Yale University Department of Mathematics
Math 370 Fields and Galois Theory
Spring 2018

Problem Set # 7 (due in class on Thursday March 29; have a great Spring break!)

Notation: Let F be a field of characteristic $p > 0$. Define the **Frobenius** map $\phi : F \to F$ by $\phi(x) = x^p$. By the "first-year's dream" the Frobenius map is a ring homomorphism. We call F **perfect** if the Frobenius map is surjective (equivalently, is a field automorphism), i.e., if every element of F has a pth root. By definition, we say that any field of characteristic 0 is perfect.

Reading: GT 9, 17.4–17.5.

Problems:

1. Prove that if F is a perfect field, then any irreducible polynomial $f(x) \in F[x]$ is separable. In class, we proved the case when F has characteristic 0, though it was a bit rushed. For completeness, redo this case nicely in your proof.

2. All about finite fields.

(a) Prove that a finite field K has characteristic p for some prime number p, and in this case, is a finite extension of $\mathbb{F}_p$. In particular, $|K| = p^n$ for some $n \geq 1$. **Hint.** Prime field.

(b) Prove that any finite field K is perfect and that $\phi \in \mathrm{Aut}_{\mathbb{F}_p}(K)$.

(c) Prove that if K is a finite field of order $q = p^n$, then K is the splitting field of the polynomial $x^q - x \in \mathbb{F}_p[x]$. **Hint.** Consider the multiplicative group $K^\times$.

(d) Prove that for any $q = p^n$, the polynomial $x^q - x \in \mathbb{F}_p[x]$ is separable and its splitting field K over $\mathbb{F}_p$ is a field with q elements. **Hint.** Show that the set of elements of K fixed by ϕ^n (the Frobenius automorphism composed with itself n times) coincides with the roots of $x^q - x$. Why does this show that the set of roots of $x^q - x$ is itself a subfield of K, and hence actually all of K?

(e) Prove that for any prime power $q = p^n$, there exists a unique isomorphism class of field of order q, i.e, there exists a field of order q and any two such fields are isomorphic. We call such a field $\mathbb{F}_q$.

(f) Prove that for $q = p^n$, the extension $\mathbb{F}_q/\mathbb{F}_p$ is Galois with Galois group cyclic of order n generated by the Frobenius ϕ.

(g) Even though you now know they are isomorphic, find an explicit isomorphism between the fields $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$ and $\mathbb{F}_2[x]/(x^3 + x + 1)$.

3. Let F be a field and $g \in F[x]$. Prove that the map $D_g : F[x] \to F[x]$ defined by $D_g(f) = g\,f'$ is an F-derivation. Prove that every F-derivation of $F[x]$ is of this form.

4. An F-derivation on an F-algebra R is called **trivial** if it takes every element to zero.

(a) Let $f(x) \in \mathbb{Q}[x]$ be a quadratic polynomial. Give necessary and sufficient conditions on $f(x)$ for the quotient ring $\mathbb{Q}[x]/(f(x))$ to admit a non-trivial $\mathbb{Q}$-derivation. **Hint.** In the quotient ring, we have $f(\bar{x}) = 0$; try applying your $\mathbb{Q}$-derivation to both sides, thinking about the cases when f is irreducible, reducible, or has a multiple root.

(b) Let F be a field of characteristic $p > 0$ and $K = F(\alpha)$ a simple extension of F such that the minimal polynomial of α over F is not separable. Prove that K has a nontrivial F-derivation. **Hint.** Try the "derivative with respect to α"; why does it make sense?