Assignment 1 – All 2 parts – Math 612

Due in class: Thursday, Jan. 21, 2016

(1) Finite multiplicative subgroups of fields are cyclic. This exercise will walk you through a proof that any finite subgroup of the multiplicative group of a field is cyclic. In particular, $\mathbf{F}_q^\times$ is cyclic of order $q-1$. There are several proofs, here is one. It basically requires a few facts about cyclic groups. Let n be a positive integer and recall the definition of the Euler totient function

$$\varphi(n) := \#(\mathbf{Z}/n\mathbf{Z})^\times. \tag{1}$$

The first thing to prove is a result from elementary number theory:

$$\sum_{d|n} \varphi(d) = n,$$

where the sum is over positive integers d dividing n.

(a) For $d \mid n$, show that there is a unique cyclic subgroup of $\mathbf{Z}/n\mathbf{Z}$ of order d.

(b) Show that the number of generators of a cyclic group of order d is $\varphi(d)$.

(c) Let Γ_d be the set of generators of the unique cyclic subgroup of $\mathbf{Z}/n\mathbf{Z}$ of order d and show that

$$\mathbf{Z}/n\mathbf{Z} = \bigsqcup_{d|n} \Gamma_d.$$

Conclude that

$$\sum_{d|n} \varphi(d) = n.$$

(d) Now, a criterion for finite cyclic groups: suppose G is a finite group of order n such that for every $d \mid n$, the set $\{g \in G : g^d = 1\}$ has cardinality at most d. Show that G is cyclic. (Hint: show that the number of elements of order d must be either $\varphi(d)$ or 0, then show that if it is 0 for some $d \mid n$, then the equation (1) implies $\#G < n$.)

(e) Finally, suppose F is a field and $G \leq F^\times$. Show that G is cyclic. (Hint: how many roots of $x^d - 1$ can there be in F?)

(2) The Frobenius automorphism. Let $q = p^n$ with p prime and n a positive integer. Recall that the map $\varphi : \mathbf{F}_q \to \mathbf{F}_q$ given by $\varphi(a) = a^p$ is a ring homomorphism. Recall

that $\text{Aut}(\mathbf{F}_q/\mathbf{F}_p)$ denotes the group of $\mathbf{F}_p$-automorphisms of $\mathbf{F}_q$. This exercise will show that $\text{Aut}(\mathbf{F}_q/\mathbf{F}_p) = \langle\varphi\rangle$.

(a) Show that $\varphi : \mathbf{F}_q \to \mathbf{F}_q$ is an $\mathbf{F}_p$-automorphism.

(b) Show that $\varphi^n = \text{id}$, but that $\varphi^d \neq \text{id}$ for all $1 \leq d < n$.

(c) Show that $\text{Aut}(\mathbf{F}_q/\mathbf{F}_p) = \langle\varphi\rangle$. (Hint: the powers of φ give n automorphisms and we have an upper bound on the number of automorphisms of a simple extension; also, by construction extensions of finite fields are normal).

(d) In fact, show that $\text{Aut}(\mathbf{F}_{q^m}/\mathbf{F}_q) = \langle\varphi^n\rangle$ and hence has order $m = [\mathbf{F}_{q^m} : \mathbf{F}_q]$ (here, $\varphi : \mathbf{F}_{q^m} \to \mathbf{F}_{q^m}$ is still given by $\varphi(a) = a^p$).

(e) Note that the map $\varphi : \overline{\mathbf{F}}_p \to \overline{\mathbf{F}}_p$ sending a to a^p is an $\mathbf{F}_p$-automorphism of $\overline{\mathbf{F}}_p$. Show that for all non-zero integers n, $\varphi^n \neq \text{id}$ and hence that $\text{Aut}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ contains a copy of $\mathbf{Z}$.

(f) For a positive integer n, let $s_n := \sum_{k=0}^{n-1} k!$. Define $\widehat{\varphi} : \overline{\mathbf{F}}_p \to \overline{\mathbf{F}}_p$ as follows: if $a \in \mathbf{F}_{p^{n!}}$ (note the factorial!), then

$$\widehat{\varphi}(a) := a^{p^{s_n}}.$$

Show that $\widehat{\varphi}$ is a (well-defined) $\mathbf{F}_p$-automorphism of $\overline{\mathbf{F}}_p$ that is not a power of φ, and hence that $\text{Aut}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ is bigger than just $\mathbf{Z}$.

(3) Extensions of finite fields are separable. Show that any algebraic extension of a finite field is separable.

(4) Let ω be a primitive third root of unity and let $\sqrt[3]{2}$ be the real cube root of 2. Show that $\mathbf{Q}(\omega, \sqrt[3]{2}) = \mathbf{Q}(\omega + \sqrt[3]{2})$ and find the minimal polynomial of $\omega + \sqrt[3]{2}$.

(5) Galois closure. Last semester we discussed the normal closure of an algebraic extension K/F. Show that if K/F is a separable algebraic extension (that is not necessarily normal) then the normal closure of K/F is separable. In this case, the normal closure is Galois and so it is called the *Galois closure* of K/F. (Hint: the normal closure is the compositum of the conjugates of K and separable extensions form a distinguished class.)