Algebraic Number Theory - Assignment 7

Matteo Durante, 2303760, Leiden University

3rd November 2018

Exercise 13

First of all, given the number field $\mathbb{K} = Q(R)$, R an order, we have that $R \subset \mathcal{O}_{\mathbb{K}}$ and they have the same rank as $\mathbb{Z}$-algebras.

Remembering that $\Delta(R) = [\mathcal{O}_{\mathbb{K}} : R]^2 \cdot \Delta(\mathcal{O}_{\mathbb{K}})$, since a square in $\mathbb{Z}$ is $\equiv 0, 1 \mod 4$, we only have to show that $\Delta(\mathcal{O}_{\mathbb{K}}) \equiv 0, 1 \mod 4$.

Consider now an integral basis for $\mathbb{K}$ over $\mathbb{Q}$, $X = \{a_1, \ldots, a_n\}$, and all of the embeddings $\sigma_i : \mathbb{K} \to \mathbb{C}$. By definition, $\Delta_{\mathbb{K}} = (\det([\sigma_i(a_j)]_{i,j=1}^n))^2$, which can be rewritten in the following way:

$$
\begin{aligned}
\Delta_{\mathbb{K}} &= \left(\sum_{\pi \in S_n} \operatorname{sgn}(\pi) \Pi_{i=1}^n \sigma_{\pi(i)}(a_i) \right)^2 \\
&= \left(\sum_{\pi \in A_n} \Pi_{i=1}^n \sigma_{\pi(i)}(a_i) - \sum_{\pi \notin A_n} \Pi_{i=1}^n \sigma_{\pi(i)}(a_i) \right)^2 \\
&= (P - N)^2 \\
P &:= \sum_{\pi \in A_n} \Pi_{i=1}^n \sigma_{\pi(i)}(a_i) \\
N &:= \sum_{\pi \notin A_n} \Pi_{i=1}^n \sigma_{\pi(i)}(a_i)
\end{aligned}
$$

We will prove that $P + N, PN \in \mathbb{Q}$.

Let L be a finite extension of $\mathbb{Q}$ which is Galois and contains $\mathbb{K}$. Let's show that $\sigma(P + N) = P + N, \sigma(PN) = PN$ for every $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$.

Let's extend every σ_i to an embedding $\overline{\sigma_i} : L \to \mathbb{C}$. By the normality of L, $\overline{\sigma}_i(L) = L$, hence $\sigma_i(\mathbb{K}) \subset L$. It follows that we can create an embedding $\sigma\sigma_i : \mathbb{K} \to \mathbb{C}$. The association $\{\sigma_1, \ldots, \sigma_n\} \to \{\sigma_1, \ldots, \sigma_n\}$ given by $\sigma_i \mapsto \sigma\sigma_i$ defines a bijection, i.e. a permutation $\tau \in S_n$ s.t. $\sigma\sigma_i = \sigma_{\tau(i)}$.

If τ is even, then:

$$\begin{aligned}\sigma(P) &= \sum_{\pi\in A_n} \Pi_{i=1}^n \sigma\sigma_{\pi(i)}(a_i)\\ &= \sum_{\pi\in A_n} \Pi_{i=1}^n \sigma_{\tau\pi(i)}(a_i)\\ &= \sum_{\pi\in \tau A_n} \Pi_{i=1}^n \sigma_{\pi(i)}(a_i)\\ &= \sum_{\pi\in A_n} \Pi_{i=1}^n \sigma_{\pi(i)}(a_i)\\ &= P\end{aligned}$$

The same goes for N.

If it is odd, then $\tau A_n = S_n \setminus A_n$ and $\tau(S_n \setminus A_n) = A_n$, thus, repeating the computations, $\sigma(P) = N$ and $\sigma(N) = P$.

It follows that $\sigma(P + N) = P + N, \sigma(PN) = PN$.

Since every embedding fixes $P+N$ and PN, they both belong to $\mathbb{Q}$ and, specifically, $P+N, PN \in \mathbb{Z}$ because both P and N are algebraic integers (they are linear combinations of products of algebraic integers since the image of an algebraic integer under an embedding is an algebraic integer).

Since $(P-N)^2 = (P+N)^2 - 4PN$, by an argument previously given we have the thesis.

Exercise 17

By definition, $\Delta_{\mathbb{K}} = \Delta(\mathcal{O}_{\mathbb{K}})$. Having $\mathbb{K} = \mathbb{Q}(\xi_{p^k})$, consider the order $R = \mathbb{Z}[\xi_{p^k}] \cong \mathbb{Z}[X]/(\phi_{p^k})$, where ϕ_{p^k} is the minimum (cyclotomic) polynomial of ξ_{p^k}.

By [1, thm. 3.12], R is a Dedekind domain, hence $\mathcal{O}_{\mathbb{K}} \subset R$ by [1, thm. 3.20(3)]. Furthermore, given that $\mathbb{Z} \subset \mathcal{O}_{\mathbb{K}}$ and $\xi_{p^k} \in \mathcal{O}_{\mathbb{K}}$, $R \subset \mathcal{O}_{\mathbb{K}}$, thus we have an equality.

Now we only have to compute $\Delta(\phi_{p^k})$ by [1, cor. 4.7].

Knowing that $\phi_{p^k} = \frac{X^{p^k}-1}{X^{p^{k-1}}-1} = \sum_{i=0}^{p-1} X^{ip^{k-1}}$, considered a primitive root of unity ξ_{p^k}, for any $1 \le j \le p^k$ s.t. $(j,p) = 1$, since $\phi'_{p^k} = \frac{p^k X^{p^k-1}(X^{p^{k-1}}-1) - p^{k-1}X^{p^{k-1}-1}(X^{p^k}-1)}{(X^{p^{k-1}}-1)^2}$, we have $\phi'_{p^k}(\xi^j_{p^k}) = \frac{p^k(\xi^j)^{-1}}{(\xi^j)^{p^{k-1}}-1} = \frac{p^k(\xi^j)^{-1}}{(\xi^{p^{k-1}})^j-1}$.

Now, let $\mu = \xi^{p^{k-1}}$, and hence $\mu^j = (\xi^j)^{p^{k-1}}$. For any j, μ is a pth root of unity.

Remembering that $\Delta(\phi_{p^k}) = (-1)^{p^k(p^k-1)/2} Res(\phi_{p^k}, \phi'_{p^k}) = (-1)^{p^k(p^k-1)/2} \Pi_{j=1,(j,p)=1}^{p^k} \phi'_{p^k}(\xi^j_{p^k}) = (-1)^{p^k(p^k-1)/2} \Pi_{j=1,(j,p)=1}^{p^k} \frac{p^k(\xi^j)^{-1}}{(\xi^{p^{k-1}})^j-1}$, we shall compute numerator and denominator separately.

Noticing that $\sum_{j=1,(j,p)=1}^{p^k} j = 1 + \ldots + p^k - p(1 + \ldots + p^{k-1}) = p^k \frac{p^k-p^{k-1}}{2}$, since $\xi^{p^k \frac{p^k-p^{k-1}}{2}} = (\xi^{p^k})^{\frac{p^k-p^{k-1}}{2}} = 1$, the numerator is $(p^k)^{p^k-p^{k-1}} = p^{p^{k-1}(pk-k)}$.

On the other hand, we see that:

$$\begin{aligned}\Pi_{j=1,(j,p)=1}^{p^k}(\mu^j - 1) &= \Pi_{i=1}^{p^{k-1}}\Pi_{j=p(i-1)+1}^{pi-1}(-1)(1-\mu^j)\\ &= \Pi_{i=1}^{p^{k-1}}(-1)^{p-1}\Pi_{j=1}^{p-1}(1-\mu^j)\\ &= (-1)^{p^{k-1}(p-1)}(\phi_p(1))^{p^{k-1}}\\ &= (-1)^{p^{k-1}(p-1)}p^{p^{k-1}}\\ &= p^{p^{k-1}}\end{aligned}$$

It follows that $\Delta_{\mathbb{K}} = \Delta(\phi_{p^k}) = (-1)^{\frac{p^k - p^{k-1}}{2}} p^{p^{k-1}(pk-k-1)}$.

References

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