Math 121, Winter 2023, Homework 5 Solutions

Section 14.2

Problem 6. *Let $K = \mathbb{Q}(\sqrt{2}, i)$ and let $F_1 = \mathbb{Q}(i), F_2 = \mathbb{Q}(\sqrt{2}), F_3 = \mathbb{Q}(\sqrt{-2})$. Prove that $Gal(K/F_1) = \mathbb{Z}/8\mathbb{Z}$, $Gal(K/F_2) = D_8$, $Gal(K/F_3) = Q_8$.*

Solution. Use the example in Section 14.2, and the diagrams on pages 580-1. These diagrams (along with the Galois correspondence) tell us that $\mathrm{Gal}(K/F_1) = \langle\sigma\rangle, \mathrm{Gal}(K/F_2) = \langle\sigma^2, \tau\rangle, \mathrm{Gal}(K/F_3) = \langle\sigma^2, \tau\sigma^3\rangle$. σ has order 8, so $\mathrm{Gal}(K/F_1) = \mathbb{Z}/8\mathbb{Z}$.

The dihedral group of order 8 has the presentation $\langle s, t | s^4 = t^2 = 1, tst = s^{-1}\rangle$. We have $(\sigma^2)^4 = 1, \tau^2 = 1$, and $\tau\sigma^2\tau = \tau^2(\sigma^3)^2 = (\sigma^2)^{-1}$, so since $\mathrm{Gal}(K/F_2)$ has order 8, it must be D_8.

Finally, the quaternion group has the presentation $\langle n, i, j, k | n^2 = 1, i^2 = j^2 = k^2 = ijk = n\rangle$. Let $n = \sigma^4, i = \sigma^2, j = \sigma\tau = \tau\sigma^3, k = \tau\sigma = \sigma^3\tau$. Then all the relations of Q_8 are satisfied (for example, $ijk = \sigma^2\sigma\tau\tau\sigma = \sigma^4 = n$), so since $\mathrm{Gal}(K/F_3)$ has order 8, it must be Q_8.

(There are simpler ways to do this if we assume knowledge about finite groups of order 8. In particular, D_8 and Q_8 are the only nonabelian groups of order 8, and we can distinguish between them by comparing the number of elements of order 2.)

Problem 7. *Determine all the subfields of the splitting field of $x^8 - 2$ which are Galois over $\mathbb{Q}$.*

Solution. Use the example in Section 14.2, and the diagrams on pages 580-1. Let K be the splitting field of $x^8 - 2$. By the Fundamental Theorem of Galois theory, $E \subset K$ is Galois over the base field $\mathbb{Q}$ if and only if $\mathrm{Aut}(K/E)$ (the corresponding group to E in the diagrams) is normal in $G = \mathrm{Gal}(K/\mathbb{Q})$. This is a group-by-group check. Use the relation $\sigma\tau\sigma^{-1} = \tau\sigma^2$, and the fact that any index-2 subgroup is normal; conjugate the generators by both σ and τ to see if their images generate the same group. To be conjugate, subgroups must have the same number of generators, which must have the same orders.

We conclude that the normal subgroups in G are $G, \langle\sigma^2, \tau\rangle, \langle\sigma\rangle, \langle\sigma^2, \tau\sigma^3\rangle, \langle\sigma^2\rangle, \langle\sigma^4\rangle$, and 1, and therefore the intermediate fields which are Galois over $\mathbb{Q}$ are $\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(i, \sqrt{2}), \mathbb{Q}(i, \sqrt[4]{2})$, and $K = \mathbb{Q}(i, \sqrt[8]{2})$.

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

Solution. Let $f(x) = x^4 - 4x^2 + 2$. This is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with the prime 2, and its roots (over a splitting field) are $\pm\theta_\pm := \pm\sqrt{2 \pm \sqrt{2}}$ (note: distinct). Since $\theta_+\theta_- = \sqrt{2}$, $\theta_- = \frac{\theta_+^2 - 2}{\theta_+} \in \mathbb{Q}(\theta_+)$, so $\mathbb{Q}(\theta_+)$ is the splitting field for f, and therefore is Galois over $\mathbb{Q}$.

Since the degree of the extension is 4, to show that the Galois group is cyclic, we just need to show that is has an element of degree 4. One possibility is an automorphism sending θ_+ to θ_- since then $\sqrt{2} = \theta_+^2 - 2 \mapsto \theta_-^2 - 2 = -\sqrt{2}$, and so $\theta_- \mapsto \frac{-\sqrt{2}}{\theta_-} = -\theta_+$, so the order of this automorphism would be 4. Such an automorphism is guaranteed by the following lemma:

Lemma 0.1. *Let $f \in F[x]$ be irreducible, and let α be a root of f. If $F(\alpha)$ is the splitting field for f over F, then $Aut(F(\alpha)/F)$ consists of precisely one automorphism sending α to each root of f.*

Proof. Each automorphism of $F(\alpha)$ fixing F depends only on the image of α, so we need only show that there exists an automorphism of $F(\alpha)$ fixing F and sending α to β. Since $F(\alpha) = F(\beta)$, this is a consequence of Theorem 13.8, taking $F' = F$ and $\phi = id$. □

Problem 19. *Show that $N_{K/F}(a\alpha) = a^n N_{K/F}(\alpha)$ and $Tr_{K/F}(a\alpha) = aTr_{K/F}(\alpha)$ for all a in the base field F, In particular show that $N_{K/F}(a) = a^n$ and $Tr_{K/F}(a) = na$ for all $a \in F$.*

Solution. $N_{K/F}(\alpha)$ is the product of the Galois conjugates of α, while $Tr_{K/F}(\alpha)$ is their sum. If $\sigma \in \mathrm{Gal}(K/F)$, then $\sigma(a\alpha) = a\sigma(\alpha)$, so when we multiply α by a, each Galois conjugate is multiplied by a. The formulas in the first sentence of the problem follow.

The second sentence follows from the first, plus the fact that $N_{K/F}(1) = Tr_{K/F}(1) = 1$, since every automorphism fixes 1.

Problem 23. *Let K be a Galois extension of F with cyclic Galois group of order n generated by σ. Suppose $\alpha \in K$ has $N_{K/F}(\alpha) = 1$. Prove that α is of the form $\alpha = \frac{\beta}{\sigma\beta}$ for some nonzero $\beta \in K$.*

Solution. As in the hint, choose $\theta \in K$ and let

$$\beta = \theta + \alpha\sigma(\theta) + \alpha\sigma(\alpha)\sigma^2(\theta) + \cdots + \alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}(\theta).$$

Then,

$$\sigma(\beta) = \sigma(\theta) + \sigma(\alpha)\sigma^2(\theta) + \sigma(\alpha)\sigma^2(\alpha)\sigma^3(\theta) + \cdots + \sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-1}(\alpha)\theta,$$

so

$$\alpha\sigma(\beta) = \alpha\sigma(\theta) + \alpha\sigma(\alpha)\sigma^2(\theta) + \alpha\sigma(\alpha)\sigma^2(\alpha)\sigma^3(\theta) + \cdots + \theta = \beta,$$

noting that the product of all the Galois conjugates of α is $N_{K/F}(\alpha) = 1$.

This means that $\alpha = \frac{\beta}{\sigma(\beta)}$ as long as $\beta \neq 0$. By the linear independence of characters, $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are linearly independent, so the character

$$\chi := 1 + \alpha\sigma + \alpha\sigma(\alpha)\sigma^2 + \cdots + \alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1} \neq 0.$$

This means there exists some $\theta \in K$ such that $\beta := \chi(\theta) \neq 0$, and the above shows that $\alpha = \frac{\beta}{\sigma(\beta)}$.

Section 14.3

Problem 3. *Prove that an algebraically closed field must be infinite.*

Solution. Let F be a finite field. The polynomial $1 + \prod_{a\in F}(x - a) \in F[x]$ has no roots in F, so F is not algebraically closed.

Problem 4. *Construct the finite field of 16 elements and find a generator for the multiplicative group. How many generators are there?*

Solution. Let $f(x) = x^4+x+1 \in \mathbb{F}_2[x]$. This is irreducible of degree 4, so $F := \mathbb{F}_2[x]/(f(x))$ is a field of order 16 (which we have seen is unique up to isomorphism). Let θ be the image of x in this quotient; then $\theta^4 = \theta + 1$ and $\mathbb{F}_2[x]/(f(x)) = \{a + b\theta + c\theta^2 + d\theta^3 | a, b, c, d \in \mathbb{F}_2\}$.

Now, $|F^\times| = 16 - 1 = 15$, and since $\theta^3 \neq 1$ and $\theta^5 = \theta^2 + \theta \neq 1$, θ must have order 15; therefore, it generates $F^\times$, which must therefore be cyclic. The number of generators for $F^\times$ is $\phi(15) = 8$.

Problem 8. *Determine the splitting field of the polynomial $f(x) = x^p - x - a$ over $\mathbb{F}_p$ where $a \neq 0, a \in F_p$. Show explicitly that the Galois group is cyclic.*

Solution. Let α be a root of f over some splitting field. Then if $k \in \mathbb{F}_p$,

$$f(\alpha + k) = \alpha^p + k^p - \alpha - k - a = k^p - k = 0,$$

where we have used the Frobenius endomorphism and Fermat's Little Theorem. This produces p roots of f, so f is separable, with $\mathbb{F}_p(\alpha)$ its splitting field, and so the extension is Galois.

Now, using the lemma above, there exists $\sigma \in \mathrm{Gal}(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$ sending α to $\alpha + 1$. The order of σ is a since $\mathbb{F}_p(\alpha)$ has characteristic p, so $\mathrm{Gal}(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$ is cyclic, with σ as a generator.