Math 418, Spring 2024 – Homework 9

Due: Wednesday, April 24th, at 9:00am via Gradescope.

Instructions: Students should complete and submit all problems. Textbook problems are from Dummit and Foote, *Abstract Algebra, 3rd Edition.* All assertions require proof, unless otherwise stated. Typesetting your homework using LaTeX is recommended, and will gain you 2 bonus points per assignment.

1. **Dummit and Foote #14.6.2a** *Determine the Galois group of the polynomial* $f(x) = x^3 - x^2 - 4$

   Solution. $f(x) = (x-2)(x^2+x+2)$ is reducible, so the Galois group of f is the same as the Galois group of $g(x) = x^2+x+2$. Now, g is irreducible by Eisenstein's criterion with the prime 2, which means that the splitting field of g and therefore g is a degree 2 extension of $\mathbb{Q}$, and therefore the Galois group is the only group of order 2, $\mathbb{Z}/2\mathbb{Z}$.

   For good measure, we compute the discriminant of g, which is $D = -7$. Since $\sqrt{D} = \sqrt{-7} \notin \mathbb{Q}$, this means that the Galois group of g is not contained in $A_2 = 1$, so must equal $S_2 = \mathbb{Z}/2\mathbb{Z}$.

2. **Dummit and Foote #14.6.10** *Determine the Galois group of* $x^5 + x - 1$. (*Hint: see D & F Proposition 14.21*

   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 D & F 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 $\sqrt{-3}$.

3. *Let* $p_k(x_1, \ldots, x_n) = x_1^k + x_2^k + \cdots + x_n^k$ *be the* power sum symmetric function*, and let* $e_k(x_1, \ldots, x_n) = \sum_{i_1 < \ldots < i_k} x_{i_1} \cdots x_{i_k}$ *be the elementary symmetric function. Let*

$$E(t) = \sum_{r=0}^{\infty} e_r(x_1, \ldots, x_n) t^r, \qquad P(t) = \sum_{r=1}^{\infty} p_r(x_1, \ldots, x_n) t^{r-1}.$$

Prove that

$$E(t) = \prod_{i=1}^{n} (1 + x_i t), \qquad P(t) = \sum_{i=1}^{n} \frac{x_i}{1 - x_i t} = \sum_{i=1}^{n} \frac{d}{dt} \ln \frac{1}{1 - x_i t}.$$

Solution. (We won't worry about convergence here, but notice that if $x_1, \ldots, x_n \in \mathbb{C}$ since there are finitely many x_i, we may choose some $t \in \mathbb{C}, t \neq 0$ such that $|tx_i| < 1$ for all i. Therefore, all the relevant series converge in an open neighborhood of $t = 0$.)

First, the elementary symmetric functions. We have

$$\begin{aligned} E(t) &= \sum_{r=0}^{\infty} e_r(x_1, \ldots, x_n) t^r \\ &= \sum_{r=0}^{\infty} \sum_{i_1 < \ldots < i_r} x_{i_1} \cdots x_{i_r} t^r \\ &= \sum_{r=0}^{\infty} \sum_{i_1 < \ldots < i_r} (x_{i_1} t) \cdots (x_{i_r} t) \\ &= \sum_{I \subseteq \{1,2,\ldots,n\}} \prod_{i \in I} x_i t. \end{aligned}$$

Expanding the product $\prod_{i=1}^{n} (1 + x_i t)$ using the distributive law gives the same expression; the term $\prod_{i \in I} x_i t$ corresponds to choosing $x_i t$ from the factor $1 + x_i t$ when $i \in I$, and choosing 1 when $i \notin I$.

Next, the power sum symmetric functions. We have

$$P(t) = \sum_{r=1}^{\infty} p_r(x_1, \ldots, x_n) t^{r-1} = \sum_{r=1}^{\infty} \sum_{i=1}^{n} x_i^r t^{r-1} = \sum_{i=1}^{n} \sum_{r=1}^{\infty} x_i^r t^{r-1} = \sum_{i=1}^{n} \frac{x_i}{1 - x_i t},$$

summing the geometric series in the last step. For the second equality, using the chain rule,

$$\frac{d}{dt} \ln \frac{1}{1 - x_i t} = -\frac{d}{dt} \ln(1 - x_i t) = \frac{x_i}{1 - x_i t}.$$

4. **Dummit and Foote #14.6.22** *Let* $f(x)$ *be a monic polynomial of degree* n *with roots* $\alpha_1, \ldots, \alpha_n$*. Let* e_i *be the elementary symmetric function of degree* i *in the roots and*

define $e_i = 0$ for $i > n$. Let $p_i = \alpha_1^i + \cdots + \alpha_n^i, i \geq 0$, be the sum of the ith powers of the roots of $f(x)$ Prove Newton's formulas:

$$p_n - e_1 p_{n-1} + e_2 p_{n-2} + \cdots + (-1)^{n-1} e_{n-1} p_1 + (-1)^n n e_n = 0.$$

(Hint: use solution to previous problem)

Solution. Multiply the desired equation by $(-1)^n$ and move everything but the last term onto the opposite side of the equation. This becomes

$$n e_n = \sum_{r=1}^{n} (-1)^{r-1} p_r e_{n-r.} \tag{1}$$

The right side of (1) is the coefficient of t^{n-1} in $P(-t)E(t)$since

$$P(-t)E(t) = \sum_{r=0}^{\infty} p_r (-t)^{r-1} \sum_{m=0}^{\infty} e_m t^m = \sum_{r,m \geq 0} (-1)^{r-1} p_r e_m t^{r-1+m} = \sum_{n \geq 0} \left(\sum_{r \geq 0} (-1)^{r-1} p_r e_{n-r} \right) t^{n-1}.$$

On the other hand, using the previous problem, we have

$$\begin{aligned}
\frac{d}{dt} \ln E(t) &= \frac{d}{dt} \ln \prod_{i=1}^{n} (1 + x_i t) \\
&= \sum_{i=1}^{n} \frac{d}{dt} \ln(1 + x_i t) \\
&= \sum_{i=1}^{n} \frac{d}{dt} \left(- \ln \frac{1}{1 + x_i t} \right) \\
&= \sum_{i=1}^{n} \frac{d}{d(-t)} \left(\ln \frac{1}{1 + x_i t} \right) = P(-t).
\end{aligned}$$

Using the chain rule,

$$P(-t) = \frac{d}{dt} \ln E(t) = \frac{E'(t)}{E(t)},$$

so

$$P(-t)E(t) = E'(t) = \sum_{n=0}^{\infty} n e_n t^{n-1},$$

and the coefficient of t^{n-1} is the left side of (1)

5. **Dummit and Foote #14.7.1** *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.

6. **Dummit and Foote #14.7.17** *Let $D \in \mathbb{Z}$ be a squarefree integer and let $a \in \mathbb{Q}$ be a nonzero rational number. Show that $\mathbb{Q}(\sqrt{a\sqrt{D}})$ cannot be a cyclic extension of degree 4 over $\mathbb{Q}$ (i.e. Gal($\mathbb{Q}(\sqrt{a\sqrt{D}})/\mathbb{Q}$) cannot be $\mathbb{Z}/4\mathbb{Z}$).*

   Solution. $\alpha := \sqrt{a\sqrt{D}}$ is a root of the polynomial $f(x) = x^4 - a^2D$. 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 $i \notin \mathbb{Q}$.