Mathematics GU4042
Introduction to Modern Algebra II

Assignment #10
Due April 21, 2017

1. (a) If $\mathbf{F}_q/\mathbf{F}_p$ are finite fields, prove that $\mathbf{F}_q/\mathbf{F}_p$ is a Galois extension (cf. the midterm).

(b) If $q = p^n$, prove that the Frobenius homomorphism $\phi : \mathbf{F}_q \to \mathbf{F}_q$ given by $\phi(x) = x^p$ (cf. Assignment 7, problem **8**) has order n and generates Gal $\mathbf{F}_q/\mathbf{F}_p$.

(c) Use this to give an alternative proof of the following (cf. Assignment 7, problem **6**): A field with p^n elements contains a field with p^m elements if and only if $m \mid n$, and in this case, there is exactly one such subfield.

2. Let $z = \sqrt{5} + i$.

(a) What is its minimal polynomial over $\mathbf{Q}$? Does it satisfy Eisenstein's criterion?

(b) What are its *conjugates* over $\mathbf{Q}$, i.e. the other roots of its minimal polynomial over $\mathbf{Q}$?

(c) What is the Galois group G of its splitting field over $\mathbf{Q}$?

(d) Explicitly name the proper subgroups of G, the corresponding invariant subfields, and the minimal polynomial of z over each one.

3. Let $E/F/K$ be field extensions.

(a) Proof or counterexample: E/K is Galois implies E/F is Galois.

(b) Proof or counterexample: E/K is Galois implies F/K is Galois.

4. (a) If F/K is Galois and E/F is the splitting field over F of a separable $f(x) \in K[x]$, prove that E/K is Galois.

Use the Extension Theorem proved in class: If $\phi : F \to \tilde{F}$ is a field homomorphism, $\tilde{f} = \phi(f)$ for $f \in F[x]$, and $E, \tilde{E}$ are splitting fields over $F, \tilde{F}$ of $f, \tilde{f}$ respectively, then the number of homomorphisms $\Phi : E \to \tilde{E}$ with $\Phi|_F = \phi$ is > 0 and $\leq [E : F]$, with equality if f is separable.

(b) Give a counterexample if we only assume $f(x) \in F[x]$ rather than $f(x) \in K[x]$. (Ask yourself where the proof you gave in (a) fails.)

5. (a) For any $n > 0$, prove that there exists a Galois extension E/F having the symmetric group Σ_n as its Galois group. Hint: take $E = \mathbf{Q}(x_1, \ldots, x_n)$.

(b) For any finite group G, prove that there exists a Galois extension E/F having G as its Galois group.

6. If E/F is a Galois extension with Galois group Σ_3, prove that E must be the splitting field of an irreducible cubic in $F[x]$. Hint: Σ_3 has non-normal subgroups; what irreducible polynomials in $F[x]$ have roots in the corresponding subfields?