Yale University Department of Mathematics
Math 370 Fields and Galois Theory
Spring 2019

Problem Set # 6 (due in class on Thursday March 7)

Notation: The **Galois group** of a polynomial $f(x)$ over a field F is defined to be the F-automorphism group of its splitting field E.

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.

Problems:

1. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Determine the $\mathbb{Q}$-automorphism group of $K/\mathbb{Q}$ by writing down all the elements as automorphisms and also by describing the isomorphism class of the group.

2. Compute the Galois group of the polynomial $f(x) = x^3 - 4x + 2 \in \mathbb{Q}[x]$.

3. Let F be a field of characteristic $\neq 2$. Let $f(x) = x^4 + bx^2 + c \in F[x]$. Assume that $f(x)$ is separable. Prove that the Galois group of $f(x)$ is isomorphic to a subgroup of the dihedral group D_8 of order 8.

4. Prove that if F is a perfect field, then any irreducible polynomial $f(x) \in F[x]$ is separable. (In class, this was stated in the case when F has characteristic 0; this is now one of the cases you'll need to prove, the other case being perfect fields of characteristic $p > 0$.)

5. 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 automorphism group $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q)$ is 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 $\mathbb{F}_2[x]/(x^3 + x + 1)$.