MAU34101 Galois theory

3 - The Galois group of a polynomial

Nicolas Mascot

mascotn@tcd.ie

Module web page

Michaelmas 2021–2022

Version: December 3, 2021

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

The Galois group of a polynomial

The Galois group of a polynomial

Let K be a field, and $F(x) \in K[x]$ separable of degree n (but possibly reducible).

Then $F(x)$ has n distinct roots $\alpha_1, \cdots, \alpha_n \in \overline{K}$.

Let $\mathrm{Spl}_K(F) = K(\alpha_1, \cdots, \alpha_n)$, a splitting field of F over K. It is a Galois extension of K: normal because splitting field, separable because F is separable.

Definition

$$\mathrm{Gal}_K(F) = \mathrm{Gal}(\mathrm{Spl}_K(F)/K).$$

Remark

Conversely, any Galois extension of K is the splitting field of some separable polynomial $\rightsquigarrow$ no loss of generality.

Reminder: What does $\mathrm{Gal}_K(F)$ look like?

Let $\sigma \in \mathrm{Gal}_K(F) = \mathrm{Gal}(K(\alpha_1, \cdots, \alpha_n)/K)$.

- σ is completely determined by what it does to the generators $\alpha_1, \cdots, \alpha_n$ of the extension.
- For each j, $\sigma(\alpha_j)$ is again a root of F, because σ is a K-automorphism so preserves rootness in $K[x]$.

$\rightsquigarrow$ σ induces a <u>permutation</u> of the roots of F, and this permutation characterises σ.

$\rightsquigarrow$ We view $\mathrm{Gal}_K(F)$ as a subgroup of S_n.

Orbits and transitivity

Definition (Orbit)

Let α_j be a root of F. Its orbit under $G = \mathrm{Gal}_K(F)$ is

$$\{\sigma(\alpha_j) \mid \sigma \in G\} \subseteq \{\textit{Roots of } F\}.$$

The orbits form a partition (disjoint union) of the set of roots of F.

Definition (Transitive)

We say that G is transitive if there is only one orbit.

Equivalently, this means that for all j, k, we can find $\sigma \in G$ such that $\sigma(\alpha_j) = \alpha_k$.

Factors = Orbits

Theorem

Let O be the set of orbits. Then for each orbit $o \in O$, the polynomial $F_o(x) = \prod_{\alpha \in o}(x - \alpha)$ lies in $K[x]$ and is irreducible.
Therefore, the complete factorisation of $F(x)$ in $K[x]$ is

$$F(x) = \prod_{o \in O} F_o(x)$$

(assuming F is monic, else we get the rescaled monic version).

Proof.

Let α_j be a root of F, and let $o \in O$ be its orbit. By the theorem on Galois extensions, $F_o(x)$ is the min poly of α over K. $\square$

Factors = Orbits

Theorem

Let O be the set of orbits. Then for each orbit $o \in O$, the polynomial $F_o(x) = \prod_{\alpha \in o} (x - \alpha)$ lies in $K[x]$ and is irreducible.

Therefore, the complete factorisation of $F(x)$ in $K[x]$ is

$$F(x) = \prod_{o \in O} F_o(x)$$

(assuming F is monic, else we get the rescaled monic version).

Corollary

F is irreducible over K $\iff$ $\mathrm{Gal}_K(F)$ is transitive.

Factors = Orbits

Example

Let $K = \mathbb{Q}$, $F(x) = (x^2 - 2)(x^2 - 3)$.
The roots of F are $\pm\sqrt{2}$, $\pm\sqrt{3}$, so F is separable.

$\operatorname{Spl}_{\mathbb{Q}}(F) = \mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
We saw in the previous chapter that $\# \operatorname{Gal}_{\mathbb{Q}}(F) = 4$, with elements $\sigma : \sqrt{2} \mapsto \pm\sqrt{2}$, $\sqrt{3} \mapsto \pm\sqrt{3}$, but never $\sqrt{2} \mapsto \pm\sqrt{3}$ as they must preserve rootness of $x^2 - 2, x^2 - 3 \in \mathbb{Q}[x]$.

$\rightsquigarrow$ Two orbits: $\{\sqrt{2}, -\sqrt{2}\}$ and $\{\sqrt{3}, -\sqrt{3}\}$.

$\rightsquigarrow$ Two irreducible factors over $\mathbb{Q}$:
$(x - \sqrt{2})(x + \sqrt{2}) = x^2 - 2$ and $(x - \sqrt{3})(x + \sqrt{3}) = x^2 - 3$.

Factors = Orbits

Example

Keep the same F, but view it as an element of $K[x]$ where $K = \mathbb{Q}(\sqrt{2})$.

Then $\mathrm{Gal}_K(F) = \mathrm{Gal}(K(\sqrt{3})/K) \simeq \mathbb{Z}/2\mathbb{Z}$ flips the sign of $\sqrt{3}$ but can no longer touch $\sqrt{2}$

$\rightsquigarrow$ 3 orbits: $\{\sqrt{2}\}$, $\{-\sqrt{2}\}$, and $\{\sqrt{3}, -\sqrt{3}\}$

$\rightsquigarrow$ 3 irreducible factors over K: $x - \sqrt{2}$, $x + \sqrt{2}$, and $x^2 - 3$.

Reminders on permutations

The example we will use in this section

Fix $n \in \mathbb{N}$.

We are going to review a few concepts about permutations, i.e. elements of S_n.

In this section, for examples, we will take $n = 6$ and $\tau \in S_6$ the permutation

$$1 \mapsto 4, \ 2 \mapsto 6, \ 3 \mapsto 3, \ 4 \mapsto 5, \ 5 \mapsto 1, \ 6 \mapsto 2.$$

Cycles

Definition (Cycle)

Let $k \leqslant n$. A k-cycle is a permutation $c \in S_n$ of the form

$$x_1 \mapsto x_2 \mapsto \cdots \mapsto x_k \mapsto x_1$$

for some distinct $x_1, \cdots, x_k \in \{1, 2, \cdots, n\}$ called the support of c, and such that c fixes all the other points of $\{1, \cdots, n\}$.
Notation: $c = (x_1, x_2, \cdots, x_k)$.

Theorem

Any permutation can be decomposed as a product of cycles with pairwise disjoint supports.

Proof.

Look at the orbits of the permutation.
(Image: we have a box of elastic bands, and we are pulling the bands out of the box, one at a time.) □

Order

Proposition

Let $\sigma \in S_n$ have cycle decomposition $k_1 + k_2 + \cdots$, meaning a k_1-cycle, a k_2-cycle, $\cdots$. Then σ has order $\operatorname{lcm}(k_1, k_2, \cdots)$.

Proof.

The order of a k-cycle is k.
Besides, cycles with disjoint supports commute. $\square$

Example

We have seen that the cycle decomposition of τ is $2+3$ (or $2+3+1$ if you prefer), so the order of τ is

$$\operatorname{lcm}(2,3) \ \big(\text{or } \operatorname{lcm}(2,3,1)\big) = 6.$$

Signature

Theorem

There is a sign morphism $\varepsilon : S_n \longrightarrow \{\pm 1\}$ *characterised by*

$$\varepsilon(k\text{-}cycle) = (-1)^{k+1}.$$

Mnemonic: It would have been easier if $\varepsilon(k\text{-cycle}) = (-1)^k$; but 1-cycles are the identity so they must have sign $+1$.

Example

$$\varepsilon(\tau) = \varepsilon\big((1,4,5)(2,6)\big) = \varepsilon\big((1,4,5)\big)\varepsilon\big((2,6)\big) = +1 \times -1 = -1.$$

Permutations with $\varepsilon = +1$ are called <u>even</u>, and those with $\varepsilon = -1$ are called <u>odd</u>.

Note that a k-cycle is even when k is odd, and vice-versa. ☹

The alternating group A_n

Definition (Alternating group)

The alternating group is $A_n = \operatorname{Ker} \varepsilon \leqslant S_n$.

In other words, it is the subset of even permutations.
Actually, A_n is normal in S_n since it is a kernel.

Remark

As soon as $n \geqslant 2$, ε is surjective, so $\# A_n = \frac{1}{2} \# S_n = \frac{n!}{2}$.

Theorem

If $n \geqslant 5$, *then* A_n *is a simple group (has no nontrivial normal subgroups).*

When is $\mathrm{Gal}_K(F) \leqslant A_n$?

The discriminant returns

Let again $F(x) \in K[x]$ separable.

Theorem

$$\mathrm{Gal}_K(F) \leqslant A_n \iff \operatorname{disc} F \textit{ is a square in } K.$$

See notes for the proof.

Remark

$\operatorname{disc} F \neq 0$ since F is separable.

Example

Let $F(x) = x^3 - 6x - 2 \in \mathbb{Q}[x]$.
Then $\operatorname{disc} F = -4(-6)^3 - 27(-2)^2 = 756 = 2^2 3^3 7^1$ is not zero so F is separable, but is not a square so $\mathrm{Gal}_{\mathbb{Q}}(F) \not\leqslant A_3$.
Besides F is irreducible over $\mathbb{Q}$ (Eisenstein) so $\mathrm{Gal}_{\mathbb{Q}}(F)$ is transitive. The classification of the subgroups of S_3 shows that

$$\mathrm{Gal}_{\mathbb{Q}}(F) = S_3.$$

The discriminant returns

Let again $F(x) \in K[x]$ separable.

Theorem

$$\mathrm{Gal}_K(F) \leqslant A_n \iff \operatorname{disc} F \textit{ is a square in } K.$$

See notes for the proof.

Remark

$\operatorname{disc} F \neq 0$ since F is separable.

Example

Let again $F(x) = x^3 - 6x - 2$ but seen in $\mathbb{R}[x]$ this time.
Then still $\operatorname{disc} F = 756 \neq 0$, but this time $\operatorname{disc} F$ is a square in $\mathbb{R}$, so $\mathrm{Gal}_{\mathbb{R}}(F) \leqslant A_3$.
(In fact, all 3 roots of F are real, so $\mathrm{Spl}_{\mathbb{R}}(F) = \mathbb{R}$ itself, so actually $\mathrm{Gal}_{\mathbb{R}}(F) = \{\mathrm{Id}\}$.)

Dedekind's theorem

Dedekind's theorem

Theorem

Let $F(x) \in \mathbb{Z}[x]$ monic and separable, and let $p \in \mathbb{N}$ prime. Suppose the factorisation $F(x) = \prod_j F_j(x)$ of $F(x)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$ involves no repeated factors. Then $\operatorname{Gal}_{\mathbb{Q}}(F)$ contains an element whose cycle decomposition is

$$(\deg F_1) + (\deg F_2) + \cdots .$$

See notes for the proof.

Remark

Since $\mathbb{Z}/p\mathbb{Z}$ is perfect, F mod p has repeated factors iff. $\operatorname{disc}(F \bmod p) = 0$.
But $\operatorname{disc} F$ is essentially defined as a determinant in the coefs of F and F', so $\operatorname{disc}(F \bmod p) = \operatorname{disc}(F) \bmod p$, so F has repeated factors mod p iff. $p \mid \operatorname{disc} F$.
As $\operatorname{disc} F \neq 0$, this only happens for finitely many p.

Dedekind's theorem

Theorem

Let $F(x) \in \mathbb{Z}[x]$ monic and separable, and let $p \in \mathbb{N}$ prime. Suppose the factorisation $F(x) = \prod_j F_j(x)$ of $F(x)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$ involves no repeated factors. Then $\operatorname{Gal}_{\mathbb{Q}}(F)$ contains an element whose cycle decomposition is

$$(\deg F_1) + (\deg F_2) + \cdots .$$

See notes for the proof.

Remark

We can try various primes p with the same F.
Cebotarev's densitity theorem states that when we do so, we hit elements of $\operatorname{Gal}_{\mathbb{Q}}(F)$ in a uniform way.

Practical factoring mod p

To apply Dedekind, we need to be able to factor in $\mathbb{Z}/p\mathbb{Z}[x]$.

Theorem

Let $G(x) \in \mathbb{Z}/p\mathbb{Z}[x]$.

- *G has repeated factors iff.* $\gcd(G, G') \neq 1$.
- *G has factor(s) of deg 1 iff. G has roots.*
- *More generally, for each $d \in \mathbb{N}$, G has factors of degree $\mid d$ iff.* $\gcd(G, x^{p^d} - x) \neq 1$.

Proof.

The point is that $x^{p^d} - x$ is the product of all monic irreducible polynomials of degree $\mid d$ in $\mathbb{Z}/p\mathbb{Z}$, so taking the gcd filters the factors of G of degree $\mid d$. See notes for details. □

Practical factoring mod p

Example

Let $F(x) = x^5 - x - 1$. We find $\operatorname{disc} F = 2869 = 19 \times 151$, so we can use any $p \notin \{19, 151\}$.

Let us factor F mod $p = 2$. $2 \nmid 2869$, so no repeated factors. The possible roots at 0 and 1, but none is a root, so no factor of degree 1. By Euclid, we find $\gcd(F, x^4 - x) = x^2 + x + 1$, so we have found the irreducible factor $x^2 + x + 1$ of F, and F has no more factors of degree $\mid 2$.
So F mod 2 factors as $2 + 3$; by Dedekind, $\mathrm{Gal}_{\mathbb{Q}}(F) \leqslant S_5$ contains an element of the form $(*, *)(*, *, *)$.

Let us now try $p = 3$. Again $3 \nmid 2869$ so no repeated factors. The possible roots are $0, 1, 2$, but none of them is a root. Besides, we find $\gcd(F, x^9 - x) = 1$, so F mod 3 actually has no factors of degree $\mid 2$. Therefore F mod 3 is irreducible, so $\mathrm{Gal}_{\mathbb{Q}}(F)$ contains a 5-cycle by Dedekind.

Proving that the Galois group is S_n

Proposition

Let $G \leqslant S_n$ be transitive. If G contains a 2-cycle and an $(n-1)$-cycle, then $G = S_n$.

Proof.

WLOG (relabel), the $n-1$-cycle is $c = (1, 2, \cdots, n-1) \in G$. Let $t = (i, j) \in G$ be the 2-cycle.

Since G is transitive, there exists $g \in G$ such that $g(j) = n$; then $G \ni gtg^{-1} = \big(g(i), g(j)\big)$, so WLOG $j = n$.

Then for all $x \in \mathbb{Z}$, $G \ni c^x t c^{-x} = \big(c^x(i), c^x(n)\big) = \big(c^x(i), n\big)$, so $G \ni (k, n)$ for all $k < n$.

But then $G \ni (u, n)(v, n)(u, n) = (u, v)$ for all u, v, and those generate S_n. $\square$

Proving that the Galois group is S_n

Example

Let again $F(x) = x^5 - x - 1 \in \mathbb{Q}[x]$, and $G = \mathrm{Gal}_{\mathbb{Q}}(F) \leqslant S_5$.

By Gauss, any factorisation of F over $\mathbb{Q}$ would actually happen over $\mathbb{Z}$, and thus survive mod 3; but we have seen that F mod 3 is irreducible, so F is irreducible over $\mathbb{Q}$; therefore G is transitive.

The factorisation of F mod 2 shows $G \ni g_2 = (*, *)(*, *, *)$; in particular $G \ni g_2^3 = (*, *)$, so WLOG $(1, 2) \in G$.

Besides, the factorisation of F mod 3 shows that G contains a 5-cycle c (which reproves transitivity).

Replacing c with one of its powers, we may assume that $c(1) = 2$, so WLOG $c = (1, 2, 3, 4, 5)$ (relabel the other roots if necessary). Then $G \ni ct = (1, 3, 4, 5)$. The proposition then shows that $G = S_5$.