Galois Theory - Week 1 - Overview of Galois Theory

Antonio León Villares

January 2023

Contents

Based on the notes by Tom Leinster, Chapter 1

1 Conjugates Over Fields

1.1 Definition: Complex Numbers Conjugate Over Reals

> $z_1, z_2 \in \mathbb{C}$ *are* ***conjugate over*** $\mathbb{R}$ *if:*
>
> $$\forall p \in \mathbb{R}[t] \ : \ p(z_1) = 0 \iff p(z_2) = 0$$
>
> *(Definition 1.1.1)*

- **What is the intuitive notion behind this definition of conjugacy?**
  - if z_1, z_2 are **conjugate over** $\mathbb{R}$, we can think of them as **indistinguishable** from the point of view of the reals
  - that is, any (sensical) property satisfied by z_1 will be satisfied by z_2 over the reals (this behaviour is encoded in the fact that they are roots of the exact same polynomial)
  - for instance, $i = \sqrt{-1}$ and $-i$ are **conjugates**. Some examples:
    - $$p(z) = z^2 + 1 \implies \begin{cases} p(i) = i^2 + 1 = 0 \\ p(-i) = (-i)^2 + 1 = 0 \end{cases}$$
    - $$p(z) = z^4 - 3z^3 - 16z^2 - 3z - 17 \implies \begin{cases} p(i) & = i^4 - 3i^3 - 16i^2 - 3i - 17 \\ & = 1 + 3i + 16 - 3i - 17 \\ & = 0 \\ p(-i) & = (-i)^4 - 3(-i)^3 - 16(-i)^2 - 3(-i) - 17 \\ & = 1 - 3i + 16 + 3i - 17 \\ & = 0 \end{cases}$$

1.2 Lemma: Equivalence Betweeen Conjugacy and Complex Conjugates

Conjugacy *over the reals is closely related to* ***complex conjugacy****.*

> *Let* $z_1, z_2 \in \mathbb{C}$*. Then:*
>
> $$z_1, z_2 \text{ are } \textbf{\textit{conjugate}} \text{ over } \mathbb{R} \iff z_1 = z_2 \text{ or } z_2 = \overline{z_1}$$
>
> *(Lemma 1.1.2)*

Proof.

(1) **Conjugacy Implies Complex Conjugacy or Equality**

Let $z_1 = x + iy$. Notice, z_1 is a root of the polynomial:

$$p(z) = (z - x)^2 + y^2$$

By conjugacy:

$$\begin{aligned} & p(z_1) = 0 \\ \iff\ & p(z_2) = 0 \\ \iff\ & (z_2 - x)^2 = -y^2 \\ \iff\ & z_2 - x = \pm iy \\ \iff\ & z_2 = x \pm iy \end{aligned}$$

so indeed $z_2 = z_1$ or $z_2 = \overline{z_1}$.

(2) **Complex Conjugacy or Equality Implies Conjugacy**

It is clear that z_1 is conjugate to itself, so we just have to show that z_1 is conjugate to $\overline{z_1}$.

Complex conjugation is a **ring homomorphism**, so it preserves **addition** and **multiplication**:

$$\overline{w_1 + w_2} = \overline{w_1} + \overline{w_2} \qquad \overline{w_1 w_2} = \overline{w_1}\,\overline{w_2}$$

Now, consider any polynomial $p \in \mathbb{R}[t]$. Then:

$$p(t) = \sum_{k=1}^{n} a_k t^k$$

so:

$$\overline{p(t)} = \overline{\sum_{k=1}^{n} a_k t^k} = \sum_{k=1}^{n} \overline{a_k}\,\overline{t^k} = \sum_{k=1}^{n} a_k \bar{t}^k = p(\bar{t})$$

where we have used the fact that:

$$a \in \mathbb{R} \implies \overline{a} = a$$

Hence:

$$p(z_1) = 0 \iff \overline{p(z_1)} = \overline{0} \iff p(\overline{z_1}) = 0$$

so indeed z_1 and $\overline{z_1}$ are conjugate over $\mathbb{R}$.

There is an alternative proof in the notes, which directly shows that if p is a polynomial such that $p(z_1) = 0$, then $p(\overline{z_1}) = 0$ too. With the converse argument we complete the proof.
To do this, we let $z_1 = x + iy$ and consider $m(t) = (t - x)^2 + y^2$, which is such that:

$$m(z_1) = m(\overline{z_2})$$

Then, from Honours Algebra, we know that there exist polynomials q, r such that:

$$p(t) = m(t)q(t) + r(t)$$

r will be such that $deg(r) < 2$, so in particular, $r(z_1) \neq 0$ (unless $r = 0$; otherwise $az_1 + b$ is never 0, as a, b are reals). Hence, if we want $p(z_1) = 0$, it must be the case that $p(t) = m(t)q(t)$. But then, $p(\overline{z_1}) = 0$ too!

□

1.3 Definition: Complex Numbers Conjugate Over Rationals

Conjugacy over the rationals is a lot more interesting than over the reals, and it leads to the richness of Galois Theory! One reason for this is that over the rationals, more than 2 numbers can be conjugate.

$z_1, z_2 \in \mathbb{C}$ *are* ***conjugate over*** $\mathbb{Q}$ *if:*

$$\forall p \in \mathbb{Q}[t] \ : \ p(z_1) = 0 \iff p(z_2) = 0$$

1.3.1 Example: Square Roots as Conjugates Over Rationals

The rationals allow for more interesting conjugates to arise. For instance, define:

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

In a similar vein to the work above, if we define a **rational conjugate**:

$$\widetilde{a + b\sqrt{2}} = a - b\sqrt{2}$$

we show that w is conjugate to w and $\tilde{w}$ **over** $\mathbb{Q}$. It is straightforward to see that:

- $\mathbb{Q}(\sqrt{2})$ is closed under **addition** and **multiplication**
- rational conjugation is a **ring homomorphism**:

$$\widetilde{w_1 + w_2} = \tilde{w_1} + \tilde{w_2} \qquad \widetilde{w_1 w_2} = \tilde{w_1}\tilde{w_2}$$

- if $a \in \mathbb{Q}$, then $\tilde{a} = a$

Hence, for any polynomial $p \in \mathbb{Q}[t]$:

$$\widetilde{p(t)} = p(\tilde{t})$$

Hence, if $w \in \mathbb{Q}(\not\in)$:

$$p(w) = 0 \iff \widetilde{p(w)} = \widetilde{0} \iff p(\tilde{w}) = 0$$

so w is conjugate to $\tilde{w}$.

If we want to show this for a specific pair of numbers, an argument based on polynomial factorisation might be more suitable.
The above tells us that $\sqrt{2}$ and $-\sqrt{2}$ are conjugate over $\mathbb{Q}$. This can be directly shown by the fact that if $p(\sqrt{2}) = 0$, we can write:

$$p(t) = (t^2 - 2)q(t) + r(t)$$

where $deg(r) < 2$. Clearly, $r(\sqrt{2}) = 0$ only when r is the 0 polynomial (since r is at most linear, and has rational coefficients), so any rational polynomial with $\sqrt{2}$ as a root is of the form:

$$p(t) = (t^2 - 2)q(t)$$

But then, clearly $p(-\sqrt{2}) = 0$ aswell. Reversing the roles of $\sqrt{2}$ and $-\sqrt{2}$ then confirms that $\pm\sqrt{2}$ are conjugate.

1.4 Definition: Complex Number Tuples Conjugate Over Rationals

Let:

$$\underline{z} = (z_1, \ldots, z_k) \in \mathbb{C}^k \qquad \underline{w} = (w_1, \ldots, w_k) \in \mathbb{C}^k$$

where $k \in \mathbb{N}$.
*$\underline{z}$ and $\underline{w}$ are **conjugate over** $\mathbb{Q}$ if:*

$$\forall p \in \mathbb{Q}[t_1, \ldots, t_k] \ : \ p(z_1, \ldots, z_k) = 0 \iff p(w_1, \ldots, w_k) = 0$$

1.5 Lemma: Complex Conjugate Tuples are Conjugate

The k-tuples:

$$(z_1, \ldots, z_k) \qquad (\overline{z_1}, \ldots, \overline{z_k})$$

*are **conjugate** over $\mathbb{Q}$.*
(Example 1.1.11)

Proof. Working as above, we know that:

$$\overline{p(z_1, \ldots, z_k)} = p(\overline{z_1}, \ldots, \overline{z_k})$$

so:

$$p(z_1, \ldots, z_k) = 0 \iff \overline{p(z_1, \ldots, z_k)} = \overline{0} \iff p(\overline{z_1}, \ldots, \overline{z_k}) = 0$$

□

1.6 Examples of Conjugates

1.6.1 i and $-i$

The tuples $(i, -i)$ and $(-i, i)$ are conjugate (this is the lemma above, but we now show it explicitly). Indeed, any polynomial over 2 variables is of the form:

$$p(t_1, t_2) = \sum_{r,s} a_{rs} t_1^r t_2^s$$

Hence:

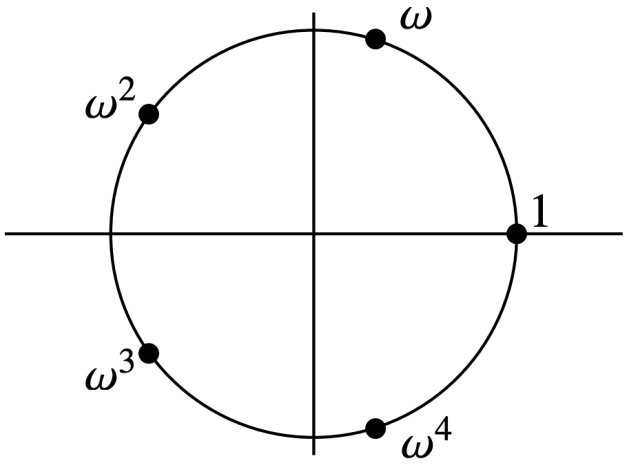
$$\begin{aligned} & p(i, -i) = 0 \\ \iff & \sum_{r,s} a_{rs} i^r (-i)^s = 0 \\ \iff & \overline{\sum_{r,s} a_{rs} i^r (-i)^s} = \bar{0} \\ \iff & \overline{\sum_{r,s} a_{rs} (-i)^r i^s} = \bar{0} \\ \iff & p(-i, i) = 0 \end{aligned}$$

1.6.2 Roots of Unity

The fifth roots of unity are the 5 complex roots of the polynomial:

$$p(z) = 1$$

One can show that these are arranged as a **pentagon**:



where $\omega = e^{\frac{2\pi i}{5}}$. 1 isn't conjugate to any of the other 4 roots (since 1 is a root of $p(t) = t - 1$, but the others aren't). However, $\omega, \omega^2, \omega^3, \omega^4$ are all mutually conjugate. It is easy to see that ω is conjugate to ω^4:

$$\omega^4 = \bar{\omega}$$

and similarly ω^2 and ω^3 are conjugate. It is less obvious to show the remaining conjugacies, however.

More generally, if p is prime and we define $\omega = e^{\frac{2\pi i}{p}}$, the set of roots of unity $\{w^n\}_{n \in [1, p-1]}$ are all conjugate to each other.

Tuple conjugacy is a bit more nuanced. For example:

$$(\omega, \omega^2, \omega^3, \omega^4) \qquad (\omega^4, \omega^3, \omega^2, \omega)$$

are conjugate (we have just taken the complex conjugate of the first tuple). Similarly:

$$(\omega, \omega^2, \omega^3, \omega^4) \qquad (\omega^2, \omega^4, \omega, \omega^3)$$

are conjugate. Intuitively, the idea is that we square each of the elements of the first tuple:

$$\begin{aligned} \omega &\mapsto \omega^2 \\ \omega^2 &\mapsto \omega^4 \\ \omega^3 &\mapsto \omega^6 = \omega \\ \omega^4 &\mapsto \omega^8 = \omega^3 \end{aligned}$$

All in all, we have a cycle (hint: this is critical in defining a Galois group!), which means that these tuples will be "indistinguishable" when viewed from $\mathbb{Q}$. Another way to see this is that if we take corresponding elements in the tuples, and multiply them, we obtain equivalent products. It is easier to see:

$$\omega \cdot \omega^2 = \omega^3 \qquad \omega^2 \cdot \omega^4 = \omega$$

and ω, ω^3 appear in the same position in the tuples.

However, the following tuples are **not** conjugate:

$$(\omega, \omega^2, \omega^3, \omega^4) \qquad (\omega^2, \omega, \omega^3, \omega^4)$$

since for example if we have:

$$p(t_1, t_2, t_3, t_4) = t_2 - t_1^2$$

then:

$$p(\omega, \omega^2, \omega^3, \omega^4) = 0$$

but:

$$p(\omega^2, \omega, \omega^3, \omega^4) = \omega - \omega^4 = \omega - \overline{\omega} \neq 0$$

1.7 Exercises

1. *[Exercise 1.1.6]* **Let $z \in \mathbb{Q}$. Show that z is not conjugate to $w \in \mathbb{C}$, for any $w \neq z$.**

   The polynomial $p(t) = t - z$ has z as a root, but since $w \neq z$, $p(w) \neq 0$. Hence, z can't be conjugate to w.

2. *[Exercise 1.1.10]* **Suppose that $(z_1, \ldots, z_k)$ and $(w_1, \ldots, w_k)$ are conjugate. Show that z_i and w_i are conjugate. Give a counterexample to show that the converse isn't true: that is, if each z_i, w_i are conjugate, the corresponding set of k-tuples aren't conjugate.**

   Since we have $p(z_1, \ldots, z_k) = 0 \iff p(w_1, \ldots, w_k) = 0$, we can define a new polynomial q, which keeps all values except t_i constant. Then clearly:

   $$q(z_i) = 0 \iff q(w_i) = 0$$

   The converse of this is false, as we saw above: $\omega, \omega^2, \omega^3, \omega^4$ are all conjugate, but putting them all in a tuple won't make the tuple conjugate. For instance:

   $$(\omega, \omega^2, \omega^3, \omega^4) \qquad (\omega^2, \omega, \omega^3, \omega^4)$$

2 The Galois Group

2.1 Definition: Galois Group of a Polynomial

One of the fundamental insights of Galois theory is that ***every polynomial has a symmetry group.***

> *Let $f \in \mathbb{Q}[t]$. Let:*
>
> $$\alpha_1, \ldots, \alpha_k$$
>
> *be the k* ***distinct*** *roots of f in $\mathbb{C}$. The* ***Galois group*** *of f is:*
>
> $$Gal(f) = \{\sigma \mid \sigma \in S_k,\ (\alpha_1, \ldots, \alpha_k) \text{ and } (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(k)}) \text{ are conjugate}\}$$
>
> *Moreover, $Gal(f)$ is a* ***subgroup*** *of S_k.*
> *(Definition 1.2.1)*

- **What roots would be considered when defining the Galois group of $f(t) = t^5(t-1)^9$?**
  - whilst this has 14 roots, it only has 2 distinct roots, so:
    $$\{\alpha_1, \alpha_2\} = \{0, 1\}$$
- **Doesn't the definition of Galois group depend on the ordering of the roots? If so, can't the same polynomial have different Galois groups?**
  - different ordering will indeed mean that there will be different permutations in $Gal(f)$
  - however, it can be shown that the different Galois groups of f are **conjugate**, in the **group theoretic sense**; that is, if H_1, H_2 are 2 Galois groups for f, $\exists a \in S_k$, such that:
    $$aH_1a^{-1} = H_2$$
  - in particular, this means that the different Galois groups are **isomorphic**, and so, **algebraically indistinguishable**
  - thus, $Gal(f)$ is a **well-defined** group, independent of **ordering**

2.2 Examples for Galois Group Intuition

2.2.1 Polynomials with Only Rational Roots

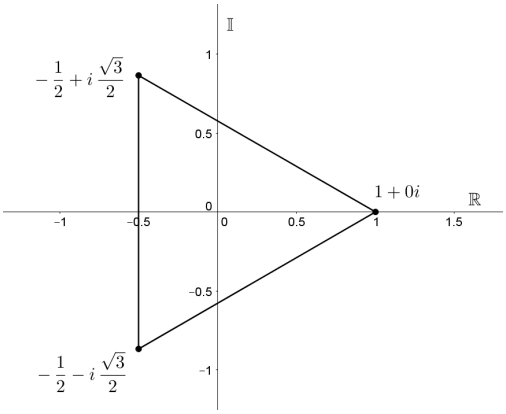
- let f be a polynomial over $\mathbb{Q}$, and assume it has k **rational** roots:
  $$\alpha_1, \ldots, \alpha_k$$
- over $\mathbb{Q}$, no rational is conjugate to other rationals: a rational q is the unique root to the polynomial $p(t) = t - q$
- if $\sigma \in Gal(f)$, then:
  $$(\alpha_1, \ldots, \alpha_k) \qquad (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(k)})$$
  are **conjugate**, so in particular α_i is conjugate to $\alpha_{\sigma(i)}$
- this is only possible if $\alpha_i = \alpha_{\sigma(i)}$
- hence, $Gal(f) = \{\iota\}$, the trivial subgroup of S_k

2.2.2 Quadratic Polynomials

- let f be a quadratic over $\mathbb{Q}$
- if the 2 roots of f are rational, then $Gal(f) = \{\iota\}$
- if the 2 roots are complex conjugate, say we have $z_1, z_2 = \bar{z_1}$. We know that (z_1, z_2) is conjugate to its complex conjugate:
$$(\bar{z_1}, \bar{z_2}) = (z_2, z_1)$$
which is precisely the non-trivial transposition of S_2. Hence, $Gal(f) = S_2$.
- the last case occurs when the 2 roots are real, in which case it can be shown that again $Gal(f) = S_2$

2.2.3 Cubic Polynomial

- consider a cubic f with only one rational root
- the rational root can be "distinguished" (i.e isn't conjugate) to the remaining 2 complex conjugate roots
- hence, any $\sigma \in Gal(f)$ must leave the rational root fixed
- the complex conjugate roots are conjugate over $\mathbb{Q}$, so the transposition which switches them will be part of the Galois group (in fact, this will be the only non-trivial element of $Gal(f)$)



This reasoning might make more intuitive sense when looking at the roots in the complex plane: the only symmetry which preserves the conjugacy relation is precisely the reflection corresponding to complex conjugation.

2.2.4 Galois Group of a Quartic with Roots of Unity

- consider:
$$f(t) = t^4 + t^3 + t^2 + t + 1$$
- notice, we can write:
$$t^5 - 1 = (t-1)f(t)$$
so the roots of f are precisely the 5th roots of unity (except for $t = 1$)
- the elements of $Gal(f)$ will be the permutations $\sigma \in S_4$, such that:
$$(\omega, \omega^2, \omega^3, \omega^4) \qquad (\omega^{\sigma(1)}, \omega^{\sigma(2)}, \omega^{\sigma(3)}, \omega^{\sigma(4)})$$
are conjugate

- we already saw that **transpositions** won't be part of the Galois group. For example, $(1\ 2) \notin Gal(f)$, since:
$$(\omega, \omega^2, \omega^3, \omega^4) \qquad (\omega^2, \omega, \omega^3, \omega^4)$$
aren't conjugate (use the polynomial $p(t_1, t_2, t_3, t_4) = t_1^2 - t_2$))
- in fact, $Gal(f) = \langle (1\ 2\ 4\ 3) \rangle \cong C_4$
- recall, (1 2 4 3) is precisely the permutation we obtained when squaring each of the roots, and which gave us that:
$$(\omega, \omega^2, \omega^3, \omega^4) \qquad (\omega^2, \omega^4, \omega, \omega^3)$$
are conjugate

2.2.5 Galois Group of a General Cubic

- if $f(t) = t^3 + bt^2 + ct + d$ has **no rational roots**, then:
$$Gal(f) \cong \begin{cases} A_3, & \sqrt{-27d^2 + 18bcd - 4c^3 - 4b^3d + b^2c^2} \in \mathbb{Q} \\ S_3, & otherwise \end{cases}$$
- recall, A_3 is the **alternating group**: the **subgroup** of S_3 containing only the **even** permutations

2.3 Exercises

1. *[Exercise 1.2.2]* **Show that $Gal(f)$ is a subgroup of S_k.**

3 Radicals and Solvable Polynomials

3.1 Definition: Radical Complex Number

> *A **complex number** is **radical** if it can be obtained from the **rationals** by using:*
>
> - *the standard **arithmetic operations***
> - *kth roots*

3.2 Definition: Polynomials Solvable by Radicals

> *A **polynomial** is **solvable by radicals** if **all** of its complex roots are **radical**.*

3.2.1 Example: Radicals and Roots of Polynomials

- all **quadratics** over $\mathbb{Q}$ are solvable by radicals: we have the **quadratic formula**:
$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$
- similarly, there are **cubic** and **quartic** formulae

- some **quintics** are solvable by radicals: for example:

$$(t-123)^5+456$$

has roots $123+\sqrt[5]{-456}$

3.3 Theorem: Solvable Galois Groups

Let $f \in \mathbb{Q}[t]$. Then:

$$f \text{ is } \textbf{\textit{solvable by radicals}} \iff Gal(f) \text{ is a } \textbf{\textit{solvable group}}$$

(Theorem 1.3.5)

3.3.1 Group Theory Recap: Solvable Groups

***Subnormal series** are a **generalisation** of **composition series**. In particular, a **subnormal series** of G is a **chain** of subsequent **normal subgroups**:*

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_s = G$$

*A group G is **solvable**, provided that it has a **subnormal series**:*

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_s = G$$

*such that each **factor**:*

$$G_{i+1}/G_i$$

*is **abelian**.*

*Let G be a **group**, and let $N \triangleleft G$. Then, G is **solvable if and only if**:*

- *N is **solvable***
- *G/N is **solvable***

*If G is **solvable** and $H \leq G$, then H is **solvable**.*

- **Why do we have formulae for quadratics, cubics and quartics?**
  - recall, if $deg(f) = n$, $Gal(f)$ is isomorphic to a subgroup of S_n
  - now, S_4 is solvable: it has a subnormal series with abelian factors:

    $$\{e\} \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$$

    where V_4 is the Klein-4 group (the group of 4 elements in which each element is its own inverse; it is abelian, since it has order 2^2, and 2 is prime). Using Lagrange's Theorem, we can see that the quotients have prime order, and so are cyclic, and therefore abelian
  - for S_3 and S_2, A_3, A_2 are normal, abelian subgroups, which gives the subnormal series
  - moreover, any subgroup of S_2, S_3, S_4 will be solvable
  - hence, it follows that quadratics, cubics and quartics are solvable by radicals!
- **Can there be a quintic formula?**
  - S_5 isn't solvable: the only (non-trivial) subgroup of S_5 is A_5, and A_5 is simple, and non-abelian
  - hence, S_5 doesn't have a subnormal series of abelian factors
  - if we find a polynomial which has S_5 as its Galois Group, then the polynomial won't be solvable by radicals, and thus, there can't exist a quintic formula
  - we will see that $f(t) = t^5 - 6t + 3$ is one such quintic