Math 414 Homework Assignment 3

DUE DATE: JAN. 28, 2016

1. Let p be a prime number. In this problem we will find the minimal polynomial of $\xi = e^{2\pi i/p}$, a primitive p-th root of unity. (Primitive means that it is one of the generators of the group $\{z \in \mathbb{Z} \mid z^p = 1\}$ of all p-th roots of unity. In general the primitive n-th roots of unity are, by definition, the generators of $\{z \in \mathbb{C} \mid z^n = 1\}$, and are all of the form $e^{2\pi ik/n}$ with $1 \leqslant k \leqslant n-1$ and $\gcd(k,n) = 1$.)

(a) Show that ξ is a root of the polynomial $f(x) = x^p - 1 \in \mathbb{Q}[x]$.

Since $\xi \neq 1$, this means that ξ is also a root of the polynomial

$$(\dagger) \qquad q(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

If we show that $q(x)$ is irreducible over $\mathbb{Q}$ we will therefore show that $q(x)$ is the minimal polynomial of ξ.

(b) Make the substitution $x = y + 1$ in ($\dagger$) and use Eisenstein's criterion to show that $q(x)$ is irreducible over $\mathbb{Q}$.

2. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ AND THE TOWER LAW.

(a) Show that $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$. (SUGGESTION : Consider the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Question 3 of Homework 2 tells you the degree of this extension.)

(b) What is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$?

(c) If $K \subseteq M \subseteq L$ are fields, the proof of the theorem on degrees in a tower shows us how to a convert a basis of L over M and a basis for M over K into a basis for L over K. What basis do you get if you apply that argument with $K = \mathbb{Q}$, $M = \mathbb{Q}(\sqrt{2})$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$?

(d) Show that 1, $\sqrt{2}$, $\sqrt{3}$, and $\sqrt{6}$ are linearly independent over $\mathbb{Q}$.

3. Let L be the field $L = \mathbb{Q}(\omega)$ where $\omega = e^{2\pi i/3}$.

(a) Find the minimal polynomial of ω over $\mathbb{Q}$.

(b) Your answer from (a) will imply that

$$\mathbb{Q}(\omega) = \{a + b\omega \ \mid \ a, b \in \mathbb{Q}\}\,.$$

Show how to multiply in this basis. That is, given $\alpha = a+b\omega$, $\beta = c+d\omega \in \mathbb{Q}(\omega)$, with $a, b, c, d \in \mathbb{Q}$, show how to write the product $\alpha\beta$ in the basis 1, ω.

(c) Show that the map $a + b\omega \mapsto (a - b) - b\omega$ is an automorphism of $\mathbb{Q}(\omega)$.

(d) Compute the group $\mathrm{Aut}(\mathbb{Q}(\omega)/\mathbb{Q})$.

4. Suppose that $\sigma \in \mathrm{Aut}(\mathbb{C})$.

(a) Explain why σ must fix $\mathbb{Q}$, i.e., $\sigma(\alpha) = \alpha$ for all $\alpha \in \mathbb{Q}$.

(b) If σ is also *continuous* (in the usual topology in $\mathbb{C}$) explain why σ must fix $\mathbb{R}$.

(c) Show that there are only two continuous field automorphisms of $\mathbb{C}$

(d) If $\sigma \in \mathrm{Aut}(\mathbb{C})$ is "given by a formula", (i.e. some recognizable function of the real and imaginary parts), presumably it must be continuous. Explain why it is difficult to write down automorphisms of $\mathbb{C}$ other than the two we know.

5. An impossible problem.

In order to enter Moscow State University as an undergraduate, candidates were required to pass an oral examination by professors in their area of study (as well as other examinations in Russian, and political knowledge). For instance, to enter the mathematics department, the candidate would have to answer mathematical questions posed by some of the faculty.

Sometimes the examiners wanted a particular candidate to fail, and a special supply of difficult or cruel questions was kept in order to make this easier.

The following is one such question[1].

Question: Find rational numbers a, b, c, and d to solve

$$(a + b\sqrt{2}\,)^2 + (c + d\sqrt{2}\,)^2 = 7 + 5\sqrt{2}.$$

You can try expanding the squares and collecting terms, but it isn't so easy to see what to do (a, b, c, and d are in $\mathbb{Q}$, and not just integers).

Prove that this problem is impossible in the following simple way: Assume that there is a solution, apply a field automorphism to the equation, and use a single property of the real numbers to arrive at a contradiction.

[1] At least, I have long thought it was one such question, but in writing the assignment I have been unable to find supporting documentation, or where I got the problem from in the first place.