Week 6: More Field theory (13.4, 13.5, 13.6)

Practice Problems

1. Determine the splitting fields over $\mathbb{Q}$ of the polynomials $x^4 - 1$ and $x^4 + 1$.
2. Find all irreducible polynomials of degrees 1, 2, and 4 over $\mathbb{F}_2$ and prove that their product is $x^{16} - x$.
3. Directly compute the product $\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x)$.

Presentation Problems

1. Let p be an odd prime. Show that $x^{p-1} - 1 = \prod_{\alpha \in \mathbb{F}_p^\times}(x - \alpha)$. Deduce that $(p-1)! \equiv -1 \pmod{p}$.
2. Let p be a prime. Show that $(1+x)^{pn} = (1+x^p)^n$ as polynomials over $\mathbb{F}_p$. By comparing coefficients, deduce that $\binom{pn}{pk} \equiv \binom{n}{k} \pmod{p}$ for all $0 \leq k \leq n$.

   Here are some (tricky) generalizations that are interesting but not directly relevant to this course:

   Bonus I: Show that $\binom{pn}{pk} \equiv \binom{n}{k} \pmod{p^2}$ for all $0 \leq k \leq n$.

   Bonus II: Show that if $p \geq 5$ then $\binom{pn}{pk} \equiv \binom{n}{k} \pmod{p^3}$ for all $0 \leq k \leq n$.
3. Let p be a prime and let $a \in \mathbb{F}_p^\times$. Show that $x^p - x + a$ is irreducible and separable.
4. Let $a \geq 2$ be an integer. For all positive integers n and d, show that d divides n if and only if $a^d - 1$ divides $a^n - 1$. Deduce that $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ if and only if d divides n.

Group Theory Problem

Before we get to the group theory problem, we will need a preliminary module-theoretic result.

0. Let R be a ring and let P be an R-module. Do not assume that R is commutative.
   (a) Show that the following are equivalent:
   - P is projective, meaning that $\mathrm{Hom}_R(P, -)$ takes exact sequences to exact sequences.
   - For every R-module homomorphism $g\colon P \to M$ and every surjective R-module homomorphism $f\colon N \to M$, there exists an R-module homomorphism $h\colon P \to N$ such that $g = f \circ h$.
   - P is a direct summand of a free R-module.

   (b) Show that free modules are projective.
   (c) Show that every R-module has a projective resolution.

1. Let G be a finite group and let H be a subgroup of G of index m.
   (a) Show that every G-module is also an H-module.
   (b) Show that every projective G-module is also a projective H-module.

   Now let A be a G-module.

   (c) Let $\cdots \to P_1 \to P_0 \to \mathbb{Z} \to 0$ be a projective resolution of $\mathbb{Z}$ where each P_n is a projective G-module. Show that we have a homomorphism of cochain complexes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(P_0, A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(P_1, A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(P_2, A) & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}H}(P_0, A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}H}(P_1, A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}H}(P_2, A) & \longrightarrow & \cdots \end{array}$$

(d) Let $\{g_1, \ldots, g_m\}$ be left coset representatives for H in G. Let $\mathrm{Hom}_{\mathbb{Z}H}(P_n, A) \to \mathrm{Hom}_{\mathbb{Z}G}(P_n, A)$ be given by $f \mapsto \sum_{i=1}^{m} g_i f(g_i^{-1} p)$. Show that we have a homomorphism of cochain complexes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}H}(P_0, A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}H}(P_1, A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}H}(P_2, A) & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(P_0, A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(P_1, A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(P_2, A) & \longrightarrow & \cdots \end{array}$$

independent of the choice of left coset representatives.

(e) Construct homomorphisms $\mathrm{res}\colon H^n(G, A) \to H^n(H, A)$ and $\mathrm{cor}\colon H^n(H, A) \to H^n(G, A)$.

(f) Show that the composition $\mathrm{cor} \circ \mathrm{res}$ is given by multiplication by m.

(g) Show that $|G| \cdot H^n(G, A) = 0$.

(h) Show that if A is finite with $\gcd(|G|, |A|) = 1$ then $H^n(G, A) = 0$.

Tricky Problems

1. Let R be a finite ring with no zero divisors. Do not assume that R is commutative.

   (a) Show that every nonzero element of R is a unit.

   (b) Show that the center $Z(R)$ is a finite field.

   (c) Let $q = |Z(R)|$. Show that $|R| = q^n$ for some integer $n \geq 1$.

   (d) Let $x \in R \setminus Z(R)$.

   i. Show that $|C_R(x)| = q^d$ for some $d < n$.

   ii. Use Lagrange's theorem to show that $q^d - 1$ divides $q^n - 1$.

   iii. Show that d divides n.

   (e) Use to class equation to obtain an expression of the form

$$q^n - 1 = (q - 1) + \sum_{i=1}^{k} \frac{q^n - 1}{q^{d_i} - 1}$$

   where each d_i is a proper divisor of n.

   (f) Show that $\Phi_n(q)$ divides $(q^n - 1)/(q^d - 1)$ for every proper divisor d of n.

   (g) Show that $|\Phi_n(q)| \leq q - 1$.

   (h) Use the product expansion $\Phi_n(q) = \prod(q - \zeta)$ to show that $n = 1$ and deduce that R is a field.

   This is known as Wedderburn's little theorem.

2. (a) Let $P(x) \in \mathbb{Z}[x]$ be a nonconstant polynomial. Show that there are infinitely many distinct prime divisors of the integers $\{P(n)\colon n \in \mathbb{Z}\}$.

   Now let m be a positive integer and let p be a prime not dividing m.

   (b) Show that $\Phi_m(a) \equiv 0 \pmod{p}$ if and only if $\gcd(a, p) = 1$ and the order of a in $(\mathbb{Z}/p\mathbb{Z})^\times$ is precisely m. *Hint*: Use the product expansion $x^n - 1 = \prod_{d|n} \Phi_d(x)$ and the fact that $x^m - 1$ is separable over $\mathbb{F}_p$.

   (c) Show that p divides $\Phi_m(a)$ for some $a \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod{m}$.

   (d) Deduce that there are infinitely many primes congruent to 1 modulo m.

   This is a special case of Dirichlet's theorem on primes in arithmetic progressions.