MAU34106 - Galois Theory

Exercise Sheet 3

Trinity College Dublin

Course homepage

Answers are due for Friday, April 4$^{\text{th}}$, 17:00.
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *A biquadratic (100pt)*

The goal of this exercise to compute the Galois group of the splitting field of the polynomial

$$x^4 - 2x^2 - 5$$

over $\mathbb{Q}$. You may freely use the following:

- The polynomial $x^4 - 2x^2 - 5$ is irreducible over $\mathbb{Q}$, with two real roots α and $-\alpha$, and two imaginary roots β and $-\beta$.
- The minimal polynomial of an imaginary number over a subfield of $\mathbb{R}$ is of degree at least 2.
- If γ is algebraic over K, then $[K(\gamma) : K]$ is equal to the degree of the minimal polynomial of γ over K.
- Groups of order 8 can be distinguished using the properties described below the exercise.

1. (10pts) Determine the minimal polynomial of β over $\mathbb{Q}(\alpha)$.

   Hint: Consider writing the coefficients of the polynomial in terms of the roots

2. (10pts) Hence, or otherwise, determine the degree of the splitting field $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$.

3. (30pts) Explain why the $G = \mathrm{Gal}(\mathbb{Q}(\alpha, \beta)/\mathbb{Q})$ is of order 8. By explicitly describing their action on α and β, write down all elements of G.

   Hint: Recall that $\sigma \in G$ must permute the roots of $x^4 - 2x^2 - 5$. In particular, $\sigma(\alpha)$ and $\sigma(\beta)$ must be distinct roots of the polynomial

4. (20pts) Hence identify G with one of the five groups of order 8.

5. (30pts) Apply the Galois correspondence: identify the fixed subfield of a subgroup of order 4 and a subgroup of order 2.

6. (Optional, but good practice!) Using the Galois correspondence, identify all intermediate fields $\mathbb{Q} \subset F \subset \mathbb{Q}(\alpha, \beta)$. Which $F/\mathbb{Q}$ are Galois extensions?

These are the only exercises that you must submit before the deadline

Further exercises on this topic can be found on the course webpage, and, I strongly encourage you to give them a try, as the best way to learn maths is through practice.

They are arranged by theme, and roughly in order of difficulty within each theme, with the first few working as good warm-ups, and the remainder being of similar difficulty to the main exercise. You are welcome to email me if you have any questions about them. The solutions will be made available alongside the problems

Groups of order 8

There are 5 groups of order 8

$$\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^3,\ D_4,\ Q_8$$

More details about these groups can be found here. These can be distinguished by checking whether they are abelian, and how many elements of each order there are:

- $\mathbb{Z}/8\mathbb{Z}$ is an abelian group with 4 elements of order 8, 2 of order 4, 1 of order 2, and the identity.
- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is abelian, with 4 elements of order 4, 3 elements of order 2, and the identity.
- $(\mathbb{Z}/2\mathbb{Z})^3$ is abelian, with 7 elements of order 2, and the identity.
- D_4 is non-abelian, with 2 elements of order 4, 5 elements of order 2, and the identity.
- Q_8 is non-abelian, with 6 elements of order 4, 1 of order 2, and the identity.

Solution 1

1. As β is imaginary, and $\mathbb{Q}(\alpha)$ is a subfield of the reals, we know that β is algebraic of degree at least 2. Looking at the x^2 coefficient of

$$x^4 - 2x^2 - 5 = (x - \alpha)(x + \alpha)(x - \beta)(x + \beta)$$

we see that $\alpha^2 + \beta^2 = 2$, and so β is a root of

$$x^2 + \alpha^2 - 2 \in \mathbb{Q}(\alpha)[x].$$

Since the minimal polynomial of β must have degree at least 2 and must divide this quadratic, we must have that $x^2 + \alpha^2 + 2$ is the minimal polynomial of β over $\mathbb{Q}(\alpha)$.

Alternatively, we can note that $\alpha^2\beta^2 = -5$, and so $\beta^2 + \frac{5}{\alpha^2} = 0$. Thus, by the same reasoning

$$x^2 + \frac{5}{\alpha^2} = x^2 + \alpha^2 + 2$$

is another presentation of the minimal polynomial of β.

2. We know that the degree $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)]$ is equal to the degree of the minimal polynomial of β over $\mathbb{Q}(\alpha)$, and so is equal to 2. Similarly, as x^4-2x^2-5 is irreducible over $\mathbb{Q}$, $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$. Thus, by Tower Law

$$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]=[\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]=2\times 4=8.$$

3. As $\mathbb{Q}(\alpha,\beta)$ is the splitting field of x^4-2x^2-5 over the characteristic 0 field $\mathbb{Q}$, it is both a normal and separable extension and hence Galois. The order of a Galois group is equal to the degree of the extension, so

$$|G|=[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]=8$$

As α,β generate $\mathbb{Q}(\alpha,\beta)$, the action of G is completely determined by its action on α and β. Furthermore, G must map the set

$$\{\alpha,-\alpha,\beta,-\beta\}$$

bijectively to itself. Thus, there are 12 possible set maps, but the only possible field maps are

$$\sigma_1:\begin{cases}\alpha\mapsto\alpha,\\ \beta\mapsto\beta,\end{cases}\qquad \sigma_2:\begin{cases}\alpha\mapsto-\alpha,\\ \beta\mapsto\beta,\end{cases}$$

$$\sigma_3:\begin{cases}\alpha\mapsto\alpha,\\ \beta\mapsto-\beta,\end{cases}\qquad \sigma_4:\begin{cases}\alpha\mapsto-\alpha,\\ \beta\mapsto-\beta,\end{cases}$$

$$\sigma_5:\begin{cases}\alpha\mapsto\beta,\\ \beta\mapsto\alpha,\end{cases}\qquad \sigma_6:\begin{cases}\alpha\mapsto-\beta,\\ \beta\mapsto\alpha,\end{cases}$$

$$\sigma_7:\begin{cases}\alpha\mapsto\beta,\\ \beta\mapsto-\alpha,\end{cases}\qquad \sigma_8:\begin{cases}\alpha\mapsto-\beta,\\ \beta\mapsto-\alpha,\end{cases}$$

as we must exclude any maps for which $\sigma(-\alpha)\neq-\sigma(\alpha)$. We know the Galois group contains 8 elements, so these must be exactly the elements of G.

4. We can easily check that

σ	Order	σ	Order
σ_1	1	σ_2	2
σ_3	2	σ_4	2
σ_5	2	σ_6	4
σ_7	4	σ_8	2

and so we must have $G \cong D_4$.

5. D_4 has 10 subgroups. For the question, we just need to pick one of order 4 and one of order 2, but here we will give every possible subgroup's fixed field. To determine the fixed subfields, we write a generic element of $\mathbb{Q}(\alpha, \beta)$ in the form

$$x = c_1 + c_2\alpha + c_3\alpha^2 + c_4\alpha^3 + c_5\beta + c_6\beta\alpha + c_7\beta\alpha^2 + c_8\beta\alpha^3.$$

   i) $H = \{\sigma_1\}$, which has fixed subfield $\mathbb{Q}(\alpha, \beta)$, which is a Galois extension of $\mathbb{Q}$.

   ii) $H = \{\sigma_1, \sigma_2\}$: An element x is fixed by H if $x = \sigma_2(x)$, or explicitly

$$x = c_1 + c_2\alpha + c_3\alpha^2 + c_4\alpha^3 + c_5\beta + c_6\beta\alpha + c_7\beta\alpha^2 + c_8\beta\alpha^3$$

   is equal to

$$\sigma_2(x) = c_1 - c_2\alpha + c_3\alpha^2 - c_4\alpha^3 + c_5\beta - c_6\beta\alpha + c_7\beta\alpha^2 - c_8\beta\alpha^3.$$

   Comparing coefficients, we find that the fixed subfield is

$$\{c_1 + c_3\alpha^2 + c_5\beta + c_7\beta\alpha^2 \mid c_1, c_3, c_5, c_7 \in \mathbb{Q}\}$$

   which we can also write as $\mathbb{Q}(\alpha^2, \beta)$. This is not a Galois extension of $\mathbb{Q}$, as H is not normal: $\sigma_6\sigma_2\sigma_6^{-1} = \sigma_3 \notin H$.

   iii) $H = \{\sigma_1, \sigma_3\}$: An element x is fixed by H if

$$x = c_1 + c_2\alpha + c_3\alpha^2 + c_4\alpha^3 + c_5\beta + c_6\beta\alpha + c_7\beta\alpha^2 + c_8\beta\alpha^3$$

   is equal to

$$\sigma_3(x) = c_1 + c_2\alpha + c_3\alpha^2 + c_4\alpha^3 - c_5\beta - c_6\beta\alpha - c_7\beta\alpha^2 - c_8\beta\alpha^3.$$

   Comparing coefficients, we see that we must have $c_5 = c_6 = c_7 = c_8 = 0$. Hence, the fixed subfield is

$$\{c_1 + c_2\alpha + c_3\alpha^2 + c_4\alpha^3\} = \mathbb{Q}(\alpha).$$

   This is not a Galois extension of $\mathbb{Q}$, as H is not normal: $\sigma_6^{-1}\sigma_3\sigma_6^{=}\sigma_2 \notin H$.

iv) $H = \{\sigma_1, \sigma_4\}$: An element x is fixed by H if

$$x = c_1 + c_2\alpha + c_3\alpha^2 + c_4\alpha^3 + c_5\beta + c_6\beta\alpha + c_7\beta\alpha^2 + c_8\beta\alpha^3$$

is equal to

$$\sigma_4(x) = c_1 - c_2\alpha + c_3\alpha^2 - c_4\alpha^3 - c_5\beta + c_6\beta\alpha - c_7\beta\alpha^2 + c_8\beta\alpha^3.$$

Comparing coefficients, we see that we must have $c_2 = c_4 = c_5 = c_7 = 0$. Hence, the fixed subfield is

$$\{c_1 + c_3\alpha^2 + c_6\beta\alpha + c_8\beta\alpha^3\}.$$

This is a Galois extension of $\mathbb{Q}$ as H is a normal subgroup.

v) $H = \{\sigma_1, \sigma_5\}$: An element x is fixed by H if

$$x = c_1 + c_2\alpha + c_3\alpha^2 + c_4\alpha^3 + c_5\beta + c_6\beta\alpha + c_7\beta\alpha^2 + c_8\beta\alpha^3$$

is equal to

$$\sigma_5(x) = c_1 + c_2\beta + c_3\beta^2 + c_4\beta^3 + c_5\alpha + c_6\beta\alpha + c_7\alpha\beta^2 + c_8\alpha\beta^3.$$

Using that $\beta^2 = 2 - \alpha^2$, we find that

$$\begin{aligned}\sigma_5(x) =&(c_1 + 2c_3) + (2c_7 + c_5)\alpha - c_3\alpha^2 - c_7\alpha^3 \\ &+ (c_2 + 2c_4)\beta + (c_6 + 2c_8)\beta\alpha - c_4\beta\alpha^2 - c_8\beta\alpha^3.\end{aligned}$$

Comparing coefficients, we see that we must have $c_3 = c_8 = 0$, $c_4 = -c_7$ and $c_5 = c_2 + 2c_4$. Hence, the fixed subfield is

$$\{c_1 + c_2(\alpha + \beta) + c_4(\alpha^3 - \beta\alpha^2 + 2\beta) + c_6\beta\alpha\}.$$

This is not a Galois extension of $\mathbb{Q}$ as H is not normal: $\sigma_2\sigma_5\sigma_2^{-1} = \sigma_8 \notin H$.

vi) $H = \{\sigma_1, \sigma_8\}$: An element x is fixed by H if

$$x = c_1 + c_2\alpha + c_3\alpha^2 + c_4\alpha^3 + c_5\beta + c_6\beta\alpha + c_7\beta\alpha^2 + c_8\beta\alpha^3$$

is equal to

$$\sigma_8(x) = c_1 - c_2\beta + c_3\beta^2 - c_4\beta^3 - c_5\alpha + c_6\beta\alpha - c_7\alpha\beta^2 + c_8\alpha\beta^3.$$

Using that $\beta^2 = 2 - \alpha^2$, we write this in terms of the basis, and compare coefficients to find that we must have $c_3 = c_8 = 0$, $c_4 = c_7$ and $c_5 = -c_2 - 2c_4$. Hence, the fixed subfield is

$$\{c_1 + c_2(\alpha - \beta) + c_4(\alpha^3 + \beta\alpha^2 - 2\beta) + c_6\beta\alpha\}.$$

This is not a Galois extension of $\mathbb{Q}$ as H is not normal: $\sigma_2\sigma_8\sigma_2^{-1} = \sigma_5 \notin H$.

vii) $H = \{\sigma_1, \sigma_6, \sigma_6^2 = \sigma_4, \sigma_6^3 = \sigma_7\}$: An element x is fixed by H if

$$x = c_1 + c_2\alpha + c_3\alpha^2 + c_4\alpha^3 + c_5\beta + c_6\beta\alpha + c_7\beta\alpha^2 + c_8\beta\alpha^3$$

is equal to

$$\sigma_6(x) = c_1 - c_2\beta + c_3\beta^2 - c_4\beta^3 + c_5\alpha - c_6\beta\alpha + c_7\alpha\beta^2 - c_8\alpha\beta^3.$$

Using that $\beta^2 = 2 - \alpha^2$, we write this in terms of the basis, and compare coefficients to find that we must have

$$c_2 = c_5 + 2c_7,\ c_4 = -c_7 = -c_4,\ c_5 = -c_2 - 2c_4,\ c_6 = -c_6 - 2c_8,\ c_3 = 0$$

which implies that $c_2 = c_3 = c_4 = c_5$ and $c_6 = -c_8$. Hence, the fixed subfield is

$$\{c_1 + c_6(\beta\alpha - \beta\alpha^3)\}.$$

This is a Galois extension of $\mathbb{Q}$ as H is a normal subgroup.

viii) $H = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ An element x is fixed by H if

$$x = c_1 + c_2\alpha + c_3\alpha^2 + c_4\alpha^3 + c_5\beta + c_6\beta\alpha + c_7\beta\alpha^2 + c_8\beta\alpha^3$$

is equal to

$$\sigma_2(x) = c_1 - c_2\alpha + c_3\alpha^2 - c_4\alpha^3 + c_5\beta - c_6\beta\alpha + c_7\beta\alpha^2 - c_8\beta\alpha^3$$

and equal to

$$\sigma_3(x) = c_1 + c_2\alpha + c_3\alpha^2 + c_4\alpha^3 - c_5\beta - c_6\beta\alpha - c_7\beta\alpha^2 - c_8\beta\alpha^3$$

Comparing coefficients to find that we must have $c_2 = c_4 = c_5 = c_6 = c_7 = c_8 = 0$. Hence, the fixed subfield is

$$\{c_1 + c_3\alpha^2\} = \mathbb{Q}(\alpha^2).$$

This is a Galois extension of $\mathbb{Q}$ as H is a normal subgroup.

ix) $H = \{\sigma_1, \sigma_4, \sigma_5, \sigma_8\}$: An element x is fixed by H if

$$x = c_1 + c_2\alpha + c_3\alpha^2 + c_4\alpha^3 + c_5\beta + c_6\beta\alpha + c_7\beta\alpha^2 + c_8\beta\alpha^3$$

is equal to

$$\sigma_4(x) = c_1 - c_2\alpha + c_3\alpha^2 - c_4\alpha^3 - c_5\beta + c_6\beta\alpha - c_7\beta\alpha^2 + c_8\beta\alpha^3$$

and equal to

$$\sigma_5(x) = c_1 + c_2\beta + c_3\beta^2 + c_4\beta^3 + c_5\alpha + c_6\beta\alpha + c_7\alpha\beta^2 + c_8\alpha\beta^3$$

Comparing coefficients to find that we must have $c_2 = c_3 = c_4 = c_5 = c_7 = c_8 = 0$. Hence, the fixed subfield is

$$\{c_1 + c_6\beta\alpha^2\}.$$

This is a Galois extension of $\mathbb{Q}$ as H is a normal subgroup.

x) $H = D_4$. The fixed subfield is $\mathbb{Q}$.