Math 742, Spring 2016
Homework 10
Due: April 15

1. Exercises

(1) Consider each polynomial below as belonging to $\mathbf{Q}[x]$, and determine the Galois group of its splitting field K over $\mathbf{Q}$.
  (a) $x^3 + x + 1$
  (b) $x^3 - 3x + 1$
  (c) $x^3 - 2x + 1$
  (d) $x^3 - x + 1$

(2) (a) Let $\phi(n)$ be the Euler totient function, i.e., the number of positive integers $\leq n$ which are relatively prime to n. Show that for each integer m, there are only finitely many n such that $\phi(n) = m$.
  (b) Let k be a finite extension of $\mathbf{Q}$. Show that k contains only finitely many roots of unity.

(3) Let ℓ, p be prime numbers. This exercise describes how the cyclotomic polynomial $\Phi_\ell(x) = (x^\ell - 1)/(x - 1)$ factors in $\mathbf{F}_p[x]$.
  (a) If $p = \ell$, show that $\Phi_\ell(x) = (x - 1)^{\ell-1}$.
  (b) If $p \neq \ell$, let ζ be a primitive ℓth root of unity in $\overline{\mathbf{F}}_p$. Show that $p^n = 1 \pmod{\ell}$ if and only if $\zeta \in \mathbf{F}_{p^n}$. Conclude that the degree d of the minimal polynomial of ζ over $\mathbf{F}_p$ is the order of p in $\mathbf{F}_\ell^\times$.
  Conclude that $\Phi_\ell(x)$ factors into $(\ell - 1)/d$ distinct irreducible polynomials of degree d.

(4) Let's continue with Example 3 in Lang, §VI.2. Which order 8 group is the Galois group G? Draw the diagram of subfields of K. (You can draw this by hand if you like, though it's good practice to learn how to type this. For example, you can use `xypic` to do this.)