Math 4055/5055: Advanced Algebra II

Assignment 4

due 18 March 2025, end of day

Fix a positive prime p, and assume throughout that all fields under consideration have characteristic p.

1. Show that if $F \subset E$ is a finite-degree field extension such that $[E : F]$ is not divisible by p, then $F \subset E$ is separable.

2. The converse does not hold: There exists a field $\mathbb{F}_{p^p}$ of order p^p; the extension $\mathbb{F}_p \subset \mathbb{F}_{p^p}$ is separable (indeed, Galois) and of degree p.

   (a) Suppose that F is a field of characteristic p, for example $F = \mathbb{F}_p$. An *Artin–Schreier polynomial* is a polynomial of the form $x^p - x - a$ for some $a \in F$. Fix a and suppose that $x^p - x - a$ has no roots in F. Consider the field $K = F[\alpha]$ where α is some root of (some irreducible factor of) $x^p - x - a$. Show that $\alpha + 1$ is another root.

   (b) Conclude that $\alpha \mapsto \alpha + 1$ extends to an automorphism of K, called the *Artin–Schreier automorphism* of K. Conclude that the Galois group of K has order at least p. Conclude that $[K : F] = p$ and that $x^p - x - a$ is irreducible over K. Extensions of this form are called *Artin–Schreier extensions*.

   (c) Show that when $K = \mathbb{F}_p$, then the Artin–Schreier polynomial has no roots as soon as $a \neq 0$. Conclude that $\mathbb{F}_p \subset \mathbb{F}_{p^p}$ is Artin–Schreier.

   (d) We therefore have two different descriptions of $\mathrm{Gal}(\mathbb{F}_{p^p}/\mathbb{F}_p)$: it is the cyclic group of order p generated by the Frobenius automorphism and it is the cyclic group of order p generated by the Artin–Schreier automorphism. Find a formula relating these two automorphisms.

   (e) Each nonzero $a \in \mathbb{F}_p$ gives a description of $\mathbb{F}_p \subset \mathbb{F}_{p^p}$ as an Artin–Schreier extension. As a varies, how do these descriptions vary? In particular, how many elements of $\mathbb{F}_{p^p}$ are Artin–Schreier?

3. (a) Let ℓ be a prime, possibly but not necessarily equal to p. How many irreducible monic polynomials of degree ℓ are there over $\mathbb{F}_p$? Hint: How many orbits does the Frobenius have when acting on $\mathbb{F}_{p^\ell}$? Alternate hint: Show that the irreducible factors of $x^{p^\ell} - x$ are all either linear or degree-ℓ.

   (b) Why are the two hints in the previous question actually the same hint?

   (c) List all the irreducible cubics over $\mathbb{F}_3$.

4. Let $F \subset E$ be an algebraic extension. Suppose that $\alpha \neq 0 \in E$ is separable over F and $\beta \neq 0 \in E$ is purely inseparable over F. Prove that $F[\alpha, \beta] = F[\alpha + \beta] = F[\alpha\beta]$.

5. The *separable degree* $[E:F]_s$ of a field extension is the degree $[E_s:F]$ where $E_s \subset E$ is the subfield of separable (over F) elements. The *inseparable degree* $[E:F]_i$ of E/F is $[E:E_s]$. Suppose that $E = F[\alpha]$ is a simple algebraic extension. What are $[E:F]_i$ and $[E:F]_s$ in terms of (the minimal polynomial of) α?

6. Suppose that $F \subset K \subset E$ is a subextension, and let $K_s \subset K$ and $E_s \subset E$ denote the subfields of elements which are separable over F. Show that $K_s \subset E_s$ is separable.

   Conclude that $[:]_s$, and hence also $[:]_i$, is multiplicative.

7. Fix a finite-degree extension $F \subset E$. Let $\bar{F} = \bar{E}$ denote the algebraic closure of F (why is $\bar{F} = \bar{E}$?), and let $F^s = \bar{F}_s \subset \bar{F}$ denote the separable closure. Show that the sets $\hom_F(E, \bar{F})$ and $\hom_F(E_s, F^s)$ are canonically isomorphic (where the hom is in the category of fields over F). Conclude that $\hom(E, \bar{F})$ is of cardinality equal to $[E:F]_s$.