Exercise 9.1.1. Let L be the splitting field of the polynomial $t^{13}-1$. Find all subgroups of $\mathrm{Gal}_{\mathbb{Q}}(L)$.

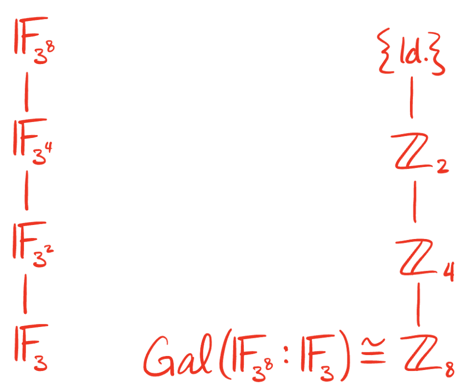
Solution. Let $f = t^{13}-1$. Since 13 is prime, we have that $f = (t-1)g$ where $g = t^{12}+\cdots+t+1 = \Phi_{13}$ is the 13th cyclotomic polynomial. We have that L is the splitting field of f, so it is also the splitting field for Φ_{13}. We know $\mathrm{Gal}_K(f) = \mathrm{Gal}_K(L)$ and by theorem $\mathrm{Gal}_{\mathbb{Q}}(\Phi_{13}) = \mathbb{Z}_{13}^* = \mathbb{Z}_{12}$, so $\mathrm{Gal}_{\mathbb{Q}}(L) \cong \mathbb{Z}_{12}$. From group theory, the only subgroups of a cyclic group $\mathbb{Z}_n$ are the unique subgroups $\langle d\rangle$ generated by the divisors d of n, which have order n/d. Thus the subgroups of $\mathrm{Gal}_{\mathbb{Q}}(L)$ are $\mathrm{Gal}_{\mathbb{Q}}(L) = \mathbb{Z}_{12}$, $\mathbb{Z}_6$, $\mathbb{Z}_4$, $\mathbb{Z}_3$, $\mathbb{Z}_2$, and the trivial group $\{\mathrm{Id.}\}$. □

Exercise 9.1.2. How many intermediate subfields are there in the extension $L:\mathbb{Q}$?

Solution. By the Fundamental Theorem of Galois Theory, there is a bijection between the set of intermediate fields of a field extension $L:K$ and the set of subgroups of the Galois group of that same extension. By Exercise 9.1.1 we have that $\mathrm{Gal}_{\mathbb{Q}}(L)$ has 6 subgroups, so by the Fundamental Theorem of Galois Theory have that there are 6 intermediate fields in the extension $L:\mathbb{Q}$, including L and $\mathbb{Q}$. □

Exercise 9.2. Draw the lattice of subfields and corresponding lattice of subgroups of $\mathrm{Gal}_{\mathbb{F}_3}(\mathbb{F}_{3^8})$. Find orders of all subgroups of $\mathrm{Gal}_{\mathbb{F}_3}(\mathbb{F}_{3^8})$.

Solution. Since $p=3$ is prime and $q=3^8$ is of the form p^n for some $n\in\mathbb{N}$, we know that $\mathrm{Gal}(\mathbb{F}_3 : \mathbb{F}_{3^8}) \cong \mathbb{Z}/8\mathbb{Z} \cong \mathbb{Z}_8$. Then by the same reasoning as in Exercise 9.1.1, we have that the subgroups of $\mathrm{Gal}(\mathbb{F}_3 : \mathbb{F}_{3^8})$ (up to isomorphism) are $\mathbb{Z}_8$, $\mathbb{Z}_4$, $\mathbb{Z}_2$, and $\{\mathrm{Id.}\}$. The orders of these subgroups are obviously 8, 4, 2, and 1 respectively.



□

Exercise 9.3. Prove Artin's theorem: let $[L:K]<\infty$, $G := \mathrm{Gal}_K(L)$. Then $[L:L^G]$ is a Galois extension.

Solution. We are given that $L:K$ is a finite extension. By theorem, we have that $|\mathrm{Gal}(L:K)| \le [L:K]$, so G is a finite group. So we know $\mathrm{Gal}_K(L) \leqslant \mathrm{Aut}(L)$ and $|G|<\infty$, and by theorem we have that $L:L^G$ is a finite Galois extension. □

Exercise 9.4. Let $L : K$ be a finite Galois extension, $G := \mathrm{Gal}_K(L)$. For any $\alpha \in L$ define

$$\mathrm{Tr}(\alpha) = \sum_{g \in G} g(\alpha) \quad \text{and} \quad \mathrm{Norm}(\alpha) = \prod_{g \in G} g(\alpha).$$

Prove that for an arbitrary $\alpha \in L$ one has $\mathrm{Tr}(\alpha), \mathrm{Norm}(\alpha) \in K$.

Solution. Since $L : K$ is a Galois extension, we have that $L^G = K$. Then $k \in K$ iff $h(k) = k$ for all $h \in G$. Notice that

$$h(\mathrm{Tr}(\alpha)) = h\left(\sum_{g \in G} g(\alpha)\right) = \sum_{g \in G} h(g(\alpha)) = \sum_{i \in G} i(\alpha) = \mathrm{Tr}(\alpha),$$

and

$$h(\mathrm{Norm}(\alpha)) = h\left(\prod_{g \in G} g(\alpha)\right) = \prod_{g \in G} h(g(\alpha)) = \prod_{i \in G} i(\alpha) = \mathrm{Norm}(\alpha).$$

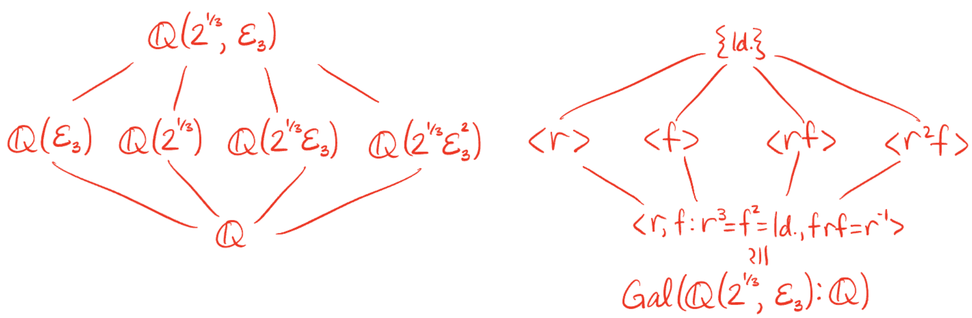
Thus $\mathrm{Tr}(\alpha), \mathrm{Norm}(\alpha) \in K$ for all $\alpha \in L$. $\square$

Exercise 9.5.1. Find all of the subfields of $\mathbb{Q}(2^{1/3}, e^{2\pi i/3})$.

Solution. We can write $\mathbb{Q}(2^{1/3}, e^{2\pi i/3}) = \mathbb{Q}(2^{1/3}, \varepsilon_3)$ where $\varepsilon_3 = \exp(2\pi i/3)$. Then, subfields of $\mathbb{Q}(2^{1/3}, \varepsilon_3)$ are $\mathbb{Q}(2^{1/3}, \varepsilon_3)$, $\mathbb{Q}(\varepsilon_3)$, $\mathbb{Q}(2^{1/3})$, $\mathbb{Q}(2^{1/3}\varepsilon_3)$, $\mathbb{Q}(2^{1/3}\varepsilon_3^2)$, and $\mathbb{Q}$. $\square$

Exercise 9.5.2. Draw the lattice of subfields and corresponding lattice of subgroups of $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(2^{1/3}, e^{2\pi i/3}))$.

Solution. The field $\mathbb{Q}(2^{1/3}, \varepsilon_3)$ is a splitting field for $t^3 - 2$ over $\mathbb{Q}$, so it is separable since any irreducible polynomial over a field of characteristic 0 is separable. Also, we note that the roots of $t^3 - 2$ are $\sqrt[3]{2}, \varepsilon_3\sqrt[3]{2}$, and $\varepsilon_3^2\sqrt[3]{2}$. Consider the permutation $\sigma : \sqrt[3]{2} \mapsto \varepsilon_3\sqrt[3]{2}$ such that σ fixes ε_3, and let τ be complex conjugation. Notice that $\sigma^3 = \tau^2 = \mathrm{Id.}$ and $\tau\sigma\tau(\sqrt[3]{2}) = \tau\sigma(\sqrt[3]{2}) = \tau(\varepsilon_3\sqrt[3]{2}) = \varepsilon_3^2\sqrt[3]{2} = \sigma^{-1}(\sqrt[3]{2})$. These are the defining characterisitics of the group D_3, so $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(2^{1/3}, e^{2\pi i/3})) \cong D_3 = \langle r, f : r^3 = f^2 = \mathrm{Id.}, frf = r^{-1}\rangle$. The only subgroups of D_3 are $D_3, \langle r\rangle, \langle f\rangle, \langle rf\rangle, \langle r^2 f\rangle$, and $\{\mathrm{Id.}\}$.



$\square$