Another Example by Dedekind

Ferran Espuña Bertomeu

January 2, 2024

Remark. $f(X) = X^3 - X + 1$ is irreducible over $\mathbb{Q}$.

Proof. If it were reducible, it would have a root in $\mathbb{Q}$. By the rational root theorem, the only possible rational roots of f are ± 1. None of these are roots of f. □

Claim 1. *Let θ be a root of f. Then, $K = \mathbb{Q}(\theta)$ is a field extension of $\mathbb{Q}$ of degree 3, and $\mathcal{O}_K = \mathbb{Z}[\theta]$.*

Proof. The first part is clear because f is irreducible over $\mathbb{Q}$. For the second part, we will calculate $\operatorname{disc}(f) = \operatorname{disc}(1, \theta, \theta^2)$ and show that it is square-free. Using Viète's formulas, we can find relations between θ and the other roots of f (say, α_1 and α_2):

- The degree 0 coefficient of f is $1 = -\theta\alpha_1\alpha_2$.
- The degree 2 coefficient of f is $0 = -(\theta + \alpha_1 + \alpha_2)$.

Now, note that $\alpha_1\alpha_2 = -\frac{1}{\theta} = \theta^2 - 1$ (this is easy to check from the equation of f). Additionally, $\alpha_1 + \alpha_2 = -\theta$. With this information, and reducing any polynomials in θ modulo f when needed, we can compute the discriminant of f:

$$\begin{aligned}\Delta(f) &= [(\theta - \alpha_1)(\theta - \alpha_2)(\alpha_1 - \alpha_2)]^2 \\ &= [\theta^2 - (\alpha_1 + \alpha_2)\theta + \alpha_1\alpha_2]^2[(\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2] \\ &= [3\theta^2 - 1]^2[4 - 3\theta^2] = -23\end{aligned}$$

□

Claim 2. *Let θ be a root of f. Consider the degree 3 extension $K = \mathbb{Q}(\theta)$. Then $23\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2$. In particular, $K \mid \mathbb{Q}$ is not Galois.*

Proof. We will use the Kummer-Dedekind theorem on the polynomial f. Since we know that $\mathcal{O}_K = \mathbb{Z}[\theta]$, we can apply it to any prime $p \in \mathbb{Z}$, and in particular to $p = 23$. The polynomial has exactly two roots modulo 23 (namely, 20 and 13). Therefore, one of the roots is double, and the other one is simple. This means that the polynomial splits as a square of a prime times a prime, and the result follows. The extension is not Galois because if it were all exponents in the decomposition would coincide. □

Remark. We can take the Kummer-Dedekind theorem a bit further to say that 23 is the *only* prime that ramifies in K. Indeed, for p to ramify, f must be inseparable modulo p, that is, f and $f' = 3X^2 - 1$ must have a common root modulo p. Let u be a root of f', i.e., $3u^2 = 1$. Since it must be a root of f as well, we have:

$$u(1-u^2) = u-u^3 = 1 \Rightarrow 2u = u(3-1) = u(3-3u^2) = 3u(1-u^2) = 3 \Rightarrow 4 = 3(2u)^2 = 27 \Rightarrow 23 = 0$$

Claim 3. *The Galois closure of $K \mid \mathbb{Q}$ is $N = KL$, where $L = \mathbb{Q}\left(\sqrt{-23}\right)$.*

Proof. N must be the splitting field of f over $\mathbb{Q}$, which we can take to contain K as it is generated over $\mathbb{Q}$ by one of the roots of f. Now, because we know $N \neq K$, we must have $[N : K] = 2 = \deg f/(X-\theta)$. Therefore, $[N : \mathbb{Q}] = 6$ so we only need to prove that $\sqrt{-23} \in N$. This is true because the discriminant of f is -23, and on the other hand it is the square of a polynomial expression in the roots of f. □

Claim 4. *$N \mid L$ is unramified.*

Proof. Suppose that a prime $\mathfrak{q} \subset \mathcal{O}_L$ ramifies in N. Since $N \mid L$ is Galois, its ramification index must divide $[N : L] = [N : \mathbb{Q}]/[L : \mathbb{Q}] = 3 \Rightarrow$ it is 3. Let $p = \mathfrak{q} \cap \mathbb{Z}$ the corresponding prime in $\mathbb{Z}$. Since $\mathfrak{q}$ divides $p\mathcal{O}_L$, the ramification index of p in $N \mid \mathbb{Q}$ must be a multiple of 3. This means that p ramifies in $K \mid \mathbb{Q}$, because $3 \nmid 2 = [N : K]$, and $N \mid K$ is Galois. By a previous remark, $p = 23$ is the only prime that ramifies in $K \mid \mathbb{Q}$. Therefore, $p = 23$. However, we have seen that a square $(\mathfrak{p}_1^2)$ divides $23\mathcal{O}_N$, so the ramification index of 23 in $N \mid \mathbb{Q}$ must be exactly 6, so $23\mathcal{O}_N = \mathfrak{r}^6$. This is incompatible with the fact that $23\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2$: If two copies of $\mathfrak{r}$ are in $\mathfrak{p}_1^2$ (i.e., $\mathfrak{p}_1 = \mathfrak{r}$), then $\mathfrak{p}_2 = \mathfrak{p}_1^4$, while if four copies of $\mathfrak{r}$ are in $\mathfrak{p}_1^2$, then $\mathfrak{p}_2 = \mathfrak{p}_1$.

□

Claim 5. *$K = N^{D_{\mathcal{P}/23}}$ for some prime $\mathcal{P} \subset \mathcal{O}_N$ above 23.*

Proof. Let us come back to the factorization of 23 in $\mathcal{O}_N$. Since $23 = \mathfrak{p}_1^2\mathfrak{p}_2$, and in N all primes must have the same exponent, $\mathfrak{p}_2$ must be a square (say, $\mathfrak{p}_2 = \mathfrak{r}^2$), with $\mathfrak{r}$ a prime in $\mathcal{O}_N$. Because the extension is Galois, we have the formula $6 = efg$, with $e = 2$ and $g \geq 2$. We must have $f = 1$ and $g = 3$, so $\mathfrak{p}_1 = \mathfrak{s}_1\mathfrak{s}_2$. All in all, $23\mathcal{O}_N = \mathfrak{r}^2\mathfrak{s}_1^2\mathfrak{s}_2^2$. Since $\mathrm{Gal}(N \mid K)$ acts transitively on the set $\{\mathfrak{s}_1, \mathfrak{s}_2\}$ of primes dividing $\mathfrak{p}_1$, its generator τ swaps them. If we think of the action on the primes dividing 23, this must mean that $\tau(\mathfrak{r}) = \mathfrak{r} \Rightarrow \tau \in D_{\mathfrak{r}/23}$, which is a subgroup of $\mathrm{Gal}(N \mid \mathbb{Q})$ with order $ef = 2$. Therefore, $K = N^{<\tau>} = N^{D_{\mathfrak{r}/23}}$.

□