

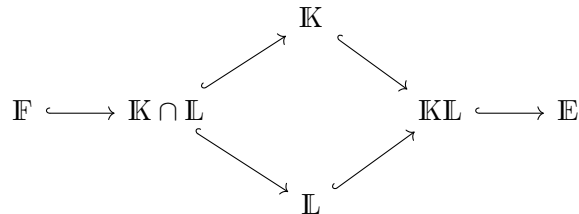
# Math 5055: Advanced Algebra II

## Assignment 2

due February 1, 2022

Homework should be submitted either as a single PDF attachment to `theo.jf@dal.ca` (please include your name in the file name!) or as a single stapled(!) collection to my mailbox in the Chase building.

- Let  $\mathbb{E}$  be the splitting field over  $\mathbb{Q}$  of  $(x^3 - 2)(x^2 - 3)$ . Compute  $\text{Gal}(\mathbb{E}/\mathbb{Q})$ , and write down the complete Galois correspondence: list all the subfields of  $\mathbb{E}$  and all the subgroups of  $\text{Gal}(\mathbb{E}/\mathbb{Q})$  and how they match.
- (a) Let  $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$  be field extensions such that  $\mathbb{E}$  is the splitting field over  $\mathbb{F}$  of some set  $S$  of polynomials. Show that then  $\mathbb{E}$  is the splitting field of some set of polynomials over  $\mathbb{K}$ .  
(b) Show that the converse does not hold. Specifically, find an example where  $\mathbb{F} \subset \mathbb{K}$  is the splitting field of some set of polynomials, and  $\mathbb{K} \subset \mathbb{E}$  is the splitting field of some set of polynomials, but  $\mathbb{F} \subset \mathbb{E}$  is not a splitting field of some set of polynomials.
- (*Lagrange's Theorem of Natural Irrationalities*)  
Suppose given a diagram of field extensions



such that  $\mathbb{F} \subset \mathbb{K}$  is finite and Galois. Prove that  $\mathbb{L} \subset \mathbb{KL}$  is finite and Galois, and that  $\text{Gal}(\mathbb{KL}/\mathbb{L}) = \text{Gal}(\mathbb{K}/(\mathbb{K} \cap \mathbb{L}))$ .

**Hints:**  $\mathbb{L} \subset \mathbb{KL}$  is the splitting field of some separable polynomial. (Why? So what?) Any  $\mathbb{F}$ -linear automorphism of  $\mathbb{KL}$  takes  $\mathbb{K}$  to itself. (Why? So what?) Compute kernel and image of  $\text{Gal}(\mathbb{KL}/\mathbb{L}) \rightarrow \text{Gal}(\mathbb{K}/\mathbb{F})$ .

- (a) Suppose that  $f(x) \in \mathbb{F}_3[x]$  is a monic irreducible cubic. Show that  $f$  must divide  $x^{27} - x$ . Conversely, show that if  $f$  is irreducible and divides  $x^{27} - x$  then  $f$  is either linear or cubic.  
(b) Use part (a) to (quickly!) count the number of monic irreducible cubics over  $\mathbb{F}_3$ .  
(c) List all the irreducible monic cubics over  $\mathbb{F}_3$ . **Hints:**
  - Observe that, as functions  $\mathbb{F}_3 \rightarrow \mathbb{F}_3$ , the polynomial  $x^3 - x$  always vanishes, whereas the polynomials  $1$  and  $x^2 + 1$  never vanish. Use this to list at least four irreducible cubics over  $\mathbb{F}_3$ .

- ii. Observe that, as functions  $\mathbb{F}_3 \rightarrow \mathbb{F}_3$ ,  $x^2 - 1$  vanishes whenever  $x \neq 0$ , whereas  $x^3$  and  $x^3 + x$  vanish only when  $x = 0$ . Use this to list at least four irreducible cubics over  $\mathbb{F}_3$ .
5. (*Artin-Schreier extensions*) Let  $p$  be a positive prime and  $a \neq 0 \in \mathbb{F}_p$ . Let  $\mathbb{E} = \mathbb{F}_p[\alpha]$  where  $\alpha$  is a root of  $x^p - x - a$  over  $\mathbb{F}_p$ . Show that  $\alpha \mapsto \alpha + 1$  extends to an automorphism of  $\mathbb{E}$ . Conclude that  $x^p - x - a$  is irreducible and that  $\mathbb{E}$  is its splitting field. How does  $\alpha \mapsto \alpha + 1$  relate to the Frobenius endomorphism of  $\mathbb{E}$ ?
6. Show that  $-1$  has a square root in the ring  $\mathbb{Z}_5 = \varprojlim \mathbb{Z}/(5^n)$  of 5-adic integers.