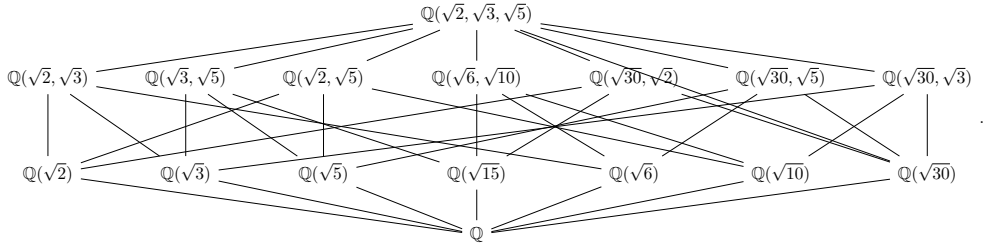
MATH 5591H HOMEWORK 11

BRENDAN WHITAKER

14.2 Exercises

3. *Determine the Galois group of* $(x^2-2)(x^2-3)x^2-5)$. *Determine all the subfields of the splitting field of this polynomial.*

We draw the subfield lattice of $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q}$. Note that every nonidentity element is of order 2, and the whole group is of order 8, so the Galois group is isomorphic to $\mathbb{Z}_2^3$.



10. *Determine the Galois group of the splitting field over* $\mathbb{Q}$ *of* x^8-3.

Let $\alpha=\sqrt[8]{3}$ and $\omega=e^{2\pi i/8}$. Note:

$$\omega^2=e^{2\pi i/4}=e^{\pi i/2}=\sqrt{e^{\pi i}}=\sqrt{-1}=i.$$

And $\omega=\sqrt{e^{2\pi i/4}}=\sqrt{i}=\frac{1+i}{\sqrt{2}}$. Note $\sqrt{2}=\frac{1+i}{\omega}=\frac{1+\omega^2}{\omega}$. So $\sqrt{2}\in\mathbb{Q}(\omega)$. Now the roots of $f(x)=x^8-3$ are $\alpha\omega^k$ where $k=0,...,7$, and thus the splitting field is $\mathbb{Q}(\alpha,\omega)$. We write out our options for constructing the automorphisms in the Galois group. We have 8 options to map α to and 4 options to map ω to (since $\varphi(8)=4$):

$$\begin{aligned}&\alpha\mapsto\alpha\omega^k, k=0,...,7\\&\omega\mapsto\omega,\omega^3,\omega^5,\omega^7.\end{aligned}\tag{1}$$

Since none of these combinations give us equivalent maps, we have exactly $8\cdot4=32$ automorphisms in our group, thus $|\mathrm{Gal}(f(x))|=|G|=32$. So let $\varphi_{k_1,l_1},\varphi_{k_2,l_2}\in G$, where $\varphi_{k,l}:\alpha\mapsto\alpha\omega^k,\varphi_{k,l}:\omega\mapsto\omega^l$. Then we have:

$$\begin{aligned}&\varphi_{k_2,l_2}\circ\varphi_{k_1,l_1}(\alpha)=\varphi_{k_2,l_2}(\alpha\omega^{k_1})=\alpha\omega^{k_2}\omega^{k_1l_2}=\alpha\omega^{k_2+k_1l_2}\\&\varphi_{k_2,l_2}\circ\varphi_{k_1,l_1}(\omega)=\varphi_{k_2,l_2}(\omega^{l_1})=\omega^{l_1l_2}.\end{aligned}\tag{2}$$

Thus $\varphi_{k_2,l_2}\circ\varphi_{k_1,l_1}=\varphi_{k_2+k_1l_2 \bmod 8,l_1l_2 \bmod 8}$, and this multiplication rule completely defines the Galois group. Furthermore, from this we see $G\cong\mathbb{Z}_8\rtimes V_4$, the nontrival semidirect product of $\mathbb{Z}_8$ and the Klein 4-group.

13. *Prove that if the Galois group of the splitting field of a cubic over* $\mathbb{Q}$ *is the cyclic group of order 3, then all the roots of the cubic are real.*

Proof. Suppose the Galois group of the splitting field of a cubic $f(x)$ is $\mathbb{Z}_3$. Note since this is a group of the form $\mathbb{Z}_p$ for p prime, we know that it has non nontrivial proper subgroups. Suppose we had an non-real root. Then we know that if $K/\mathbb{Q}$ is the splitting field of f, then $i\in K\Rightarrow\mathbb{Q}(i)/\mathbb{Q}$ is a subextension of K. But note that $\mathbb{Q}(i)/\mathbb{Q}$ has degree 2, and the Galois theorem gives us a bijection between nontrivial subgroups of the Galois group and nontrivial subextensions, hence $[K:\mathbb{Q}]=3$. If $\mathbb{Q}(i)$ were a subextension of K, we would have $2|3$, a contradiction, so all roots must be real. □

Date: SP18.

14. *Show that $K = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a cyclic quartic field, i.e., is a Galois extension of degree 4 with a cyclic Galois group.*

Proof. Recall that an extension is Galois if and only if it is the splitting field of a separable polynomial. Note that $\alpha = \sqrt{2+\sqrt{2}}$ is a root of $f(x) = (x^2-2)^2 - 2 = x^4 - 4x^2 + 2$. We show that this is the minimal polynomial of α by showing it is irreducible. Note that $2 \nmid 1$, the leading coefficient, and $2|-4, 2$, and $2^2 \nmid 2$, so it is irreducible by Eisenstein's criterion. So $\deg \alpha = 4 \Rightarrow [K:\mathbb{Q}] = 4$. Note the roots of f are $\pm\sqrt{2\pm\sqrt{2}}$, and so it has no multiple roots $\Rightarrow$ it is separable. So we need only prove that K is the splitting field of f. Clearly we have $x-\alpha$ and $x+\alpha$ for the roots of the form $\pm\sqrt{2+\sqrt{2}}$. So we need only show $\sqrt{2-\sqrt{2}} \in K$. Note since $\alpha^2 = 2+\sqrt{2}$, we know $\sqrt{2} \in K$. But $\frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}}\frac{\sqrt{2-\sqrt{2}}}{\sqrt{2-\sqrt{2}}} = \frac{\sqrt{2}\sqrt{2-\sqrt{2}}}{\sqrt{4-2}} = \sqrt{2-\sqrt{2}} = \beta$, thus $\pm\beta \in K$, and hence K is the splitting field of f, so K is Galois. Now note since all 3 conjugates of α also have degree 4, we know that all automorphsims of K are given by $\alpha \mapsto \alpha, -\alpha, \beta, -\beta$. Denote these by $1, \varphi_1 ..., \varphi_3$, respectively. Then we know:

$$\beta = \frac{\alpha^2 - 2}{\alpha}. \tag{3}$$

So:

$$\varphi_2(\beta) = \varphi_2\left(\frac{\alpha^2-2}{\alpha}\right) = \frac{\beta^2-2}{\beta} = -\frac{\sqrt{2}}{\beta} = -\alpha. \tag{4}$$

Thus the order of φ_2 is > 2 which means it must be 4 since our group has order 4, so we know that our group must be isomorphic to $\mathbb{Z}_4$. □

15. *(Biquadratic Extensions) Let F be a field of characteristic $\neq 2$.*

(a) *if $K = F(\sqrt{D_1}, \sqrt{D_2})$ where $D_1, D_2 \in F$ have the property that none of D_1, D_2, D_1D_2 is a square in F, prove that K/F is a Galois extension with Gal(K/F) isomorphic to the Klein 4-group.*

Proof. Since D_1, D_2 are not squares, we know $F(\sqrt{D_1})/F$ and $F(\sqrt{D_2})/F$ are both extensions of degree 2. And since D_1D_2 is not a square, we know that $F(\sqrt{D_2})/F(\sqrt{D_1})$ is a nontrivial extension (has degree 2). Thus we know that K/F has degree 4. We wish to first show it is Galois. Let $\alpha = \sqrt{D_1}, \beta = \sqrt{D_2}$. Then $m_{\alpha,F} = x^2 - D_1, m_{\beta,F} = x^2 - D_2$. And since the roots of these are $\pm\alpha, \pm\beta$, we know they are both separable, so α, β are separable, so K/F is separable. Also, K is normal since the only conjugates of α, β are $-\alpha, -\beta$, so K/F is normal and separable, thus it is Galois. We enumerate the automorphisms of K in the Galois group G. We have choices of mappings:

$$\begin{aligned} \alpha &\mapsto \alpha, -\alpha \\ \beta &\mapsto \beta, -\beta. \end{aligned} \tag{5}$$

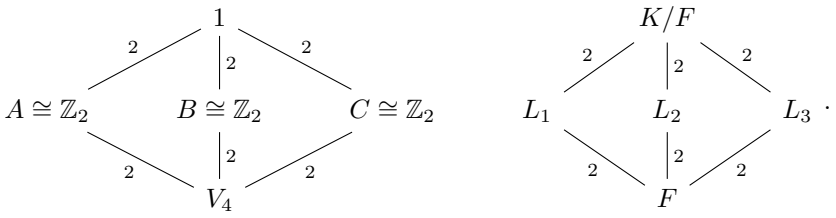
So we have:

$$\begin{aligned} 1 &: \alpha \mapsto \alpha, \quad \beta \mapsto \beta \\ \varphi_1 &: \alpha \mapsto -\alpha, \quad \beta \mapsto \beta \\ \varphi_2 &: \alpha \mapsto \alpha, \quad \beta \mapsto -\beta \\ \varphi_3 &: \alpha \mapsto -\alpha, \quad \beta \mapsto -\beta. \end{aligned} \tag{6}$$

Clearly, each has order 2, so it is V_4. □

(b) *Conversely, suppose K/F is a Galois extension with Gal(K/F) isomorphic to V_4. Prove that $K = F(\sqrt{D_1}, \sqrt{D_2})$ where $D_1, D_2 \in F$ have the property that none of D_1, D_2, D_1D_2 is a square in F.*

Proof. Suppose K/F is Galois with $G = \text{Gal}(K/F)$ isomorphic to V_4. By the Galois theorem, we know that the subgroup lattice of G is in (flipped) bijection with the subextension lattice of K/F. So since we know the lattice of V_4, we know the structure of the subextensions of K:



Since they are of degree 2, all of L_1, L_2, L_3 must be of the form $F(\sqrt{D_i})$ for some D_i not a square in F. Furthermore D_iD_j cannot be a square in F, otherwise L_i, L_j are the same extension, which is a contradiction. □

14.3 Exercises

8. *Determine the splitting field of the polynomial $f(x) = x^p - x - a$ over $\mathbb{F}_p$ where $a \neq 0, a \in \mathbb{F}_p$. Show explicitly that the Galois group is cyclic. [Show $\alpha \mapsto \alpha + 1$ is an automorphism.]*

Proof. Suppose α is a root. Then we have $\alpha^p - \alpha + a = 0$. Behold:

$$\begin{aligned}(\alpha+1)^p - (\alpha+1) - a &= \left(\sum_{k=0}^{p}\binom{p}{k}\alpha^k\right) - \alpha - 1 - a \\ &= \left(\sum_{k=1}^{p-1}\binom{p}{k}\alpha^k\right) + \alpha^p - \alpha - a \\ &= \sum_{k=1}^{p-1}\binom{p}{k}\alpha^k \\ &= \sum_{k=1}^{p-1}\frac{p!}{k!(p-k)!}\alpha^k.\end{aligned} \tag{7}$$

We claim that $\frac{p!}{k!(p-k)!}$ is divisible by p for all integer values of k in the range $[1, p-1]$. Note for these values of k that $p \nmid (k!(p-k)!)$ but that $p|p!$, and the binomial coefficient is an integer, so we must have that $p\left|\left(\frac{p!}{k!(p-k)!}\right)\right.$. Thus:

$$\sum_{k=1}^{p-1}\frac{p!}{k!(p-k)!}\alpha^k \mod p \equiv 0.$$

And since we are over $\mathbb{F}_p$, we know that $\alpha + 1$ must then be a root. The roots of f are $\alpha + k$ for $k = 0, ..., p-1$, hence f is separable, and so $\mathbb{F}_p(\alpha)$ is the splitting field of a separable polynomial, and thus is Galois. And we have an automorphism $\varphi : \alpha \mapsto \alpha + 1$ because an inverse is given by $\alpha \mapsto \alpha - 1 = \alpha + p - 1$, these are both field homomorphisms, and they map $\mathbb{F}_p(\alpha) \to \mathbb{F}_p(\alpha)$, so then G must be cyclic since any other automorphism maps $\alpha \mapsto \alpha + k$ which is φ^k. □