



UNSW  
A U S T R A L I A



UNIVERSITY OF NEW SOUTH WALES

SCHOOL OF MATHEMATICS AND STATISTICS

---

## Assignment 2

Galois Theory

---

*Author:*  
Edward McDonald

*Student Number:*  
3375335

## Question 1

For this question we work over the field  $\mathbb{Q}$ , and  $f(x) := x^3 + 2x + 2$ .

**Lemma 1.**  *$f$  has no roots in  $\mathbb{Q}$ .*

*Proof.* Let  $a, b \in \mathbb{Z}$  with  $f(a/b) = 0$  and  $\gcd(a, b) = 1$ . Then

$$a^3 + 2ab^3 + 2b^3 = 0.$$

Hence,  $2|a^2$ . Since 2 is prime, we conclude that  $2|a$ .

Let  $a = 2c$ , then

$$8c^3 + 4cb^3 + 2b^3 = 0.$$

Hence  $4|2b^3$ , so  $2|b^3$ . Thus,  $2|b$ .

This contradicts  $\gcd(a, b) = 1$ . Hence  $f$  has no rational roots.  $\square$

**Lemma 2.**  *$f$  is irreducible in  $\mathbb{Q}[x]$ .*

*Proof.* If  $f = gh$  for  $g, h \in \mathbb{Q}[x]$ , then  $\deg(g) + \deg(h) = 3$ . So without loss of generality  $\deg(g) = 1$ . But this means  $f$  has a rational root, which is impossible.  $\square$

**Lemma 3.**  *$f$  has exactly one root over  $\mathbb{R}$ .*

*Proof.* We compute  $f'(x) = 3x^2 + 2 \geq 2 > 0$ . Hence the function  $f$  is monotonically everywhere increasing.

Since  $f(-1) = -1$  and  $f(0) = 2$ , by the intermediate value theorem there is some  $c \in (-1, 0)$  such that  $f(c) = 0$ . Since  $f$  is monotonically increasing, this is the unique zero of  $f$  over  $\mathbb{R}$ .  $\square$

Now let  $\beta_1, \beta_2, \beta_3 \in \mathbb{C}$  be the distinct roots of  $f$  over  $\mathbb{C}$ , with  $\beta_2 = \overline{\beta_3}$ , and  $\beta_1 \in \mathbb{R}$ . Let  $K = \mathbb{Q}(\beta_1, \beta_2, \beta_3)$ .

**Lemma 4.** *Let  $\sigma : \mathbb{C} \rightarrow \mathbb{C}$  be the complex conjugation function,  $\sigma(z) = \overline{z}$ . Then  $\sigma \in \text{Aut}(K/\mathbb{Q})$ ,  $\sigma^2 = \text{id}_{\mathbb{C}}$  and  $\sigma(\beta_2) = \beta_3$ .*

*Proof.* It is evident that  $\sigma \in \text{Aut}(\mathbb{C})$ , and  $\sigma(z) = z$  for all  $z \in \mathbb{Q}$  and  $\sigma^2 = \text{id}_{\mathbb{C}}$ . By definition,  $\sigma(\beta_2) = \beta_3$ ,

Let  $z \in K$ . Then there is some  $p \in \mathbb{Q}[x, y, z]$  such that  $z = p(\beta_1, \beta_2, \beta_3)$ . Since  $\sigma$  fixes  $\mathbb{R}$ , we have  $\sigma(z) = p(\beta_1, \beta_3, \beta_2) \in K$ .

Hence  $\sigma \in \text{Aut}(K/\mathbb{Q})$  has order 2.  $\square$

**Lemma 5.** *As a  $\mathbb{Q}$ -space,  $\mathbb{Q}(\beta_1)$  has a basis  $\{1, \beta_1, \beta_1^2\}$ , and  $[\mathbb{Q}(\beta_1) : \mathbb{Q}] = 3$ .*

*Proof.* Any  $x \in \mathbb{Q}(\beta_1)$  can be expressed as a polynomial,

$$x = b_0 + b_1\beta_1 + b_2\beta_1^2 + b_3\beta_1^3 + \dots$$

with coefficients  $b_j \in \mathbb{Q}$ . However since  $\beta_1^3 = -2 - 2\beta_1$ , we can ignore terms of order greater than 2.

Hence  $\{1, \beta_1, \beta_1^2\}$  spans  $\mathbb{Q}(\beta_1)$ .

These elements of  $K$  are linearly independent over  $\mathbb{Q}$ , since otherwise  $\beta_1$  would satisfy some quadratic in  $\mathbb{Q}[x]$ , which this is impossible as  $f$  is irreducible.

Hence  $\mathbb{Q}(\beta_1)$  is three dimensional as a  $\mathbb{Q}$ -space. Thus  $[\mathbb{Q}(\beta_1) : \mathbb{Q}] = 3$ .  $\square$

It is clear that if  $\sigma \in \text{Aut}(K/\mathbb{Q})$ , and  $f(\gamma) = 0$  then  $f(\sigma(\gamma)) = 0$ .

**Theorem 1.** *There is an injective group homomorphism,  $\text{Aut}(K/\mathbb{Q}) \rightarrow S_3$ .*

*Proof.* Let  $\sigma \in \text{Aut}(K/\mathbb{Q})$ . Then for  $j \in \{1, 2, 3\}$ ,  $\sigma(\beta_j) = \beta_{\tau_\sigma j}$  for some  $\tau_\sigma \in S_3$ . Since  $K$  is generated by  $\{\beta_1, \beta_2, \beta_3\}$  as a  $\mathbb{Q}$ -algebra,  $\sigma$  is uniquely determined by its values on  $\{\beta_1, \beta_2, \beta_3\}$ .

Denote that map  $\psi : \text{Aut}(K/\mathbb{Q}) \rightarrow S_3$  by  $\psi(\sigma) = \tau_\sigma$ .

Let  $\sigma_1, \sigma_2 \in \text{Aut}(K/\mathbb{Q})$ .

Then  $(\sigma_1 \circ \sigma_2)(\beta_j) = \beta_{(\tau_{\sigma_1} \circ \tau_{\sigma_2})(j)}$ .

Hence  $\psi(\sigma_1 \circ \sigma_2) = \psi(\sigma_1) \circ \psi(\sigma_2)$ .

Thus  $\psi$  is a group homomorphism.

$\psi$  must be injective, as if  $\tau_{\sigma_1} = \tau_{\sigma_2}$ , then  $\sigma_1(\beta_j) = \sigma_2(\beta_j)$  for all  $j$ . But elements of  $\text{Aut}(K/\mathbb{Q})$  are uniquely determined by their values on  $\beta_1, \beta_2, \beta_3$ . Hence  $\sigma_1 = \sigma_2$ .  $\square$

**Theorem 2.**  $\text{Aut}(K/\mathbb{Q}) \sim S_3$ .

*Proof.* Since complex conjugation is an element of order 2 in  $\text{Aut}(K/\mathbb{Q})$ , we have a subgroup of order 2 so  $2 \mid |\text{Aut}(K/\mathbb{Q})|$ .

Since  $3 = [\mathbb{Q}(\beta_1) : \mathbb{Q}]$ , we conclude that  $3 \mid [K : \mathbb{Q}(\beta_1)][\mathbb{Q}(\beta_1) : \mathbb{Q}] = [K : \mathbb{Q}] = |\text{Aut}(K/\mathbb{Q})|$ .

Thus  $6 \mid |\text{Aut}(K/\mathbb{Q})|$ . But since there is an injective map from  $\text{Aut}(K/\mathbb{Q})$  to  $S_3$ , we know that  $|\text{Aut}(K/\mathbb{Q})| = 6$ .

Hence the map  $\psi$  in theorem ?? is bijective, hence a group isomorphism.  $\square$

## Question 2

We let  $S_0 \subset \mathbb{R}^2$  be a finite set of points, and  $S_n$  is the set of points constructible from straightedge and compass in  $n$  steps.

The fields  $K_n$  are defined recursively.  $K_0$  is the field extension of  $\mathbb{Q}$  given by the coordinates of points in  $S_0$  and distances between points in  $S_0$ , and  $K_n$  is the field extension of  $K_{n-1}$  generated by the coordinates of points in  $S_n$  and the distances between points of  $S_n$ .

**Theorem 3.** *For  $n \geq 1$ ,  $K_n = K_{n-1}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_t})$  for some  $a_1, a_2, \dots, a_t \in K_{n-1}$ .*

*Proof.* Suppose  $l_1$  and  $l_2$  are lines passing through distinct points of  $S_{n-1}$ , with  $l_1$  passing through  $p_1, q_1 \in S_{n-1}$  and  $p_2, q_2 \in S_{n-1}$ . Then  $l_1$  and  $l_2$  can be parametrised as

$$\begin{aligned} l_1 &: p_1 + \lambda(q_1 - p_1) \\ l_2 &: p_2 + \mu(q_2 - p_2) \end{aligned}$$

for parameters  $\lambda, \mu \in \mathbb{R}$ . We can find the point of intersection by solving the system of linear equations

$$p_1 + \lambda(q_1 - p_1) = p_2 + \mu(q_2 - p_2).$$

By Cramer's rule, since the coordinates of  $p_1, p_2, q_1, q_2$  are in  $K_{n-1}$ , the solution for  $\lambda$  and  $\mu$  must also lie in  $K_{n-1}$ .

Now suppose  $C_1$  and  $C_2$  are two circles with centres  $p = (p_x, p_y), q = (q_x, q_y) \in S_{n-1}$  and radii equal to the lengths of line segments joining points of  $S_{n-1}$ . Denote the radii by  $r_1$  and  $r_2$  respectively. The cartesian equations for the circles are

$$\begin{aligned} C_1 : (x - p_x)^2 + (y - p_y)^2 &= r_1^2 \\ C_2 : (x - q_x)^2 + (y - q_y)^2 &= r_2^2 \end{aligned}$$

We must solve this pair of equations for  $x$  and  $y$ .

Now, by the quadratic formula,  $x \in K_{n-1}(\sqrt{a})$  where  $a \in K_{n-1}(y)$ . Thus there is a polynomial  $f \in K_{n-1}(y)[x]$  such that

$$(f(a) - q_x)^2 + (y - q_y)^2 = r_2^2.$$

blah blah AG. □

**Lemma 6.** *There is an integer  $s \geq 1$  such that  $[K_N : K_0] = 2^s$ .*

*Proof.* Since  $K_n = K_{n-1}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_t})$ , we have

$$[K_n : K_{n-1}] = [K_{n-1}(\sqrt{a_1}, \dots, \sqrt{a_t} : K_{n-1}(\sqrt{a_2}, \dots, \sqrt{a_t})] \dots [K_{n-1}(\sqrt{a_t}) : K_{n-1}].$$

Each of the terms in the product on the left is 2, since each extension is quadratic. Hence,  $[K_n : K_{n-1}]$  is a power of 2. Thus,

$$[K_N : K_0] = [K_N : K_{N-1}][K_{N-1} : K_{N-2}] \dots [K_1 : K_0]$$

is a power of 2. □

**Theorem 4.** *If  $S_0 = \{(0, 0), (1, 0)\}$ , then no  $K_n$  contains a root of  $x^3 - 2$ .*

*Proof.* Since the coordinates and distances in  $S_0$  are rational, we have  $K_0 = \mathbb{Q}$ . Since the polynomial  $x^3 - 2$  is monotonically non-decreasing over  $\mathbb{R}$ , it has a unique real root. By Eisenstein's criterion,  $x^3 - 2$  is irreducible, so if  $\sqrt[3]{2}$  denotes the unique real root,  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ .

Now if  $\sqrt[3]{2} \in K_n$  for some  $n$ , we have  $K_n$  is a field extension of  $\mathbb{Q}(\sqrt[3]{2})$ .

Hence,  $[K_n : \mathbb{Q}(\sqrt[3]{2})]$  is well defined, and

$$[K_n : \mathbb{Q}] = [K_n : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}].$$

Thus  $3 \mid [K_n : \mathbb{Q}]$ .

But this is impossible since we know  $[K_n : \mathbb{Q}] = [K_n : K_0]$  is a power of 2. □