# Mathematics GU4042
# Introduction to Modern Algebra II

**Assignment #7**

Due March 24, 2017

Throughout, let $F$ be a field.

**1.** Let $f, g \in F[x]$, let $E$ be a splitting field for $f$ over $F$, and let $D$ be a splitting field for $g$ over $E$. Show that $D$ is a splitting field for $fg$ over $F$.

**2.** (a) Show that the splitting field $E$ of $f \in F[x]$ is a finite extension of $F$; indeed, if $n = \deg f$, show that $[E : F] \leq n!$. Hint: reduce to the irreducible case and consider $F[x]/(f)$.

(b) Show that equality holds in (a) for $F = \mathbf{Q}$ and $f(x) = x^3 - 2$. (You may use the intermediate value theorem from calculus.)

**3.** Show that any irreducible $f \in \mathbf{F}_p[x]$ of degree $n$ divides $x^q - x$, where $q = p^n$. Hint: consider $\mathbf{F}_p[x]/(f)$ and use the fact that $\mathbf{F}_p$ is perfect.

**4.** Let $F$ be a finite field with $p^n$ elements for $p$ prime. If $a$ generates the cyclic group $F^\times$, show that the minimal polynomial of $a$ over $\mathbf{F}_p$ has degree $n$.

**5.** Is the finite field $\mathbf{F}_4$ isomorphic as a ring to $\mathbf{Z}_4$? What about to $\mathbf{Z}_2 \times \mathbf{Z}_2$? Why or why not?

**6.** We proved in class that a field $F$ with $p^n$ elements contains a field with $p^m$ elements if and only if $m \mid n$. Prove that, in this case, there is only one such subfield.

**7.** For any prime number $p$ and any nonzero $a \in \mathbf{F}_p$, prove that $x^p - x + a$ is irreducible in $\mathbf{F}_p[x]$. Hint: show first that in any field extension, if $r$ is a root, then so is $r + 1$.

**8.** (a) Prove that for a finite field $F$ of characteristic $p$, the *Frobenius map* $\phi : F \to F$ given by $\phi(a) = a^p$ is a homomorphism such that $\phi|_{\mathbf{F}_p} = \mathrm{id}$.

(b) For any nonzero $f \in \mathbf{F}_p[x]$, if $a$ is a root in any field extension, prove that $a^p$ is too.

**9.** (a) Prove that over a finite field $F$ with $q$ elements, $x^{q-1} - 1 = \prod_{a \in F^\times}(x - a)$.

(b) Prove that the product of all nonzero elements of a finite field is $-1$.

(c) Prove *Wilson's theorem*: if $p$ is a prime number, then $(p-1)! \equiv -1 \pmod{p}$.