MAT 347Y: Groups, rings, and fields
Homework #13
Due on Friday, March 6 at 10:10am in class

1. *Note:* These questions appear in my notes in Section 3, but we skipped explaining them in class so as to include them here in the homework instead. You will want to use everything we did explain from Section 3, though.

   Let us define $\mathcal{P}$ to be the set of positive integers n such that a regular n-gon is constructible with straight edge and compass.

   (a) Prove that $2^m \in \mathcal{P}$ for all $m \geq 0$.

   (b) Prove that if $a \in \mathcal{P}$ and $b|a$, then $b \in \mathcal{P}$.

   (c) Let a, b be positive integers that are relatively prime. Prove that $ab \in \mathcal{P}$ iff $a, b \in \mathcal{P}$. (*Hint:* Use Bezout's identity to relate $2\pi/ab$, $2\pi/a$, and $2\pi/b$.)

   (d) Let $\alpha = \cos 2\pi/5$. Find the minimal polynomial of α over $\mathbb{Q}$. Use it to show that $5 \in \mathcal{P}$.

   (e) For every integer n, let $\zeta_n = e^{2\pi i/n}$. Let p be a prime. What is the minimal polynomial of ζ_p over $\mathbb{Q}$? What is the degree of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$? Conclude that if $p \in \mathcal{P}$, then $p - 1$ is a power of 2.

   (f) *Bonus questions:* Prove that $9 \notin \mathcal{P}$.

   Note: A prime $p \in \mathbb{Z}$ such that $p - 1$ is a power of 2 is called a *Fermat prime*. It is easy to prove that such a prime has to be of the form $p = 2^{2^m} + 1$ for some integer m. The first few ones are

   $$2^1 + 1 = 3, \quad 2^2 + 1 = 5, \quad 2^4 + 1 = 17, \quad 2^8 + 1 = 257, \quad 2^{16} + 1 = 65537.$$

   Fermat conjectured that every number of the form $2^{2^m} + 1$ was prime. If only he had not stopped after the first five terms, he would have realized that such number is not prime already when $m = 6$. Fermat liked to bluff. Sometimes he got luck (like with Fermat's Last Theorem), but not this time.

   In any case, we have reduced the problem of "which regular n-gons are constructible?" to finding out which $p^k \in \mathcal{P}$ for p a Fermat prime and $k \geq 1$. Make sure you convince yourself that this is true.

2. For each of the following field extensions K/F, calculate the Galois group $\mathrm{Gal}(K/F)$. Draw the lattice of intermediate field subextensions. Draw the lattice of subgroups of $\mathrm{Gal}(L/K)$. Describe explicitly the two maps in the Galois correspondance on each case. Do they define a bijection?

(a) $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$

(b) $F = \mathbb{F}_7$, $K = F[X]/(X^3 - 2)$. (*Hint:* The Galois group has order 3.)

Note: Notice the differences between both examples even though they both consist of "adding $\sqrt[3]{2}$".

3. Let $p \in \mathbb{Z}$ be an odd prime. Describe the group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. (By "describe" I mean list its elements and describe what they do to a set of generators, and then identify the isomorphism type of this group – it is isomorphic to a well-know group with name.)

4. We want to compute the Galois group of the (non-algebraic!) extension $\mathbb{C}(X)/\mathbb{C}$. Here, X is a formal variable. Specifically, we want to prove that $\mathrm{Gal}(\mathbb{C}(X)/\mathbb{C}) \cong \mathrm{GL}(2,\mathbb{C})/Z(\mathrm{GL}(2,\mathbb{C}))$. This quotient is called $\mathrm{PGL}(2,\mathbb{C})$.

   Consider the group of invertible 2×2 matrices with entries in $\mathbb{C}$, namely $\mathrm{GL}(2,\mathbb{C})$. For each $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{C})$, define a function $\phi_A : \mathbb{C}(X) \to \mathbb{C}(X)$ by

$$\phi_A(r(X)) = r\left(\frac{aX+b}{cX+d}\right).$$

   Here $r(X)$ is a formal rational expression in X (i.e. a ratio of two polynomials).

   (a) Prove that $\phi_A \in \mathrm{Gal}(\mathbb{C}(x) : \mathbb{C})$.

   (b) Prove that the map $\Phi : \mathrm{GL}_2(\mathbb{C}) \to \mathrm{Gal}(\mathbb{C}(x) : \mathbb{C})$ which sends A to ϕ_A is a group homomorphism.

   (c) Prove that $\ker(\Phi) = Z(GL(2,\mathbb{C})) = \mathbb{C}I = \{cI : c \in \mathbb{C}\}$, where I is the identity matrix.

   (d) Prove that Φ is surjective; in other words, all $\mathbb{C}$-automorphisms of $\mathbb{C}(X)$ are of the above form. (*Hint:* Use Problem 18 on Section 13.2 in the book.)

   (e) Let $H = \Phi(T)$, where $T = \left\{\left(\begin{smallmatrix} 1 & c \\ 0 & 1 \end{smallmatrix}\right) : c \in \mathbb{C}\right\}$. Show that H is a subgroup of $\mathrm{Gal}(\mathbb{C}(X)/\mathbb{C})$. Find the invariant subfield of H. Is $\widehat{G}(\widehat{I}(H)) = H$?