

Math 211 (Modern Algebra II), HW# 3,

Spring 2026; Instructor: Sam Hopkins; Due: Friday, February 27th

Throughout, recall that for a prime power $q = p^n$, \mathbb{F}_q denotes the field with q elements, which we proved in class exists and is unique.

1. In this problem, you will construct \mathbb{F}_4 “from scratch.” Let the elements of \mathbb{F}_4 be $\{0, 1, a, b\}$. Since the characteristic of \mathbb{F}_4 is 2, we know how 0 and 1 must add and multiply. So what we need to figure out is how a and b behave.
 - (a) Write down the addition table of \mathbb{F}_4 . **Hint:** remember that addition is commutative, that the characteristic of \mathbb{F}_4 is 2, and that additive inverses have to exist and be unique.
 - (b) Write down the multiplication table of \mathbb{F}_4 . **Hint:** remember that multiplication is commutative, and that multiplicative inverses have to exist and be unique.
 - (c) Consider the map $\varphi: \mathbb{F}_4 \rightarrow \mathbb{F}_4$ given by $\varphi: x \mapsto x^2$. Explain, using your tables, why this φ is an automorphism. What are the fixed points of φ ?
2. Let p be a prime. Recall that for a finite field K of characteristic p , the *Frobenius automorphism* $\varphi: K \rightarrow K$ is given by $\varphi: x \mapsto x^p$.

Fermat’s Little Theorem says that $a^p \equiv a \pmod{p}$ for all integers $a \in \mathbb{Z}$. On a homework assignment from last semester you proved Fermat’s Little Theorem using some group theory. Give another proof of Fermat’s Little Theorem by using the Frobenius automorphism.

Hint: how must φ behave on \mathbb{F}_p itself?

3. Let p be a prime and let $f(x) \in \mathbb{F}_p[x]$ be irreducible of degree n . Let $g(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. Prove that $f(x)$ divides $g(x)$. **Hint:** recall that \mathbb{F}_{p^n} is the splitting field of $g(x)$.
4. Let $K = \mathbb{F}_2(t)$ be the field of rational functions, in the variable t , with coefficients in \mathbb{F}_2 . (We use t because we also want to consider polynomials, in the usual variable x , over this field.) Consider the polynomial $f(x) = x^2 - t \in K[x]$.
 - (a) Explain why $f(x)$ is irreducible.
 - (b) Explain why $f(x)$ is not separable. **Hint:** recall the relationship we discussed in class between the separability of a polynomial and its formal derivative.

(This is the simplest example of a polynomial which is irreducible but not separable.)