Week 5: Field extensions and geometry (13.1, 13.2, 13.3)

Practice Problems

1. Let $\zeta_n = e^{2\pi i/n}$.

   (a) Show that $\mathbb{Q}(\zeta_1) = \mathbb{Q}(\zeta_2) = \mathbb{Q}$.

   (b) Show that $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$.

   (c) Show that $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{-3})$.

   (d) Show that $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$.

   (e) Show that $\mathbb{Q}(\frac{1+\sqrt{5}}{2}) = \mathbb{Q}(\sqrt{5})$.

2. Compute the minimal polynomials over $\mathbb{Q}$ of ζ_1, ζ_2, ζ_3, ζ_4, ζ_6, ζ_8, and $\frac{1+\sqrt{5}}{2}$.

3. Show directly that $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is a field automorphism of $\mathbb{Q}(\sqrt{2})$.

Presentation Problems

1. Let F be a finite field. Show that the cardinality of F is a power of a prime.

2. Let $\sigma\colon \mathbb{R} \to \mathbb{R}$ be a field automorphism.

   (a) Show that $\sigma(x) = x$ for all $x \in \mathbb{Q}$.

   (b) Show that $\sigma(x) \geq 0$ if and only if $x \geq 0$.

   (c) Show that σ is strictly increasing.

   (d) Show that $\sigma(x) = x$ for all $x \in \mathbb{R}$.

3. Show that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

4. (a) Is the regular 5-gon constructible?

   (b) Is the regular 7-gon constructible?

   (c) Is the regular 9-gon constructible?

Module Theory Problem

Modules are a generalization of vector spaces, but not all of the nice properties carry over. Here we investigate what kind of properties fail, and what still holds. Let A be a commutative ring, let S be a set, and define $F^A(S)$ to be the set of all finite formal sums $a_1 s_1 + \cdots + a_n s_n$ of elements $s_i \in S$ with coefficients $a_i \in A$. There is an inclusion map $i\colon S \hookrightarrow F^A(S)$ given by $i(s) = 1s$.

1. Define an A-module structure on $F^A(S)$ that satisfies the following universal property:

   For any A-module M and any function $f\colon S \to M$, there exists a unique A-module homomorphism $\varphi\colon F^A(S) \to M$ such that $\varphi \circ i = f$.

$$\begin{tikzcd}
F^A(S) \arrow[r, dashed, "\varphi"] & M \\
S \arrow[u, hook, "i"] \arrow[ur, "f"'] &
\end{tikzcd}$$

   Because of the above, we say that F is the free module on the set S (like how free groups work).

2. Let M be an A-module and let S be a subset of M. By the previous part, the inclusion function $S \hookrightarrow M$ induces a map $\varepsilon\colon F^A(S) \to M$.

- We say that S is linearly independent if ε is injective.
- We say that S is a spanning set if ε is surjective.
- We say that S is a basis if ε is bijective (which gives an A-module isomorphism $F^A(S) \cong M$).

Write down a more concrete definition of these terms (just in terms of S and M, without referencing $F^A(S)$), and show that they coincide with the concepts from linear algebra when A is a field.

3. If M admits a basis then M is called a free module. Find an example of a non-free module (i.e., a module which does not admit a basis).

   Hint: Try looking at $\mathbb{Z}$-modules (abelian groups).

4. Given a vector space V over a field k, we know that V has a basis and that the cardinality of any two bases of V are equal. The dimension of V is defined as this cardinality. By the previous part, we should not expect to be able to define the dimension of an arbitrary module. Can we define an analogous concept for free modules? Show that for any two sets S, T, if $F^A(S) \cong F^A(T)$, then $|S| = |T|$.

   Hint: Take a maximal ideal of A and reduce to the case where A is a field.

   Conclude that for a free module M, every basis of M has the same cardinality, and so it is meaningful to define the rank of M to be the cardinality of any basis for it.

5. Let $M = \mathbb{Z}[x]$ be the free $\mathbb{Z}[x]$-module of rank 1. Find a non-free $\mathbb{Z}[x]$-submodule of M. In particular, observe that this submodule is not spanned by a single element.

6. Suppose that F and F' are free of finite rank n, m and that $F \cong F' \oplus P$ for some module P. Show that if P is free, then P must have rank $n - m$. Do you think that P is necessarily free? We will answer this next week.

Tricky Problems

1. Show that $x^4 + 1$ is reducible in $(\mathbb{Z}/p\mathbb{Z})[x]$ for every prime p.

2. The Fibonacci sequence is defined by $F_0 = 0$, $F_1 = 1$, and $F_{n+1} = F_n + F_{n-1}$ for all $n \geq 1$.

   Let K be a field. Define the Fibonacci sequence in K by $F_0^K = 0$, $F_1^K = 1$, and $F_{n+1}^K = F_n^K + F_{n-1}^K$ for all $n \geq 1$. Consider the polynomial $p(x) = x^2 - x - 1$ in $K[x]$.

   (a) Show that if φ and ψ are distinct roots of $p(x)$ in K then $F_n^K = (\varphi^n - \psi^n)/(\varphi - \psi)$ for all $n \geq 0$.

   Let $p \neq 2, 5$ be a prime.

   First suppose that $\mathbb{Z}/p\mathbb{Z}$ has a square root of 5. Let $K = \mathbb{Z}/p\mathbb{Z}$.

   (b) Show that $p(x)$ has two distinct roots φ and ψ in K.

   (c) Show that $\varphi^{p-1} = \psi^{p-1}$ and deduce that F_{p-1} is divisible by p.

   Now suppose that $\mathbb{Z}/p\mathbb{Z}$ does not have a square root of 5. Let $K = (\mathbb{Z}/p\mathbb{Z})(\sqrt{5})$.

   (d) We define conjugation on K by $\overline{a + b\sqrt{5}} = a - b\sqrt{5}$. Show that the conjugation map $x \mapsto \overline{x}$ is a field automorphism of K.

   (e) Show that the Frobenius map $x \mapsto x^p$ is a field automorphism of K.

   (f) Show that $5^{(p-1)/2} \equiv -1 \pmod{p}$ and deduce that these two automorphisms of K are the same (i.e., that $x^p = \overline{x}$).

   (g) Show that $p(x)$ has two distinct roots φ and ψ in K.

   (h) Show that $\overline{\varphi} = \psi$ and $\overline{\psi} = \varphi$.

(i) Show that $\varphi^{p+1} = \psi^{p+1}$ and deduce that F_{p+1} is divisible by p.

One consequence of the law of quadratic reciprocity is that $\mathbb{Z}/p\mathbb{Z}$ has a square root of 5 if and only if $p \equiv 1, 4 \pmod 5$. Then for any prime p,

- If $p \equiv 1, 4 \pmod 5$ then F_{p-1} is divisible by p.
- If $p \equiv 2, 3 \pmod 5$ then F_{p+1} is divisible by p.
- If $p \equiv 0 \pmod 5$ then F_p is divisible by p.