Math 418, Spring 2024 – Homework 7

Due: Friday, March 29th, 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 #13.3.3:** *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.

2. **Dummit and Foote #13.3.4:** *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 $\phi(15) = 8$.

3. **Dummit and Foote #13.3.8:** *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.

   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. By Dummit & Foote Theorem 13.6, there is a unique isomorphism $F(\alpha) \to F(\beta)$ fixing F and sending α to β, and since $F(\alpha) = F(\beta)$ this is an automorphism. □

Using this lemma, 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.

4. **Dummit and Foote #13.4.2:** *Find a primitive element for* $K := \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ *over* $\mathbb{Q}$.

   Solution. Since char $\mathbb{Q} = 0$, the primitive element theorem says such an element α must exist. Now, K is a Galois extension since it is the splitting field of the separable polynomial $(x^2-2)(x^2-3)(x^2-5)$. Furthermore, the extension is degree 8 since $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subsetneq K$. Let $G = \mathrm{Gal}(K/\mathbb{Q})$; this must have fixed field $\mathbb{Q}$ (proof: since $K/\mathbb{Q}$ is Galois, $|G| = [K : \mathbb{Q}] = 8$. If $E := \mathrm{Fix}G \supsetneq \mathbb{Q}$, then $[K : E] < |G| = \mathrm{Gal}(G/E)$, a contradiction).

   As we have shown in class, if $\alpha \in K$,

   $$m_{\mathbb{Q}}(\alpha) = \prod_{a \in G\alpha} (x - a),$$

   so if we can find a polynomial such that $|G\alpha| = 8$, then $m_{\mathbb{Q}}(\alpha)$ will have degree 8, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$, and so $\mathbb{Q}(\alpha) = K$.

   One such element is $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{5}$. An element of G sends

   $$\sqrt{2} \mapsto \pm\sqrt{2}, \qquad \sqrt{3} \mapsto \pm\sqrt{3}, \qquad \sqrt{5} \mapsto \pm\sqrt{5},$$

   and all 8 choices are distinct automorphisms which send α to distinct elements.

5. **Dummit and Foote #13.4.3:** *Let F be a field contained in the ring $Mat_n(\mathbb{Q})$ of $n \times n$ matrices over $\mathbb{Q}$. Here, $\mathbb{Q} \subseteq Mat_n(\mathbb{Q})$ is identified with the scalar diagonal matrices by the inclusion*

   $$q \mapsto qI = \begin{bmatrix} q & & & \\ & q & & \\ & & \dots & \\ & & & q \end{bmatrix}.$$

   Prove that $[F : \mathbb{Q}] \leq n$. (I do have a hint for this one, if you ask)

   Solution. Since char $F = 0$, the primitive element theorem tells us that $F = \mathbb{Q}(\alpha)$ for some element $\alpha \in F$. Let $f(x)$ be the characteristic polynomial for the matrix α. Then $\deg f = n$, and $f(\alpha) = 0$ by the Cayley-Hamilton theorem. Therefore, $[F : \mathbb{Q}] = \deg \alpha \leq \deg f = n$.