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 (†) and use Eisenstein's criterion to show that $q(x)$ is irreducible over $\mathbb{Q}$.

Solution.

(a) We have $f(\xi) = \xi^p - 1 = (e^{2\pi i/p})^p - 1 = e^{2\pi i} - 1 = 1 - 1 = 0$.

(b) Using (†) we compute that

$$\begin{aligned} q(y+1) &= \tfrac{(y+1)^p - 1}{(y+1)-1} = \tfrac{(y^p + \binom{p}{1}y^{p-1} + \binom{p}{2}y^{p-2} + \cdots + \binom{p}{p-2}y^2 + \binom{p}{p-1}y + 1) - 1}{y} \\ &= y^{p-1} + \tbinom{p}{1}y^{p-2} + \tbinom{p}{2}y^{p-3} + \cdots + \tbinom{p}{p-2}y + \tbinom{p}{1}. \end{aligned}$$

This polynomial satisfies Eisenstein's criterion with respect to the prime p : The leading term is not divisible by p, all the other terms are divisible by p, and the constant term, while divisible by p, is not divisible by p^2. Therefore the polynomial $q(y+1)$, and hence $q(x)$, 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 $\mathbb{Q}$.

Solution.

(a) By **H1** Q3 and **H2** Q3 we know that $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$. We also know that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. The tower law then tells us that $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. Thus the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$ has degree 2. Since $x^2 - 3 \in \mathbb{Q}(\sqrt{2})[x]$ has $\sqrt{3}$ as a root, the minimal polynomial must divide $x^2 - 3$, but since both of these are monic of degree 2, the minimal polynomial must be $x^2 - 3$.

(b) By our structure theorem for simple extensions, once we know that the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$ has degree 2, we know that 1, $\sqrt{2}$ is a basis for $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$.

(c) Suppose we have three fields $K \subseteq M \subseteq L$. The proof of the tower law tells us that if $\alpha_1,\ldots,\alpha_r$ is a basis of M over K, and if $\beta_1,\ldots,\beta_s$ is a basis of L over M, then the set of rs possible products $\{\alpha_i\beta_j\}_{i=1,j=1}^{r,s}$ is a basis of L over K.

Therefore, since 1, $\sqrt{2}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, and 1, $\sqrt{3}$ a basis of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$, the proof tells us that

$$1 \cdot 1 = 1, 1 \cdot \sqrt{2} = \sqrt{2}, \sqrt{3} \cdot 1 = \sqrt{3}, \text{ and } \sqrt{3} \cdot \sqrt{2} = \sqrt{6}$$

is a basis of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$.

(d) A subset $\{v_1,\ldots,v_t\}$ of a vector space V over a field k is a basis if and only if the set is linearly independent and it spans. In particular, the condition of being a basis includes the condition of being linearly independent. By part (c) we know 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ is a basis for $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$. Thus 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ 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 $\mathrm{Aut}(\mathbb{Q}(\omega)/\mathbb{Q})$.

Solution.

(a) The element $\omega = e^{2\pi i/3}$ is a primitive 3-rd root of unity, and $p = 3$ is a prime. Therefore by Q1 of this homework assignment the minimal polynomial for ω is $q(x) = x^2 + x + 1$.

(b) From part (a) we have $q(\omega) = \omega^2 + \omega + 1 = 0$, which we can rewrite as $\omega^2 = -\omega - 1$. Therefore

$$\begin{aligned}(a + b\omega) \cdot (c + d\omega) &= ac + (ad + bc)\omega + bd\omega^2 = ac + (ad + bc)\omega + bd(-\omega - 1) \\ &= (ac - bd) + (ad + bc - bd)\omega.\end{aligned}$$

(c) Let $\sigma\colon \mathbb{Q}(\omega) \longrightarrow \mathbb{Q}(\omega)$ be the map $\sigma(a + b\omega) = (a - b) - b\omega$ (where $a, b \in \mathbb{Q}$). The formula describes a $\mathbb{Q}$-linear map from $\mathbb{Q}(\omega)$ to itself, whose matrix in the basis 1, ω is

$$\begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix}.$$

The determinant of this matrix is $(1)(-1) - (0)(-1) = -1 \neq 0$, so the matrix is invertible, and hence σ is a bijective map. Thus, σ is a bijective map which fixes $\mathbb{Q}$ and is compatible with addition. It remains to check if σ is compatible with multiplication.

Let $\alpha = a + b\omega$ and $\beta = c + d\omega$ be elements of $\mathbb{Q}(\omega)$ with $a, b, c, d \in \mathbb{Q}$. Using the formula in part (b) we have

$$\begin{aligned}\sigma(\alpha \cdot \beta) &= \sigma\Big((ac - bd) + (ad + bc - bd)\omega\Big) \\ &= \Big((ac - bd) - (ad + bc - bd)\Big) - (ad + bc - bd)\omega. \\ &= (ac - ad - bc) - (ad + bc - bd)\omega.\end{aligned}$$

On the other hand, we have $\sigma(\alpha) = (a-b) - b\omega$, and $\sigma(\beta) = (c-d) - d\omega$, and again using the formula from part (b) to multiply we get

$$\begin{aligned}
\sigma(\alpha)\cdot\sigma(\beta) &= \Big((a-b) - b\omega\Big)\cdot\Big((c-d) - d\omega\Big) \\
&= \Big((a-b)(c-d) - (-b)(-d)\Big) + \Big((a-b)(-d) + (-b)(c-d) - (-b)(-d)\Big)\,\omega \\
&= (ac - bc - ad + bd - bd) + (-ad + bd - bc + bd - bd)\omega \\
&= (ac - bc - ad) - (ad + bc - bd)\omega.
\end{aligned}$$

Comparing the formulas we have

$$\sigma(\alpha\cdot\beta) = (ac - ad - bc) - (ad + bc - bd)\omega = \sigma(\alpha)\cdot\sigma(\beta),$$

and therefore σ is compatible with multiplication. Therefore σ is an automorphism of $\mathbb{Q}(\omega)$.

(d) Our bound on the order of the automorphism group tells us that

$$|\operatorname{Aut}(\mathbb{Q}(\omega)/\mathbb{Q})| \leqslant [\mathbb{Q}(\omega):\mathbb{Q}] = 2,$$

and therefore that $\operatorname{Aut}(\mathbb{Q}(\omega)/\mathbb{Q})$ is either the trivial group or group of order 2.

In part (c) we saw that σ is an automorphism of $\mathbb{Q}(\omega)$ which fixes $\mathbb{Q}$. It is a nontrivial automorphism since $\sigma(\omega) = -1-\omega \neq \omega$. Thus $\operatorname{Aut}(\mathbb{Q}(\omega)/\mathbb{Q}) = \{\mathrm{Id}, \sigma\}$.

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

(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 $\sigma \in \operatorname{Aut}(\mathbb{C})$ 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.

Solution.

(a) In class we have seen that for any field automorphism we have $\sigma(1) = 1$, and hence $\sigma(2) = \sigma(1+1) = \sigma(1) + \sigma(1) = 1 + 1 = 2$, and similarly $\sigma(a) = a$ for every positive integer a. Since σ is a field automorphism it is a group homomorphism under addition, and hence preserves additive inverses, i.e, $\sigma(-a) = -\sigma(a)$ for all $a \in \mathbb{Z}$. Thus (using the result for positive a) we conclude that σ fixes $\mathbb{Z}$. Since field automorphisms are also compatible with division, we then get that for any $a/b \in \mathbb{Q}$, $\sigma(a/b) = \sigma(a)/\sigma(b) = a/b$, and so σ fixes $\mathbb{Q}$.

(b) If $f\colon \mathbb{C} \longrightarrow \mathbb{C}$ is a continuous function, then for any convergent sequence $\{a_n\}_{n\geqslant 0}$ of complex numbers with limit L we have $\lim_{n\to\infty} f(a_n) = f(L)$. This is sometimes also written in the form $\lim_{n\to\infty} f(a_n) = f(\lim_{n\to\infty} a_n)$, to emphasize that continuous functions let us "pull limits through the function".

Every real number L is a limit of a convergent sequence $\{a_n\}_{n\geqslant 0}$ of rational numbers. Hence if $\sigma\colon \mathbb{C} \longrightarrow \mathbb{C}$ is a continuous automorphism of $\mathbb{C}$, we have that $\sigma(a_n) = a_n$ for all n (by part (a) and since $a_n \in \mathbb{Q}$) and therefore

$$L = \lim_{n\geqslant 0} a_n = \lim_{n\geqslant 0} \sigma(a_n) = \sigma(L),$$

where the last equality uses the fact that σ is continuous. I.e., we have that $\sigma(L) = L$ for all $L \in \mathbb{R}$, and hence σ fixes $\mathbb{R}$.

(c) By part (b) any continuous automorphism of $\mathbb{C}$ must fix $\mathbb{R}$, and so belong to $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$. By our theorem bounding the order of the automorphism group, we have $|\mathrm{Aut}(\mathbb{C}/\mathbb{R})| \leqslant [\mathbb{C} : \mathbb{R}] = 2$. However, we already know complex conjugation is a nontrivial automorphism of $\mathbb{C}$. Together with $\mathrm{Id}_{\mathbb{C}}$ this gives $|\mathrm{Aut}(\mathbb{C}/\mathbb{R})| = 2$. As both of these automorphisms are continuous, we see that they are the only continuous automorphisms of $\mathbb{C}$.

(d) If we want to write down an automorphism of $\mathbb{C}$ "with a formula", presumably the formula is a continuous function. From part (c) there are only two such automorphisms of $\mathbb{C}$, and this explains why they are the only two we ever see.

Remark. Recall that if X and Y are sets, then X^Y means the set of all maps from Y to X. (For finite sets X and Y the set of all maps from Y to X has cardinality $|Y|^{|X|}$, which is where the notation comes from.) This notation is sometimes helpful when talking about the cardinality of infinite sets. For instance, $\aleph_0$ is the cardinal used to denote countable sets (like $\mathbb{N}$, $\mathbb{Z}$, or $\mathbb{Q}$). The cardinal $2^{\aleph_0}$ is the cardinality of all maps from $\mathbb{N}$ to 2. If you think about the binary expansion of real numbers in the real interval $(0, 1)$, this shows that $2^{\aleph_0}$ is the same cardinality as $\mathbb{R}$.

It is known that the cardinality of $\mathrm{Aut}(\mathbb{C})$ is $2^{(2^{\aleph_0})}$, i.e, 2 to the cardinality of $\mathbb{R}$. This is quite large, yet we are only able to explicitly write down two of those automorphisms!

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.

Solution. The equation is an equation in $\mathbb{Q}(\sqrt{2})$. The group $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ consists of the identity and the automorphism σ which acts by $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$. Now assume that a solution to

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

exists, witn a, b, c, and $d \in \mathbb{Q}$. Applying σ, this means that the equation

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

would also hold. However, the right side of the equation above is negative ($7 - 5\sqrt{2} < 0$), and the left hand side is a sum of squares of real numbers, which is always greater than or equal to zero. This is a contradiction, and therefore there could have been no solution to the original equation.

REMARK. Groups are the way we encode symmetry in mathematics. The symmetries we are most used to observing are geometric ones, like the symmetries of a cube, icosahedron, a rose-shaped stain glass window, or the bilateral symmetry of the human body. In fact, our brains seem to be primed to notice geometric symmetries. In contrast, our brains are very bad at noticing algebraic ones, as this question demonstrates. One reason for the importance of Galois theory in mathematics is that it is the theory of algebraic symmetries, particularly the algebraic symmetries of fields, and is applicable everywhere that fields come up.

[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.