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 check 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 a prime. Show that $x^{p-1} - 1 = \prod_{\alpha \in \mathbb{F}_p^\times}(x - \alpha)$. Deduce that $(p-1)! \equiv -1 \pmod{p}$.

   This last result is known as Wilson's theorem (4/4).

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 $0 \le k \le n$.

   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 $0 \le k \le n$.

   Bonus II: Show that if $p \ge 5$ then $\binom{pn}{pk} \equiv \binom{n}{k} \pmod{p^3}$ for all $0 \le k \le n$.

3. Let p be a prime and let $a \in \mathbb{F}_p^\times$. Show that $x^p - x + a$ is irreducible and separable over $\mathbb{F}_p$.

4. Let $a \ge 2$ 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.

Module Theory Problem

1. Let $\mathbb{S}^2 = \{(x,y,z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\}$ be the unit sphere. A vector field on $\mathbb{S}^2$ is a continuous function (in the ε-δ sense) $X \colon \mathbb{S}^2 \to \mathbb{R}^3$ such that $X(p)$ is tangent to $\mathbb{S}^2$ at p for each $p \in \mathbb{S}^2$, meaning that $X(p) \cdot p = 0$ at each $p \in \mathbb{S}^2$. The set of all such vector fields is denoted $\mathfrak{X}(\mathbb{S}^2)$.

   (a) Let $C(\mathbb{S}^2)$ denote the set of continuous functions $\mathbb{S}^2 \to \mathbb{R}$. Define a commutative ring structure on $C(\mathbb{S}^2)$ and a $C(\mathbb{S}^2)$-module structure on $\mathfrak{X}(\mathbb{S}^2)$.

   (b) Let M denote the set of all continuous functions $\mathbb{S}^2 \to \mathbb{R}^3$. Define a $C(\mathbb{S}^2)$-modules structure on M such that M is free of rank 3 and contains $\mathfrak{X}(\mathbb{S}^2)$ as a submodule.

   (c) Show that $\mathfrak{X}(\mathbb{S}^2)$ is a direct summand of M, and in fact that $M \cong \mathfrak{X}(\mathbb{S}^2) \oplus C(\mathbb{S}^2)$.
   This isomorphism $M \xrightarrow{\sim} \mathfrak{X}(\mathbb{S}^2) \oplus C(\mathbb{S}^2)$ should make the diagrams

$$\begin{tikzcd} M \arrow[r, "\sim"] & \mathfrak{X}(\mathbb{S}^2) \oplus C(\mathbb{S}^2) \\ \mathfrak{X}(\mathbb{S}^2) \arrow[u, hook] \arrow[ur, hook] & \end{tikzcd} \qquad \begin{tikzcd} M \arrow[r, "\sim"] & \mathfrak{X}(\mathbb{S}^2) \oplus C(\mathbb{S}^2) \arrow[dl, two heads] \\ \mathfrak{X}(\mathbb{S}^2) \arrow[u, hook] & \end{tikzcd}$$

   commute.

   (d) The Hairy Ball Theorem from Topology says that there is no nonvanishing vector field on $\mathbb{S}^2$. In other words, for any $X \in \mathfrak{X}(\mathbb{S}^2)$ there is a point $p \in \mathbb{S}^2$ for which $X(p) = 0$. Assuming the Hairy Ball Theorem, prove that $\mathfrak{X}(\mathbb{S}^2)$ is not free.
   Bonus: If you know what $\pi_1(\mathbb{S}^1) \cong \mathbb{Z}$ means, try to prove the Hairy Ball Theorem.

Because $\mathfrak{X}(\mathbb{S}^2)$ is a direct summand of a free module, it gives an example of a "projective module". In fact, by the Serre-Swan theorem, every (finitely generated) projective module over $C(\mathbb{S}^2)$ is of the same general form. Projective modules are abundant in geometry, and are crucial to some very important construction of homological algebra. Before we define projective modules, we need a lemma. Fix a commutative ring R.

2. For any R-module P, the functor $\mathrm{Hom}_R(P, -)$ is left-exact: for any short exact sequence of R-modules

$$0 \longrightarrow X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z \longrightarrow 0,$$

the sequence

$$0 \longrightarrow \mathrm{Hom}_R(P, X) \xrightarrow{\alpha_*} \mathrm{Hom}_R(P, Y) \xrightarrow{\beta_*} \mathrm{Hom}_R(P, Z)$$

is also exact.

In general, β_* is not necessarily surjective. Another way to say this is that $\mathrm{Hom}_R(P, -)$ is not necessarily exact (meaning that applying it to a short exact sequence does not necessarily give a short exact sequence). For example, applying $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, -)$ to $0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ does not give a short exact sequence (try it!). Like being a direct summand of a free module, $\mathrm{Hom}_R(P, -)$ being exact characterizes projective modules.

3. Prove that for an R-module P, the following are equivalent:

   (a) The functor $\mathrm{Hom}_R(P, -)$ is exact.

   (b) For any surjective R-module homomorphism $\pi\colon M \to N$ and any R-module homomorphism $f\colon P \to N$, there is an R-module homomorphism $\tilde{f}\colon P \to M$ making the diagram

$$\begin{tikzcd} & M \arrow[d, two heads, "\pi"] \\ P \arrow[ur, dashed, "\tilde{f}"] \arrow[r, "f"] & N \end{tikzcd}$$

   commute (i.e., such that $f = \pi \circ \tilde{f}$). Note that we do not require $\tilde{f}$ to be unique.

   (c) Any surjective R-module homomorphism $\pi\colon M \to P$ has a section (an R-module homomorphism $\sigma\colon P \to M$ such that $\pi \circ \sigma = \mathrm{id}_P$).

   (d) Any short exact sequence of R-modules $0 \to M \to N \to P \to 0$ splits.

   (e) There is an R-module Q such that $P \oplus Q$ is a free R-module.

   If the above hold, we say that P is a projective R-module.

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.