Math 562/662 **Spring 2019**
Homework 5 **Drew Armstrong**

---

1. Two Small Issues. Let $\mathbb{E} \supseteq \mathbb{F}$ be any field extension.

(a) If $f(x) \in \mathbb{F}[x]$ splits in $\mathbb{E}[x]$ and $g(x)|f(x)$ in $\mathbb{F}[x]$, prove that $g(x)$ also splits in $\mathbb{E}[x]$.

(b) Let $p(x), q(x) \in \mathbb{F}[x]$ be irreducible polynomials that are not associate. Prove that $p(x)$ and $q(x)$ have no common root in $\mathbb{E}$. [Hint: Since $p(x), q(x)$ are coprime in $\mathbb{F}[x]$ we have $p(x)f(x) + q(x)g(x) = 1$ for some $f(x), g(x) \in \mathbb{F}[x]$.]

2. The Galois Group of a Finite Field. Let $\mathbb{E}$ be a field of size p^k and recall that the *Frobenius endomorphism* $\varphi : \mathbb{E} \to \mathbb{E}$ is defined by $\varphi(\alpha) = \alpha^p$.

(a) Use the fact that $\mathbb{E}$ is finite to prove that $\varphi \in \text{Gal}(\mathbb{E}/\mathbb{F}_p)$.

(b) Prove that φ has order k as an element of $\text{Gal}(\mathbb{E}/\mathbb{F}_p)$.

(c) Conclude that $\text{Gal}(\mathbb{E}/\mathbb{F}_p) = \langle \varphi \rangle$ is cyclic of size k.

3. Repeated Roots, Part II We say that a polynomial $f(x) \in \mathbb{F}[x]$ is *inseparable* if it has a repeated root in some field extension. Otherwise we say that $f(x)$ is *separable*. Prove that

$$f(x) \text{ is separable} \quad \Longleftrightarrow \quad \gcd(f, Df) = 1.$$

4. Finite Fields are Separable. Let $\mathbb{E}$ be finite field of characteristic p. For all polynomials $f(x) \in \mathbb{E}[x]$ we will show that

$$f(x) \text{ is irreducible} \quad \Longrightarrow \quad f(x) \text{ is separable}.$$

(a) Let $f(x) \in \mathbb{F}_p[x]$ be irreducible and assume for contradiction that $f(x)$ is inseparable. Prove that the derivative $Df(x) \in \mathbb{F}_p[x]$ is the zero polynomial.

(b) Use part (a) to show that $f(x) = g(x^p)$ for some polynomial $g(x) \in \mathbb{F}_p[x]$.

(c) Finally, show that $g(x^p) = h(x)^p$ for some polynomial $h(x) \in \mathbb{F}_p[x]$. Contradiction. [Hint: You showed in a previous problem that the Frobenius map $\alpha \mapsto \alpha^p$ is surjective.]

5. Cyclotomic Extensions are Abelian. Let $\omega = e^{2\pi i/n} \in \mathbb{C}$.

(a) For all $\sigma \in \text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ prove that $\sigma(\omega) = \omega^{k_\sigma}$ for some $\gcd(k_\sigma, n) = 1$.

(b) Prove that the map $\sigma \mapsto k_\sigma$ defines an injective group homomorphism

$$\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times,$$

hence $\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ is abelian.

(c) Let $\Phi_n(x) \in \mathbb{Q}[x]$ be the cyclotomic polynomial. Prove that

$$\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times \quad \Longleftrightarrow \quad \Phi_n(x) \text{ is irreducible}.$$

6. Radical Implies Solvable. Consider field extensions $\mathbb{E} \supseteq \mathbb{F}(\alpha) \supseteq \mathbb{F}$ where $\alpha^n \in \mathbb{F}$ for some $n \geq 2$ and suppose that $\mathbb{F}$ contains a primitive n-th root of unity.

(a) For any $\sigma \in \text{Gal}(\mathbb{E}/\mathbb{F})$ and $\beta \in \mathbb{F}(\alpha)$ prove that $\sigma(\beta) \in \mathbb{F}(\alpha)$.

(b) Prove that $\text{Gal}(\mathbb{E}/\mathbb{F}(\alpha)) \subseteq \text{Gal}(\mathbb{E}/\mathbb{F})$ is a normal subgroup. [Hint: Use part (a) to define a group homomorphism $\text{Gal}(\mathbb{E}/\mathbb{F}) \to \text{Gal}(\mathbb{F}(\alpha)/\mathbb{F})$ with kernel $\text{Gal}(\mathbb{E}/\mathbb{F}(\alpha))$.]

(c) Prove that the quotient group is abelian.