consider $s(y) = (x^3 + x^{-3})\sin(y) - \sin(2y)$. Keeping x fixed, we will find a bound as y varies (the function has maximum and minimum because it is differentiable, periodic and bounded; furthermore, this function is odd, thus maximum and minimum coincide up to sign).

$s'(y) = (x^3 + x^{-3})\cos(y) - 2\cos(2y) = -4\cos^2(y) + (x^3 + x^{-3})\cos(y) + 2$.

For h s.t. $s'(h) = 0$, we have that $\cos(h) \neq 0$ and $t = x^3 + x^{-3} = 4\cos(h) - \frac{2}{\cos(h)}$, therefore there $s(h) = -2\frac{\sin^3(h)}{\cos(h)}$.

It follows that $(s(h))^2 \leq 4(3\cos^2(h) - 3 + \frac{1}{\cos^2(h)}) = t^2 + 4 - 4\cos^2(h)$.

Fixing an h which maximizes s, this means that $|\Delta_{\mathbb{K}}| \leq |\Delta(1, \mu, \mu^2)| \leq 4(x^6 + 6 + x^{-6} - 4\cos^2(h))$.

Let's go back to $s'(h) = 0$.

The polynomial $g(y) = 4y^2 - (x^3 + x^{-3})y - 2$ has two real roots (positive discriminant), one positive and one negative (their product is -2), as the possible values of $\cos(h)$.

Since $g(1) = 2 - (x^3 + x^{-3}) < 0$, the positive one is > 1, thus $\cos(h) < 0$. Since $g(-\frac{x^{-3}}{2}) = \frac{3}{2}(u^{-6} - 1) \leq 0$, $\cos(h) \leq -\frac{x^{-3}}{2}$, i.e. $4\cos^2(h) \geq x^{-6}$.

It follows that $|\Delta_{\mathbb{K}}| \leq 4(x^6 + 6) = 4u^3 + 24$.

Exercise 22

First of all, since $f = X^3 + aX - 1 \in \mathbb{Z}[X]$ is s.t. it has no integer roots, for they would have to divide 1, we get that f is irreducible in $\mathbb{Z}[X]$ and $\alpha \notin \mathbb{Z}$, thus f is irreducible in $\mathbb{Q}[X]$ and $\alpha \in \overline{\mathbb{Q}} \backslash \mathbb{Q}$.

Furthermore, notice that $\alpha \in \mathcal{O}_{\mathbb{K}}$, where $\alpha(\alpha^2 + a) = 1$, hence $\alpha, \alpha^2 + a \in \mathcal{O}_{\mathbb{K}}^*$.

Since $\mathbb{K} = \mathbb{Q}(\alpha) \cong \mathbb{Q}[X]/(f)$ is s.t. $[\mathbb{K} : \mathbb{Q}] = 3$, either $\mathcal{O}_{\mathbb{K}}$ (an order of rank 3) has 3 real embeddings or 1 real and 2 complex.

If the real ones were 3, then all of the roots of f would be real, which is absurd because $\sum_{i=1}^3 \alpha_i^2 = (\sum_{i=1}^3 \alpha_i)^2 - 2\sum_{1 \leq i < j \leq 3} \alpha_i \alpha_j = 0 - 2a = -2a < 0$.

It follows that $r = 1$ and $s = 1$. Let's call our only real embedding σ.

There are no roots of unity besides ± 1 in $\mathcal{O}_{\mathbb{K}}$ because $r > 0$.

By [1, thm. 5.13], we get that $\mathcal{O}_{\mathbb{K}}^*$ has rank $r + s - 1 = 1$, i.e. it is $=< -1 > \times < \mu >$, where $\sigma(\mu) > 1$.

Now, we will try to find $\mathcal{O}_{\mathbb{K}}$.

First, we will consider $R = \mathbb{Z}[X]/(f) \cong \mathbb{Z}[\alpha] \cong \mathbb{Z} + \mathbb{Z} \cdot \alpha + \mathbb{Z} \cdot \alpha^2$, which is contained in it and is an order of rank 3 s.t. $Q(R) = \mathbb{K}$.

Notice that $|\Delta(R)| = |\Delta(f)| = 4a^3 + 27$ is square-free, hence, since $\Delta(R) = [\mathcal{O}_{\mathbb{K}} : R]^2 \cdot \Delta_{\mathbb{K}}$, $[\mathcal{O}_{\mathbb{K}} : R] = 1$, thus $R = \mathcal{O}_{\mathbb{K}}$ and we are done.

We still have to prove α is a fundamental unit. Since the extensions through the different roots of f are isomorphic, we may suppose that $\alpha \in \mathbb{R}$ and therefore $\mathbb{Z}[\alpha] \subset \mathbb{R}$ (here we are choosing to work with the real embedding, that is the real representation of our ring). In particular, $\mu = \sigma(\mu) > 1$.

Noticing that $f(0) < 0, f(1/2) > 0$, we get $0 < \alpha < 1/2$. We shall show that $\alpha^{-1} = \alpha^2 + a > 2$ is a fundamental unit and the thesis will follow.

Notice that, by [1, ex. 21], $|\Delta_{\mathbb{K}}| = 4a^3 + 27 \leq 4\mu^3 + 24$, hence $(a^3 + 3/4)^{2/3} \leq \mu^2$. If we can prove that $\alpha^2 + a < (a^3 + 3/4)^{2/3}$, i.e. $(\alpha^2 + a)^3 < (a^3 + 3/4)^2$, then we are done because it means that ours is a unit satisfying $\mu \leq \alpha^2 + a < \mu^2$ and therefore $= \mu$.

However, since $\alpha < 1/2$, plugging in $1/2$ we get $(\alpha^2 + a)^3 < (1/4 + a)^3$, hence we may just verify that $(1/4 + a)^3 \leq (a^3 + 3/4)^2$, which can be verified by expanding the powers and getting $a^3 + 3a^2/4 + 3a/16 + 1/64 \leq a^6 + 3a^3/2 + 9/16$, which leads to $a^6 + a^3/2 + 35/64 \geq 3a^2/4 + 3a/16$. This last inequality is verified for $a \geq 2$ because $a^6 \geq 3a^2/4$ and $a^3/2 \geq 3a/16$ for these a.

References

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