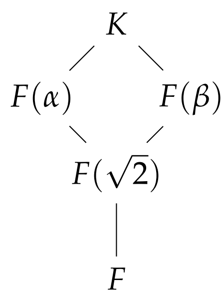
MODERN ALGEBRA 2: PRACTICE PROBLEMS FOR THE FINAL

Problem. Let $F = \mathbf{Q}(\omega)$. Determine the Galois group over F of the splitting field of (a) $\sqrt[3]{2+\sqrt{2}}$ (b) $\sqrt{2+\sqrt[3]{2}}$.

Let $\alpha = \sqrt[3]{2+\sqrt{2}}$ and $\beta = \sqrt[3]{2-\sqrt{2}}$. Consider $K = F(\alpha, \beta)$. Then K is a splitting field of the polynomial $p(x) = (x^3 - \alpha^3)(x^3 - \beta^3)$, which has coefficients in F. We do not yet know that $p(x)$ is irreducible. In any case, the irreducible polynomial of α must divide $p(x)$, and hence K contains the splitting field of the irreducible polynomial of α. Our goal is to determine $\mathrm{Gal}(K/F)$, and use it to find the irreducible polynomial of α, and its splitting field.

We have the following diagram of subfields



.

The extension $F(\sqrt{2})/F$ has degree 2. The extension $F(\alpha)/F(\sqrt{2})$ has degree 3. This is equivalent to showing that $2+\sqrt{2}$ is not a cube in $F(\sqrt{2})$. If it were, then $2-\sqrt{2}$ would also be a cube (of the conjugate), and their product 2 would also be a cube. But 2 is clearly not a cube in $F(\sqrt{2})$ (see the next lemma).

Note that the group $\mathrm{Gal}(F(\sqrt{2})/F)$ is cyclic of order 2 generated by $\sqrt{2} \mapsto -\sqrt{2}$, and the group $\mathrm{Gal}(F(\alpha)/F(\sqrt{2}))$ is cyclic of order 3 generated by $\alpha \mapsto \omega\alpha$. Since $\mathrm{Gal}(K/F)$ surjects onto $\mathrm{Gal}(F(\sqrt{2})/F)$, there must be an automorphism of K that sends $\sqrt{2}$ to $\sqrt{-2}$. Since $\mathrm{Gal}(K/F(\sqrt{2}))$ surjects onto $\mathrm{Gal}(F(\alpha)/F(\sqrt{2}))$, there must be an automorphism of K that sends α to $\omega\alpha$. Likewise, there must be an automorphism of K that sends β to $\omega\beta$.

Let us now consider the action of $\mathrm{Gal}(K/F)$ on the six roots $\{\alpha, \omega\alpha, \omega^2\alpha, \beta, \omega\beta, \omega^2\beta\}$ of our polynomial $p(x)$. Let us divide the sixtuple into two triples $A = \{\alpha, \omega\alpha, \omega^2\beta\}$ and $B = \{\beta, \omega\beta, \omega^2\beta\}$. Since $\mathrm{Gal}(K/F)$ includes an automorphism that takes α to $\omega\alpha$, the three elements of A lie in one orbit. Similarly, the three elements of B lie in one orbit. Note that the elements of A cube to $2+\sqrt{2}$ and the elements of B cube to $2-\sqrt{2}$. Since $\mathrm{Gal}(K/F)$ includes an automorphism that takes $\sqrt{2}$ to $-\sqrt{2}$, such an automorphism must take elements of A to elements of B. We deduce that the entire sixtuple is one orbit of $\mathrm{Gal}(K/F)$. As a consequence, $p(x)$ is irreducible over F and K is indeed its splitting field.

As far as $G = \mathrm{Gal}(K/F)$ is concerned, we know the following. We have a surjection

$$G \to \mathrm{Gal}(\mathbf{F}(\sqrt{2})/F) \cong \mathbf{Z}/2\mathbf{Z},$$

whose kernel $N = \mathrm{Gal}(K/\mathbf{F}(\sqrt{2}))$ surjects onto $\mathrm{Gal}(F(\alpha)/F(\sqrt{2})) \cong \mathbf{Z}/3\mathbf{Z}$ and onto $\mathrm{Gal}(F(\beta)/F(\sqrt{2})) \cong \mathbf{Z}/2\mathbf{Z}$. By combining the two, we get a homomorphism

$$\phi\colon N \to \mathrm{Gal}(F(\alpha)/F(\sqrt{2})) \times \mathrm{Gal}(F(\beta)/F(\sqrt{2})) \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}.$$

See that ϕ must be injective—an automorphism in $\ker \phi$ fixes α and β, and hence all of K. Either ϕ is an isomorphism (in which case $N \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$, $\deg(K/F(\sqrt{2})) = 9$, and $F(\alpha) \neq F(\beta)$) or an injection (in which case $N \cong \mathbf{Z}/3\mathbf{Z}$, $\deg(K/F(\sqrt{2})) = 3$, and $F(\alpha) = F(\beta)$.) We claim that the first is true by contradiction. Suppose the second, and let the image of N in $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ be generated by (i, j). Note that (i, j) corresponds to a pair of automorphisms (σ, τ) where $\sigma\colon \alpha \to \omega^i\alpha$ and $\tau\colon \beta \to \omega^j\beta$. Since the projection from N to both factors is surjective, neither i nor j is zero. Therefore, either $i = j$ or $i = -j$. Set

$$\gamma = \begin{cases} \alpha\beta & \text{if } i = -j \\ \alpha/\beta & \text{if } i = j. \end{cases}$$

Then γ is fixed by all of N, and therefore must be an element of $F(\sqrt{2})$. We can check explicitly that neither $\alpha\beta$ nor α/β lies in $F(\sqrt{2})$ (see the next lemma).

In summary, we have a surjection $\mathrm{Gal}(K/F) \to \mathbf{Z}/2\mathbf{Z}$ with kernel $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$. This makes $\mathrm{Gal}(K/F)$ a semidirect product

$$\mathrm{Gal}(K/F) \cong (\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}) \rtimes \mathbf{Z}/2\mathbf{Z}.$$

Although this is not a complete description, we will stop at this stage.

Lemma 1. *Let $\alpha = \sqrt[3]{2+\sqrt{2}}$ and $\beta = \sqrt[3]{2-\sqrt{2}}$. Then neither $\alpha\beta$ nor α/β is in $\mathbf{Q}(\omega, \sqrt{2})$.*

Proof. We must prove that $(\alpha\beta)^3$ and $(\alpha/\beta)^3$ are not cubes in $\mathbf{Q}(\omega, \sqrt{2})$. It suffices to show that they are not cubes in $\mathbf{Q}(\sqrt{2})$. Since $\mathbf{Q}(\omega, \sqrt{2})/\mathbf{Q}(\sqrt{2})$ is a quadratic extension, an element that is not a cube in $\mathbf{Q}(\sqrt{2})$ cannot be a cube in $\mathbf{Q}(\omega, \sqrt{2})$.

We have $(\alpha\beta)^3 = 2$. Since 2 is not a cube in $\mathbf{Q}$, it cannot be a cube in a quadratic extension of $\mathbf{Q}$; in particular, not in $\mathbf{Q}(\sqrt{2})$.

We have $(\alpha/\beta)^3 = 3 + 2\sqrt{2}$ and we want to show that $x^3 - (3+2\sqrt{2})$ is irreducible over $\mathbf{Q}(\sqrt{2})$. Note that this would follow if we showed that $(x^3 - (3+2\sqrt{2}))(x^3 - (3-2\sqrt{2}))$ is irreducible over $\mathbf{Q}$. One can do that, but here is a slicker argument (but still using only the things we have learned!). We want to show that the polynomial $x^3 - (3+2\sqrt{2})$ is irreducible over $\mathbf{Q}(\sqrt{2})$. Since $\mathbf{Q}(\sqrt{2})$ is the fraction field of the UFD $\mathbf{Z}[\sqrt{2}]$, it suffices to show that $x^3 - (3+2\sqrt{2})$ is irreducible over $\mathbf{Z}[\sqrt{2}]$. For this, it suffices to show that $x^3 - (3+2\sqrt{2})$ is irreducible modulo a prime of $\mathbf{Z}[\sqrt{2}]$. Consider $\pi = 3 - \sqrt{2}$. Then

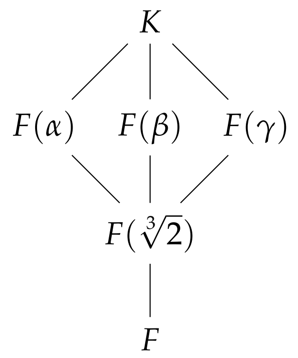
$$\mathbf{Z}[\sqrt{2}]/(\pi) = \mathbf{Z}[t]/(t^2 - 2, 3 - t) = \mathbf{Z}/7\mathbf{Z},$$

so π is prime. We have

$$x^3 - (3+2\sqrt{2}) \equiv x^3 - 9 \equiv x^3 - 2 \pmod{\pi},$$

and $x^3 - 2$ is irreducible over $\mathbf{Z}/7\mathbf{Z}$ since 2 is not a cube modulo 7. □

A similar strategy works for $\alpha = \sqrt{2+\sqrt[3]{2}}$. I will not spell out all the details, but we get a sixtuple of roots $\alpha, -\alpha, \beta, -\beta, \gamma, -\gamma$, where $\alpha = \sqrt{2+\sqrt[3]{2}}$, $\beta = \sqrt{2+\omega\sqrt[3]{2}}$, and $\gamma = \sqrt{2+\omega^2\sqrt[3]{2}}$. The diagram becomes



The group $G = \mathrm{Gal}(K/F)$ surjects onto $\mathrm{Gal}(F(\sqrt[3]{2})/F) \cong \mathbf{Z}/3\mathbf{Z}$, and the kernel injects into $\mathrm{Gal}(F(\alpha)/F(\sqrt[3]{2})) \times \mathrm{Gal}(F(\beta)/F(\sqrt[3]{2})) \times \mathrm{Gal}(F(\gamma)/F(\sqrt[3]{2})) \cong (\mathbf{Z}/2\mathbf{Z})^3$. We must then determine the image of this injection. As before, it turns out to be everything (but it's harder to show). In the end, we get

$$\mathrm{Gal}(K/F) \cong (\mathbf{Z}/2\mathbf{Z})^3 \rtimes \mathbf{Z}/3\mathbf{Z}.$$