MAU34101 Galois theory

Introduction: What is Galois theory about?

Nicolas Mascot
mascotn@tcd.ie
Module web page

Michaelmas 2021–2022
Version: September 13, 2021

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

A calculation in $\mathbb{C}$

In $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$, we have

$$\frac{3+2i}{1-2i} = \frac{(3+2i)(1+2i)}{(1-2i)(1+2i)} = \frac{3+8i+4i^2}{1-4i^2} = \frac{-1+8i}{5}.$$

A calculation in $\mathbb{C}$

In $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$, we have

$$\frac{3+2i}{1-2i} = \frac{(3+2i)(1+2i)}{(1-2i)(1+2i)} = \frac{3+8i+4i^2}{1-4i^2} = \frac{-1+8i}{5}.$$

We can also deduce that

$$\frac{3-2i}{1+2i} = \frac{-1-8i}{5}$$

thanks to complex conjugation $\sigma : \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \overline{z} \end{array}$ being a field automorphism. But why?

A calculation in $\mathbb{C}$

In $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$, we have

$$\frac{3+2i}{1-2i} = \frac{(3+2i)(1+2i)}{(1-2i)(1+2i)} = \frac{3+8i+4i^2}{1-4i^2} = \frac{-1+8i}{5}.$$

We can also deduce that

$$\frac{3-2i}{1+2i} = \frac{-1-8i}{5}$$

thanks to complex conjugation $\sigma : \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \overline{z} \end{array}$ being a field automorphism. But why?

The only thing about i that this calculation uses is $i^2 = -1$. So it will remain valid if we replace i with any number α such that $\alpha^2 = -1$.

A calculation in $\mathbb{Q}(\sqrt{2})$

In $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, we have

$$\frac{3+\sqrt{2}}{1-\sqrt{2}} = \frac{(3+\sqrt{2})(1+\sqrt{2})}{(1-\sqrt{2})(1+\sqrt{2})} = \frac{3+4\sqrt{2}+\sqrt{2}^2}{1-\sqrt{2}^2} = -5-4\sqrt{2}.$$

A calculation in $\mathbb{Q}(\sqrt{2})$

In $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, we have

$$\frac{3+\sqrt{2}}{1-\sqrt{2}} = \frac{(3+\sqrt{2})(1+\sqrt{2})}{(1-\sqrt{2})(1+\sqrt{2})} = \frac{3+4\sqrt{2}+\sqrt{2}^2}{1-\sqrt{2}^2} = -5-4\sqrt{2}.$$

The only thing about $\sqrt{2}$ that this calculation uses is $\sqrt{2}^2 = 2$. So it will remain valid if we replace $\sqrt{2}$ with any number α such that $\alpha^2 = 2$, e.g. $\alpha = -\sqrt{2}$

$$\rightsquigarrow \frac{3-\sqrt{2}}{1+\sqrt{2}} = -5+4\sqrt{2}.$$

A calculation in $\mathbb{Q}(\sqrt{2})$

In $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, we have

$$\frac{3+\sqrt{2}}{1-\sqrt{2}} = \frac{(3+\sqrt{2})(1+\sqrt{2})}{(1-\sqrt{2})(1+\sqrt{2})} = \frac{3+4\sqrt{2}+\sqrt{2}^2}{1-\sqrt{2}^2} = -5-4\sqrt{2}.$$

The only thing about $\sqrt{2}$ that this calculation uses is $\sqrt{2}^2 = 2$. So it will remain valid if we replace $\sqrt{2}$ with any number α such that $\alpha^2 = 2$, e.g. $\alpha = -\sqrt{2}$

$$\rightsquigarrow \frac{3-\sqrt{2}}{1+\sqrt{2}} = -5+4\sqrt{2}.$$

In fact, we see that $\tau : \begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \longrightarrow & \mathbb{Q}(\sqrt{2}) \\ a+b\sqrt{2} & \longmapsto & a-b\sqrt{2} \end{array}$ is a field automorphism.

A calculation in higher degree

Let $P(x) = x^5 + 2x^2 + 3 \in \mathbb{Q}[x]$, whose complex roots are

$$-1.49\cdots, \quad -0.18\cdots \pm 1.02\cdots i, \quad 0.93\cdots \pm 0.98\cdots i.$$

Let α be the real root. What is $\dfrac{1}{\alpha^4 + 2\alpha - 2}$ in

$$\mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 \mid a, b, c, d, e \in \mathbb{Q}\}\ ?$$

A calculation in higher degree

Let $P(x) = x^5 + 2x^2 + 3 \in \mathbb{Q}[x]$, whose complex roots are

$$-1.49\cdots, \quad -0.18\cdots \pm 1.02\cdots i, \quad 0.93\cdots \pm 0.98\cdots i.$$

Let α be the real root. What is $\dfrac{1}{\alpha^4 + 2\alpha - 2}$?

Let $Q(x) = x^4 + 2x - 2 \in \mathbb{Q}[x]$. The Bézout identity $U(x)P(x) + V(x)Q(x) = 1$, where

$$U = -8x^3 + 12x^2 - 18x + 11, \; V = 8x^4 - 12x^3 + 18x^2 - 11x + 16,$$

shows that

$$\frac{1}{\alpha^4 + 2\alpha - 2} = \frac{1}{Q(\alpha)} = V(\alpha) = 8\alpha^4 - 12\alpha^3 + 18\alpha^2 - 11\alpha + 16.$$

A calculation in higher degree

Let $P(x) = x^5 + 2x^2 + 3 \in \mathbb{Q}[x]$, whose complex roots are

$$-1.49\cdots, \quad -0.18\cdots \pm 1.02\cdots i, \quad 0.93\cdots \pm 0.98\cdots i.$$

Let α be the real root. What is $\dfrac{1}{\alpha^4 + 2\alpha - 2}$?

Let $Q(x) = x^4 + 2x - 2 \in \mathbb{Q}[x]$. The Bézout identity $U(x)P(x) + V(x)Q(x) = 1$, where

$$U = -8x^3 + 12x^2 - 18x + 11, \; V = 8x^4 - 12x^3 + 18x^2 - 11x + 16,$$

shows that

$$\frac{1}{\alpha^4 + 2\alpha - 2} = \frac{1}{Q(\alpha)} = V(\alpha) = 8\alpha^4 - 12\alpha^3 + 18\alpha^2 - 11\alpha + 16.$$

In fact, this holds for all 5 roots of P, not just for the real one!

Upshot: automorphisms!

Numbers having the same minimal polynomial $P(x)$ have the same properties (anthying stemming from $P(\alpha) = 0$).

$\rightsquigarrow$ Algebraically, they are indistiguishable.

$\rightsquigarrow$ We expect the existence of automorphisms which exchanges them.

Automorphisms detect membership of subfields

In the extension $\mathbb{R} \subset \mathbb{C}$, the elements of $\mathbb{R}$ are the elements of $\mathbb{C}$ fixed by $\sigma : \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \overline{z} \end{array}$.

In the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$, the elements of $\mathbb{Q}$ are the elements of $\mathbb{Q}(\sqrt{2})$ fixed by $\tau : \begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \longrightarrow & \mathbb{Q}(\sqrt{2}) \\ a + b\sqrt{2} & \longmapsto & a - b\sqrt{2} \end{array}$.

Automorphisms detect membership of subfields

In the extension $\mathbb{R} \subset \mathbb{C}$, the elements of $\mathbb{R}$ are the elements of $\mathbb{C}$ fixed by $\sigma : \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \overline{z} \end{array}$.

In the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$, the elements of $\mathbb{Q}$ are the elements of $\mathbb{Q}(\sqrt{2})$ fixed by $\tau : \begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \longrightarrow & \mathbb{Q}(\sqrt{2}) \\ a + b\sqrt{2} & \longmapsto & a - b\sqrt{2} \end{array}$.

$\rightsquigarrow$ Can detect elements of the small field by the automorphism.

Automorphisms detect membership of subfields

In the extension $\mathbb{R} \subset \mathbb{C}$, the elements of $\mathbb{R}$ are the elements of $\mathbb{C}$ fixed by $\sigma : \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \overline{z} \end{array}$.

In the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$, the elements of $\mathbb{Q}$ are the elements of $\mathbb{Q}(\sqrt{2})$ fixed by $\tau : \begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \longrightarrow & \mathbb{Q}(\sqrt{2}) \\ a + b\sqrt{2} & \longmapsto & a - b\sqrt{2} \end{array}$.

$\rightsquigarrow$ Can detect elements of the small field by the automorphism.

More generally, if we had a big extension $K \subset L$ with several automorphisms, the fixed points of each automorphism would give us subextensions $K \subseteq E \subseteq L$.
$\rightsquigarrow$ **Galois correspondence** between fields and groups (of automorphisms).

Unsolvability by radicals

Field extensions constructed by taking radicals result in "easy" automorphism groups.

In degree ≥ 5, automorphism groups are usually "complicated".

$\rightsquigarrow$ Cannot express the roots by radicals.