Solutions to Sheet 9

Exercise 1

Let $K = \mathbb{Q}(\zeta_8)$.

1. Show that $K = \mathbb{Q}(\sqrt{2}, \mathrm{i})$.
2. Let p be an odd prime number. Show that $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv 1, 7 \pmod 8$.

Solution.

1. Note that $\zeta_8 = \frac{1}{\sqrt{2}} + \frac{\mathrm{i}}{\sqrt{2}}$, so that we have $\mathbb{Q}(\zeta_8) \subset K$. But we have $\deg \mathbb{Q}(\zeta_8) = \varphi(8) = 4$ and also $\deg \mathbb{Q}(\sqrt{2}, \mathrm{i})4$, which implies equality. There are other many ways to do this.

2. We have seen that $\left(\frac{2}{p}\right) = 1$ if and only if p splits totally in $\mathbb{Q}(\sqrt{2})$, i.e., $p = \mathfrak{p}_1\mathfrak{p}_2$ for two distinct prime ideals of $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$. Since the discriminant of $\mathbb{Q}(\sqrt{2}) = 8$, we also know that every odd prime is unramified in $\mathbb{Q}(\sqrt{2})$ (as a prime ramifies iff it divides the discriminant).
But being split totally is equivalent to having frobenius element equal to the identity: For every prime $\mathfrak{p} \subset \mathcal{O}_K$ over $p\mathbb{Z}$ we have that $\#D(\mathfrak{p}|p) = e(\mathfrak{p}|p)f(\mathfrak{p}|p) = f(\mathfrak{p}|p)$, and we obtain

$$p > 2 \text{ totally split in } \mathbb{Q}(\sqrt{2}) \iff \forall \mathfrak{p} \mid p\mathcal{O}_{\mathbb{Q}(\sqrt{2})} : f(\mathfrak{p}|p) = 1 \iff \forall \mathfrak{p} \mid p\mathcal{O}_{\mathbb{Q}(\sqrt{2})} : \#D = 1.$$

Since p is unramified we know that for every $\mathfrak{p} \mid p\mathcal{O}_K$, $D(\mathfrak{p}|p) \cong \mathrm{Gal}(\mathcal{O}_{\mathbb{Q}(\sqrt{2})}/\mathfrak{p}|\mathbb{Z}/p\mathbb{Z})$, and the latter is generated by the Frobenius element. In particular, we find that (by definition), $D(\mathfrak{p}|p)$ is generated by the generalized Frobenius element $\left(\frac{\mathbb{Q}(\sqrt{2})/Q}{\mathfrak{p}}\right)$, which by Definition-Lemma 3.31 is isomorphic to the restriction of $\left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right)$ to $\mathbb{Q}(\sqrt{2})$. We are now almost done, because we know how to compute the Frobenius element in K! It is given by $\zeta_8 \mapsto \zeta_8^p$. Now we use that $\sqrt{2} = \zeta_8 + \zeta_8^7$, and one readily checks that

$$\left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right)(\sqrt{2}) = \left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right)(\zeta_8 + \zeta_8^7) = \zeta_8^p + \zeta_8^{-p} = \sqrt{2}$$

if and only if $p \equiv 1, 7 \pmod 8$.

Exercise 2

Let $p \geq 2$ be a prime number. Set $K = \mathbb{Q}(\zeta_p)$. Show that $\Delta_K = (-1)^{(p-1)(p-2)/2}p^{p-2}$.

Solution. Note that $\zeta_p, \dots, \zeta_p^{p-1}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$ by results of the script (Lemma 3.36). Hence it suffices to show that $\Delta_{K/\mathbb{Q}}(\zeta_p, \dots, \zeta_p^{p-1}) = (-1)^{(p-1)(p-2)/2}p^{p-2}$. We know that $\mathrm{Gal}(K/\mathbb{Q}) \cong \{\sigma_i | 1 \leq i < p-1\}$, where σ_i is the morphism sending ζ_p to ζ_p^i. We have seen that

$$\Delta_{K/\mathbb{Q}}(\zeta_p, \dots, \zeta_p^{p-1}) = \det A^2,$$

where A is the matrix with ij-th entry given by $\sigma_i(\zeta_p^j)$. Now A is a Vandermonde matrix, and we obtain

$$\det A^2 = \left(\prod_{1 \leq i < j \leq p-1} (\zeta_p^i - \zeta_p^j)\right)^2 = (-1)^{(p-1)(p-2)/2} \prod_{i \neq j} (\zeta_p^i - \zeta_p^j) = \pm \prod_{i=1}^{p-1} \varphi_p'(\zeta_p^i)$$

where $\varphi_p(X) = \frac{X^p-1}{X-1}$ is the p-th cyclotomic polynomial. We can differentiate the equation

$$\varphi_p(X)(X-1) = X^p - 1$$

to find that

$$\varphi_p'(X)(X-1) + \varphi_p(X) = pX^{p-1}.$$

This gives

$$... = (-1)^{(p-1)(p-2)/2} p^{p-1} \prod_{i=1}^{p-1} \frac{1}{1-\zeta_p^i} = (-1)^{(p-1)(p-2)/2} p^{p-1} \varphi_p(1)^{-1} = (-1)^{(p-1)(p-2)/2} p^{p-2}.$$

In the last step we used that $X^p - 1 = \prod_{i=0}^{p-1}(X - \zeta_p^i)$, so that $\varphi_p(X) = \frac{X^p-1}{X-1} = \prod_{i=1}^{p-1}(X - \zeta_p^i)$.

Max von Consbruch, email: mvconsbruch@uni-bonn.de. Date: December 11, 2023