Math 742, Spring 2016
Homework 9
Due: April 11 (Monday)

1. Exercises

(1) Let a, b be positive integers. If p is a prime, then show that at least one of a, b, ab is a square in $\mathbf{F}_p$. In particular, the polynomial

$$(x^2-2)(x^2-3)(x^2-6) \in \mathbf{Z}[x]$$

has a root modulo p for all primes p, but no root in $\mathbf{Q}$.

(2) (a) Let G be a finite group. Let $X, Y \subseteq G$ be subsets such that $|X| + |Y| > |G|$. Show that every element of G can be written as xy where $x \in X$ and $y \in Y$.

(b) Let K be a finite field. Use (a) to show that every element in K is a sum of two squares, i.e., for all $a \in K$ there exists $x, y \in K$ such that $a = x^2 + y^2$.

(3) Describe $\mathbf{F}_4$ and $\mathbf{F}_8$ *explicitly*. More specifically, find a way to list its elements and to describe addition, multiplication, division. Using your description, find a generator for its multiplicative group (the nonzero elements under multiplication).

(4) Calculate the Galois group of $(x^2-2)(x^2-3)(x^2-5)$ over $\mathbf{Q}$. What are all of the subfields between $\mathbf{Q}$ and its splitting field?

(5) Let k be any field and $k(t)$ its function field. Consider the automorphism $\sigma\colon k(t) \to k(t)$ defined by $\sigma(f(t)) = f(t+1)$. Show that the fixed subfield of σ is k if k has characteristic 0, and is $k(t^p - t)$ if k has characteristic $p > 0$.

2. Further reading

When you compute Galois groups of low degree polynomials, you should expect to see some small finite groups. So it might be a good idea to memorize the structure (subgroup lattice and which subgroups are normal) of the "small" groups, where small has different meanings, but for sure of size ≤ 11. For size 12, there are 5 groups up to isomorphism; there are many references for this, here's one:

`http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/group12.pdf`

The Galois group of the splitting field of a separable polynomial of degree d is some subgroup of the symmetric group S_d. So again, it might be useful to familiarize yourself with the subgroups of S_d when d is small. In this case, $d \leq 5$ is reasonable. Here's a table for the different subgroups of S_5 up to isomorphism: `http://groupprops.subwiki.org/wiki/Subgroup_structure_of_symmetric_group:S5#Table_classifying_isomorphism_types_of_subgroups`