MAT 314: HOMEWORK 7

DUE TH, APRIL 18, 2019

Throughout this problem set, $\mathbb{F}$ is a field.

1. Show that if E is an extension of field F such that any polynomial $f \in F[x]$ splits in E, then E is algebraically closed: every polynomial from $E[x]$ splits in E.

2. Show that any extension of $\mathbb{Q}$ of degree 2 is of the form $E = \mathbb{Q}(\sqrt{d})$ for some rational d.

3. Find degree and minimal polynomial over $\mathbb{Q}$ of the following complex numbers:
(a) $\sqrt{-3} + \sqrt{2}$
(b) $\sqrt{1 + \sqrt{2}}$

4. Let $\mathbb{F}_q$ be the finite field with q elements, $q = p^n$.
Prove that $\mathbb{F}_{p^n}$ contains a subfield with p^m elements if and only if m is a divisor of n. In this case, such a subfield is unique.

5. A complex number z is called *primitive* nth root of unity if $z^n = 1$, but for all $1 \le k < n$, we have $z^k \neq 1$.
(a) Show that if z is a primitive nth root of unity, then all other primitive nth roots of unity are z^k, where k is relatively prime with n. In particular, the number of such primitive roots of unity is $\varphi(n)$, where $\varphi(n)$ is Euler's function.
(b) Define the *cyclotomic polynomial*

$$\Phi_n(x) = \prod (x - z_i) \in \mathbb{C}[x]$$

where the product is taken over all primitive nth roots of unity.
Prove that then

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

where the product is taken over divisors d of n (including 1 and n).
(c) Prove that $\Phi_n(x)$ has integer coefficients.
(d) Compute the following cyclotomic polynomials:
(i) $\Phi_p(x)$, where p is prime
(ii) $\Phi_6(x)$
(iii) $\Phi_4(x)$
(iv) $\Phi_{12}(x)$.

The cyclotomic polynomials play an important role in the study of filed extensions. It is known that for any n, $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.

6. Let $z = e^{2\pi i/5} \in \mathbb{C}$, and let $t = (z + z^{-1})/2 = \cos(2\pi/5)$.
(a) Show that we have a chain of extensions

$$\mathbb{Q} \subset \mathbb{Q}(t) \subset \mathbb{Q}(z)$$

and $[\mathbb{Q}(z) : \mathbb{Q}(t)] = [\mathbb{Q}(t) : \mathbb{Q}] = 2$.
(b) Find the minimal polynomials of t, z.
(c) Write a formula for z which only uses rational numbers, arithmetic operations, and square roots.