Math 121, Winter 2023, Homework 7 Solutions

Section 14.6

Problem 8. *Determine the Galois group of* $f(x) = x^4 + 8x + 12$.

Solution. This is already a depressed quartic. Proving irreducibility is a bit of a pain, but the rational root theorem says that any rational roots must be $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6$, or ± 12, but none can be a root since if $|x| = 1$, $x^4 + 12 > 12 > |8x|$ and if $x \geq 2$, $x^4 + 12 > x^4 \geq 8|x|$. If $f(x) = (x^2 + ax + b)(x^2 + cx + d)$ over $\mathbb{Q}$ (or over $\mathbb{Z}$, by Gauss' Lemma), we must have $c = -a$ since f has no cubic term, and since f also has no quadratic term, we must have $b + d = -a^2$. But none of the integer factorizations $12 = bd$ have $b + d$ equaling a (negative) square, so this is impossible.

The discriminant of f is $D = -27(8^4) + 256(12)^3 = 331776 = (576)^2$. By Proposition 34, $\mathrm{Gal}(f) \subseteq A_4$.

The resolvent cubic of f is $h(x) = x^3 - 32x + 144$. We again use the rational root theorem to show that h is irreducible. The possible roots are the integer factors a of 144, and one can check that none of them are roots; thus h is irreducible. Using the list on Dummit and Foote page 615, $\mathrm{Gal}(f) = A_4$.

(Note that we can do this problem without the resolvent cubic using the ideas of Section 14.8: reducing modulo primes less than 20, we see that $\mathrm{Gal}(f)$ contains a 3-cycle and a product of two 2-cycles. Since f is irreducible, $\mathrm{Gal}(f)$ is transitive, and the only such subgroups of S_4 are A_4 and S_4. Since $\sqrt{D} \in \mathbb{Q}$, we have $\mathrm{Gal}(f) = A_4$.)

Problem 10. *Determine the Galois group of* $x^5 + x - 1$.

Solution. Note that f factors: $f(x) = (x^2 - x + 1)(x^3 + x^2 - 1)$. Both of these factors are irreducible since neither has a root modulo 2. The Galois group for the quadratic factor $g(x)$ is Z_2, and the Galois group for the cubic factor $h(x)$ is S_3, since its discriminant, $D = -23$, is not a square in $\mathbb{Q}$.

Let K_1 be the splitting field of g and let K_2 be the splitting field of h. Then $K := K_1K_2$ is the splitting field of f, and by Proposition 21, $\mathrm{Gal}(K/\mathbb{Q})$ is the subgroup of $\mathrm{Gal}(K_1/\mathbb{Q}) \times \mathrm{Gal}(K_2/\mathbb{Q})$ of pairs of elements which are equal on the intersection $K_1 \cap K_2$.

We claim that this intersection is simply $\mathbb{Q}$, so that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(K_1/\mathbb{Q}) \times \mathrm{Gal}(K_2/\mathbb{Q})$. Suppose otherwise. Since $K_1 \cap K_2 \subseteq K_1$, and K_1 has degree 2 over $\mathbb{Q}$, so must $K_1 \cap K_2$, and so $K_1 = K_1 \cap K_2$ i.e. $K_1 \subseteq K_2$. By the quadratic formula, $K_1 = \mathbb{Q}(\sqrt{-3})$. By the Galois correspondence, $\mathrm{Gal}(K_2/K_1) = A_3$ (since it must be an index 2 subgroup of S_3). Therefore, the discriminant $D = -23$ of h must be a square in $\mathbb{Q}(\sqrt{-3})$. However, this is not the case since $\sqrt{-23}$ is not a $\mathbb{Q}$-linear combination of 1 and $\sqrt{-3}$.

Section 14.7

Problem 1. *Use Cardano's Formulas to solve the equation $f(x) = x^3 + x^2 - 2 = 0$. In particular show that the equation has the real root*

$$\frac{1}{3}\left(\sqrt[3]{26 + 15\sqrt{3}} + \sqrt[3]{26 - 15\sqrt{3}} - 1\right).$$

Show directly that the roots of this cubic are $1, -1 \pm i$. Explain this by proving that

$$\sqrt[3]{26 + 15\sqrt{3}} = 2 + \sqrt{3}, \qquad \sqrt[3]{26 - 15\sqrt{3}} = 2 - \sqrt{3}$$

so that

$$\sqrt[3]{26 + 15\sqrt{3}} + \sqrt[3]{26 - 15\sqrt{3}} = 4.$$

Solution. f is associated to the depressed cubic $g(y) = y^3 - \frac{1}{3}y - \frac{52}{27}$ by the parameter shift $x = y - \frac{1}{3}$, as explained on page 630 of Dummit and Foote. The discriminant of g is $D = -4(-1/3)^3 - 27(-52/27)^2 = -100$. The quantities A and B given on page 632 of Dummit and Foote are

$$A = \sqrt[3]{-\frac{27}{2}\frac{-52}{27} + \frac{3}{2}\sqrt{300}} = \sqrt[3]{26 + 15\sqrt{3}}, \qquad B = \sqrt[3]{-\frac{27}{2}\frac{-52}{27} - \frac{3}{2}\sqrt{300}} = \sqrt[3]{26 - 15\sqrt{3}}.$$

Since A and B are both real, the real root of g is given by

$$\frac{A+B}{3} = \frac{1}{3}\left(\sqrt[3]{26 + 15\sqrt{3}} + \sqrt[3]{26 - 15\sqrt{3}}\right).$$

Because of the shift $x = y = \frac{1}{3}$, the corresponding root of f is

$$\alpha := \frac{A+B}{3} = \frac{1}{3}\left(\sqrt[3]{26 + 15\sqrt{3}} + \sqrt[3]{26 - 15\sqrt{3}} - 1\right).$$

Now, $f(1) = 1^3 + 1^2 - 2 = 1 + 1 + -2 = 0$ and $f(-1 \pm i) = (-1 \pm i)^3 + (-1 \pm i)^2 - 2 = (-1 \pm 3i + 3 \mp i) + (1 \mp 2i - 1) - 2 = 0$, so these are the roots of f, and since 1 is the only real root, we must have $\alpha = 1$.

We have $(2 \pm \sqrt{3})^3 = 8 \pm 12\sqrt{3} + 18 \pm 3\sqrt{3} = 26 \pm 15\sqrt{3}$, so

$$\sqrt[3]{26 \pm 15\sqrt{3}} = 2 \pm \sqrt{3}.$$

Thus, we have

$$\alpha = \frac{1}{3}\left(2 + \sqrt{3} + 2 - \sqrt{3} - 1\right) = \frac{1}{3}(4 - 1) = 1,$$

as desired.

Problem 4. *Let $K = \mathbb{Q}(\sqrt[n]{a})$, where $a \in \mathbb{Q}, a > 0$ and suppose $[K : \mathbb{Q}] = n$. Let E be any subfield of K and let $[E : \mathbb{Q}] = d$. Prove that $E = \mathbb{Q}(\sqrt[d]{a})$.*

Solution. By the Tower Law, $d|n$. Let L be the splitting field of $x^n - a$; then $L/\mathbb{Q}$ and L/E are Galois. We want to compute the norm $N_{K/E}(\sqrt[n]{a})$, which lies in E by Exercise 17 of Dummit and Foote, Section 14.2. However, since K/E is not necessarily Galois, we need to be careful; see the definition of norm given in that same problem. Let $H := \mathrm{Gal}(L/K)$ be the subgroup of $G := \mathrm{Gal}(L/E)$ that fixes K, and let $\sigma_1, \ldots, \sigma_k$ be a set of coset representatives for G/H (in general, this is not a group since H is not necessarily normal). Then, we have $N_{K/E}(\sqrt[n]{a}) = \sigma_1(\sqrt[n]{a}) \cdots \sigma_k(\sqrt[n]{a})$. (Note that if you do this wrong and take the product over the full Galois group, you get the $|H|$-th power of the correct norm).

For each i, $\sigma_i(\sqrt[n]{a}) = \zeta_n^{i_j}\sqrt[n]{a}$ for some i_j, so $N_{K/E}(\sqrt[n]{a}) = \zeta(\sqrt[n]{a})^k$ for some nth root of unity ζ. By the Tower Law, $k = |G|/|H| = [L : E]/[L : K] = [K : E] = n/d$, so $N_{K/E}(\sqrt[n]{a}) = \zeta(\sqrt[n]{a})^{n/d} = \zeta\sqrt[d]{a}$.

Now, $\zeta\sqrt[d]{a} \in E$, so since $E \subseteq K \subseteq \mathbb{R}$, we must have $\zeta = \pm 1$, so $E \supseteq \mathbb{Q}(\sqrt[d]{a})$. We must have $\deg \sqrt[d]{a} = d$, since $x^{n/d} - \sqrt[d]{a}$ is a degree n/d polynomial over $\mathbb{Q}(\sqrt[d]{a})$ which $\sqrt[n]{a}$ satisfies. Therefore, E and $\mathbb{Q}(\sqrt[d]{a})$ have the same degree, and thus are equal.

Problem 9. *Let F be a field of characteristic p and let K be a cyclic extension of F of degree p. Prove that $K = F(\alpha)$ where α is a root of the polynomial $x^p - x - a$ for some $a \in F$.*

Solution. First note that since K/F is cyclic (and thus Galois),

$$\mathrm{Tr}_{K/F}(-1) = \sum_{\sigma \in \mathrm{Gal}(K/F)} \sigma(-1) = p \cdot (-1) = 0$$

since $|\mathrm{Gal}(K/F)| = p$ and -1 is fixed by any automorphism. Let σ be a generator of $\mathrm{Gal}(K/F)$. By the additive version of Hilbert Theorem 90, there exists some $\alpha \in K$ such that $\alpha - \sigma(\alpha) = -1$. Let $a = \alpha^p - \alpha$. Then

$$\sigma(a) = (\alpha + 1)^p - \alpha - 1 = \alpha^p + 1 - \alpha - 1 = \alpha^p - \alpha = a,$$

where we have used the fact that the Frobenius map is a homomorphism. This means that a is fixed by σ, and since σ is a generator for $\mathrm{Gal}(K/F)$, a is fixed by the whole Galois group and thus $a \in F$. This means that $x^p - x - a \in F[x]$, and by construction has α as a root.

Finally, since $\alpha - \sigma(\alpha) = -1$, the Galois conjugates of α are $\alpha + j, 0 \leq j < p$. This is p distinct elements, so $[F(\alpha) : F] = p$. By the Tower Law, we must now have $[K : F] = 1$, so $K = F(\alpha)$.

Problem 17. *Let $D \in \mathbb{Z}$ be a squarefree integer and let $a \in \mathbb{Q}$ be a nonzero rational number. Show that $Q(\sqrt{a\sqrt{D}})$ cannot be a cyclic extension of degree 4 over $\mathbb{Q}$.*

Solution. $\alpha := \sqrt{a\sqrt{D}}$ is a root of the polynomial $f(x) = x^4 - a^2 D$. If f is reducible, the degree of $\mathbb{Q}(\sqrt{a\sqrt{D}})$ over $\mathbb{Q}$ is less than 4, so assume that f is irreducible (as it is unless $a = 0$ or $\sqrt{D} \in \mathbb{Q}$).

The roots of f are $\pm\alpha, \pm i\alpha$. Suppose $Q(\sqrt{a\sqrt{D}})$ is a cyclic extension of degree 4 over $\mathbb{Q}$; then this extension is Galois, and there exists a 4-cycle $\sigma \in \mathrm{Gal}(f)$. This means that $\sigma(\alpha) = \pm i\alpha$, so applying σ again, $\sigma^2(\alpha) = \sigma(\pm i\alpha) = \pm\sigma(i)(\pm i\alpha) = \sigma(i) \cdot i\alpha$. Since $\sigma^2(\alpha)$ must equal $-\alpha$ if σ has order 4, we must have $\sigma(i) = i$. But then i is fixed by $\mathrm{Gal}(f)$, which is a contradiction since $i \notin \mathbb{Q}$.