Computing the Galois group of a polynomial

Curtis Bright

University of Waterloo

April 8, 2013

What is a Galois group?

- Let $f \in \mathbb{Q}[x]$ have roots $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. Then the *Galois group* of f is defined to be

$$\mathrm{Gal}(f) \coloneqq \mathrm{Gal}(\mathbb{Q}(\alpha_1, \ldots, \alpha_n)/\mathbb{Q}).$$

  That is, the group of automorphisms of the splitting field of f over $\mathbb{Q}$.

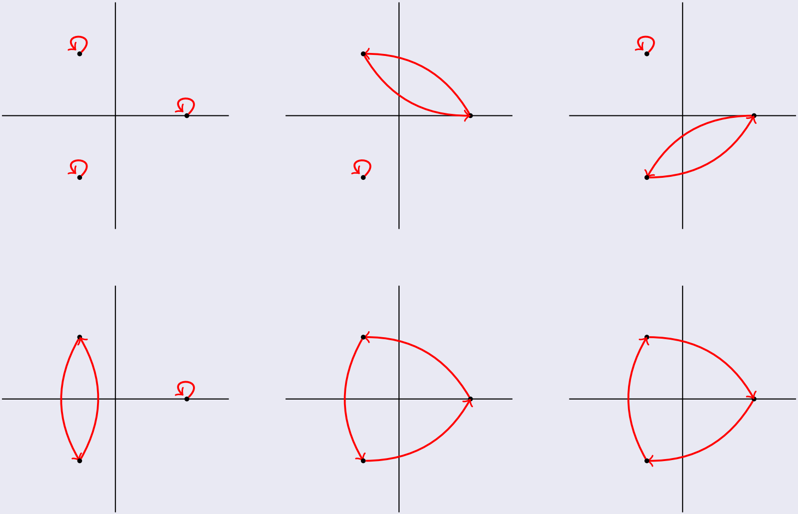
What do the automorphisms $\sigma \in \mathrm{Gal}(f)$ look like?

- The values $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ completely determine σ.
- $\sigma(\alpha_i)$ is also a root of f:

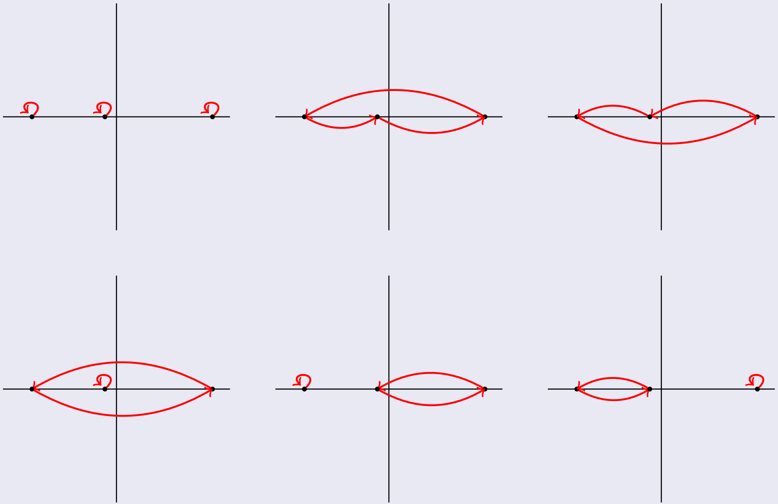
  $$f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = \sigma(0) = 0$$

  Similarly, $\sigma^{-1}(\alpha_i)$ is a root of f.
- In other words, σ permutes the roots of f, and we can consider $\sigma \in S_n$.

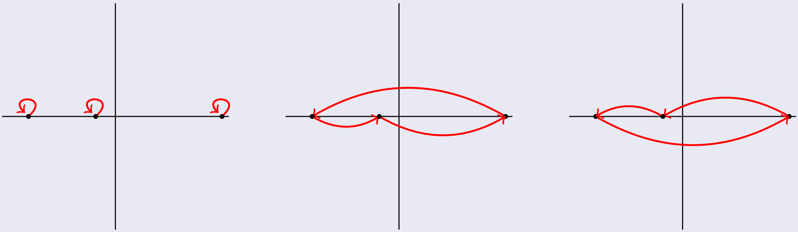
Example: $\mathrm{Gal}(x^3 - 2)$



Example: $\mathrm{Gal}(x^3 - 4x - 1)$



Example: $\mathrm{Gal}(x^3 - 3x - 1)$



Why aren't there any transpositions in $\mathrm{Gal}(x^3 - 3x - 1)$?

- The discriminant of $x^3 - 3x - 1$ is

$$\Delta \coloneqq (-1)^{3(3-1)/2} \prod_{i \neq j} (\alpha_i - \alpha_j) = 81.$$

So σ fixes $\sqrt{\Delta} = 9 \in \mathbb{Q}$, as well as

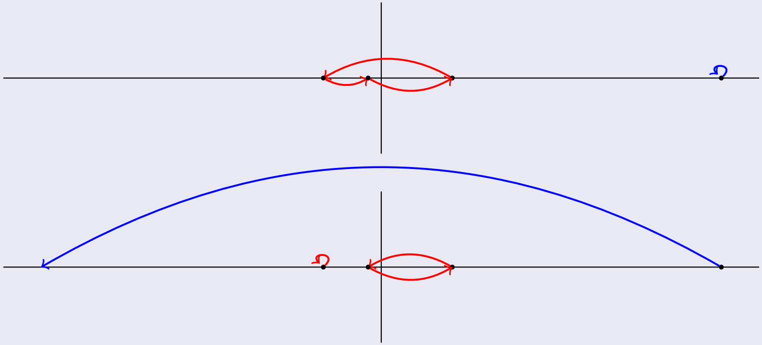
$$\prod_{i<j} (\alpha_i - \alpha_j) = \pm\sqrt{\Delta}.$$

Therefore

$$\prod_{i<j} (\sigma(\alpha_i) - \sigma(\alpha_j)) = \prod_{i<j} (\alpha_i - \alpha_j). \qquad (*)$$

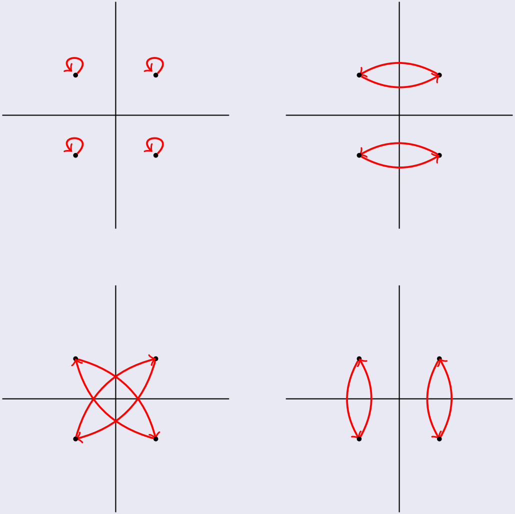
- If σ was a transposition, $(*)$ would not hold.

$S_3 \supset \mathrm{Gal}(x^3 - 3x - 1)$ acting on $\sqrt{\Delta}$

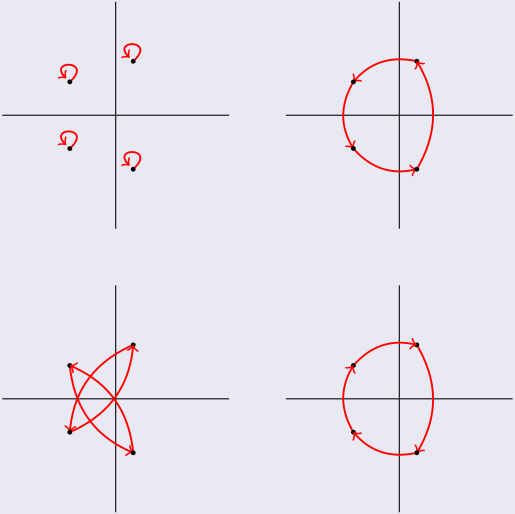


- If $\sqrt{\Delta} \in \mathbb{Z}$ then this is necessarily fixed by every automorphism, so the second mapping is *not* an automorphism.

Example: $\mathrm{Gal}(x^4 + 1)$



Example: $\mathrm{Gal}(x^4 + x^3 + x^2 + x + 1)$



For simplicity...

- We assume that f is irreducible.
- Then f is *separable* (has distinct roots) since f' has smaller degree and is nonzero (as $\mathrm{char}(\mathbb{Q}) = 0$) so $\gcd(f, f') = 1$.
- Then $\mathrm{Gal}(f)$ is *transitive* (for all α_i, α_j there is some $\sigma \in \mathrm{Gal}(f)$ which sends α_i to α_j) since by Thm. 4 there is an embedding of $\mathbb{Q}(\alpha_i)$ in $\mathbb{C}$ with $\alpha_i \mapsto \alpha_j$.
  - Intuitively: $\mathbb{Q}(\alpha_i) \cong \mathbb{Q}(\alpha_j)$
  - But we can't necessarily specify $\alpha_i \mapsto \alpha_j$ and $\alpha_j \mapsto \alpha_k$ *simultaneously*.

In general...

$$\mathrm{Gal}(gh) \subseteq \mathrm{Gal}(g) \times \mathrm{Gal}(h)$$

Furthermore...

- We assume f is monic and has integer coefficients.
- The general case reduces to this by applying transformations of the form (for nonzero $c \in \mathbb{Q}$)

$$f(x) \mapsto cf(x)$$
$$f(x) \mapsto f(cx)$$

  which do not change the splitting field of f.
- If $f(x) \coloneqq \frac{1}{b} \sum_{i=0}^{n} a_i x^i$ for $a_i, b \in \mathbb{Z}$ then we apply

$$f(x) \mapsto b a_n^{n-1} f(x/a_n).$$

Symmetric polynomials

- A polynomial $p \in R[x_1, \ldots, x_n]$ is *symmetric* if

$$p(x_1, \ldots, x_n) = p(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

for all permutations $\sigma \in S_n$.

Example

- The polynomial

$$x_1^2 + \cdots + x_n^2$$

is symmetric in $\mathbb{Q}[x_1, \ldots, x_n]$, but not in $\mathbb{Q}[x_1, \ldots, x_{n+1}]$.

Elementary symmetric polynomials

- The polynomials $s_1, \ldots, s_n \in R[x_1, \ldots, x_n]$ defined by

$$\begin{aligned} s_1 &\coloneqq x_1 + x_2 + \cdots + x_n \\ s_2 &\coloneqq x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\ &\vdots \\ s_n &\coloneqq x_1x_2\cdots x_n \end{aligned}$$

  are known as the *elementary symmetric polynomials*.
- They appear as the coefficients of the *general polynomial of degree n*: $\prod_{i=1}^{n}(x - x_i) = x^n - s_1x^{n-1} + \cdots + (-1)^n s_n$.

The fundamental theorem of symmetric polynomials

- Every symmetric polynomial in $R[x_1, \ldots, x_n]$ can be written as a polynomial in $s_1, \ldots, s_n$ with coefficients in R.

Orbit of a polynomial under S_n

- The *orbit* of $p \in \mathbb{Z}[x_1, \ldots, x_n]$ under S_n is the set of polynomials that p can be sent to by permuting the x_i.
- Measures "how close" a polynomial is to being symmetric.
  - If $\mathrm{orb}(p) = \{p\}$ then p is symmetric.
  - If $|\mathrm{orb}(p)| = n!$ then every permutation of the x_i yields a new polynomial, so p is as far from being symmetric as possible.

Examples

- The orbit of $x_1 + x_2$ is $\{x_1 + x_2\}$ under S_2, but is $\{x_1 + x_2, x_1 + x_3, x_2 + x_3\}$ under S_3.
- The orbit of $x_1 - x_2$ is $\{x_1 - x_2, x_2 - x_1\}$ under S_2 and is $\{x_1 - x_2, x_2 - x_1, x_1 - x_3, x_3 - x_1, x_2 - x_3, x_3 - x_2\}$ under S_3.

The resolvent polynomial

- The *resolvent polynomial* of $p \in \mathbb{Z}[x_1, \ldots, x_n]$ and $f \in \mathbb{Z}[x]$ with roots $\alpha_1, \ldots, \alpha_n$ is

$$R_{p,f}(y) \coloneqq \prod_{p_i \in \mathrm{orb}(p)} (y - p_i(\alpha_1, \ldots, \alpha_n)).$$

- A new polynomial whose roots are combinations (determined by p) of f's roots.

Example

- With $p(x_1, x_2, x_3) \coloneqq x_1 + x_2$ and $f(x) \coloneqq x^3 - 2$ we have

$$\begin{aligned} R_{p,f}(y) &= (y - (\alpha_1 + \alpha_2))(y - (\alpha_1 + \alpha_3))(y - (\alpha_2 + \alpha_3)) \\ &= y^3 + 2 \end{aligned}$$

Example

- With $p(x_1, x_2, x_3, x_4) \coloneqq x_1 + x_2$ we have

$f(x)$	$R_{p,f}(y)$
$x^4 + 1$	$y^6 - 4y^2$
$x^4 + x^3 + x^2 + x + 1$	$y^6 + 3y^5 + 5y^4 + 5y^3 - 2y - 1$

Example

- With $p \coloneqq \prod_{i>j}(x_i - x_j)$ we have $\operatorname{orb}(p) = \{p, -p\}$ and

$$\begin{aligned} R_{p,f}(y) &= \Big(y - \prod_{i>j}(\alpha_i - \alpha_j)\Big)\Big(y + \prod_{i>j}(\alpha_i - \alpha_j)\Big) \\ &= y^2 - \operatorname{disc}(f) \end{aligned}$$

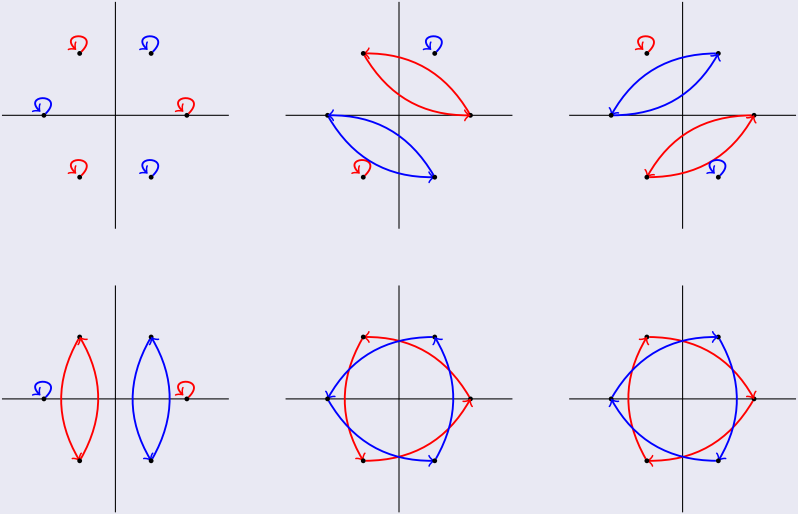
The coefficients of the resolvent polynomial

- By construction, the coefficients of the resolvent polynomial are symmetric polynomials in $\alpha_1, \ldots, \alpha_n$.
- Thus they can be written in terms of the elementary symmetric polynomials in $\alpha_1, \ldots, \alpha_n$.
- The elementary symmetric polynomials in $\alpha_1, \ldots, \alpha_n$ are (up to sign) the coefficients of f.
- Therefore,

  $$R_{p,f}(y) \in \mathbb{Z}[y]$$

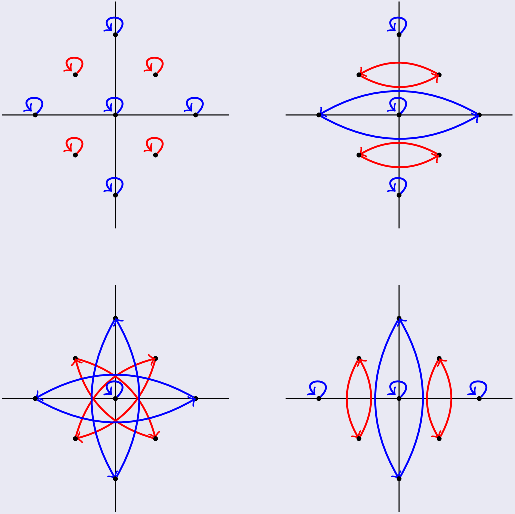
  when $p \in \mathbb{Z}[x_1, \ldots, x_n]$ and $f \in \mathbb{Z}[x]$.
- This also gives a method of computing the resolvent polynomial. (In practice, one can also approximate its roots and calculate it numerically.)

Example: $f := x^3 - 2$, $p := x_1 + x_2$



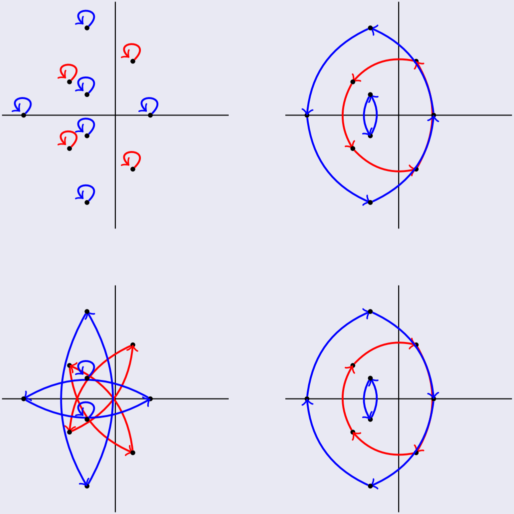
$\sigma \in \mathrm{Gal}(f)$ acts on the zeros of $R_{p,f}(y)$

Example: $f := x^4 + 1$, $p := x_1 + x_2$



$\sigma \in \mathrm{Gal}(f)$ acts on the zeros of $R_{p,f}(y)$

Example: $f := x^4 + x^3 + x^2 + x + 1$, $p := x_1 + x_2$



$\sigma \in \mathrm{Gal}(f)$ acts on the zeros of $R_{p,f}(y)$

Observation

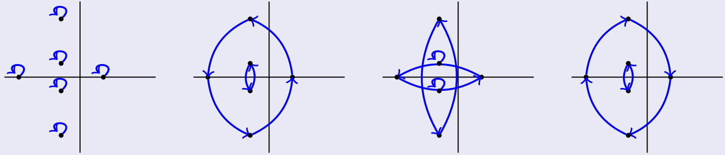
- In each case, the action of $\sigma \in \mathrm{Gal}(f) \subseteq S_n$ on the m roots of $R_{p,f}(y)$ actually gives $\mathrm{Gal}(R_{p,f}) \subseteq S_m$.
- Let $\phi \colon S_n \to S_m$ be defined so that $\phi(\sigma)$ is the action of σ on the roots of $R_{p,f}(y)$.
- If the roots of $R_{p,f}(y)$ are distinct (so ϕ is unambiguous) then
$$\mathrm{Gal}(R_{p,f}) = \phi(\mathrm{Gal}(f)).$$
- Idea: use knowledge of $\mathrm{Gal}(R_{p,f})$ to determine $\mathrm{Gal}(f)$.

Proof idea

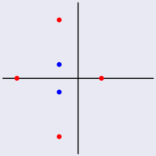
- If σ is an automorphism, $\phi(\sigma)$ is also an automorphism, so $\phi(\mathrm{Gal}(f)) \subseteq \mathrm{Gal}(R_{p,f})$.
- The opposite containment follows from applying ϕ to $\mathrm{Gal}(R_{p,f}) \subseteq \mathrm{Gal}(f)$, since ϕ fixes $\mathrm{Gal}(R_{p,f})$.

'Local' transitivity

- Consider the previous *non-transitive* $\mathrm{Gal}(R_{p,f})$:



- The orbits of $R_{p,f}$'s roots under $\mathrm{Gal}(f)$ form a partition of $R_{p,f}$'s roots into two subsets (of size 4 and 2):



- This can be determined by factoring $R_{p,f}$ into irreducibles.

'Local' transitivity (cont'd)

- This info can be used to limit the possibilities for $\mathrm{Gal}(f)$.
- The roots of $R_{p,f}$ are:

$$\begin{array}{ccc} \alpha_1+\alpha_2 & \alpha_1+\alpha_3 & \alpha_1+\alpha_4 \\ \alpha_2+\alpha_3 & \alpha_2+\alpha_4 & \alpha_3+\alpha_4 \end{array}$$

- Their orbits under the Klein four-group $V_4 \coloneqq \{1,(12)(34),(13)(24),(14)(23)\}$ are:

$$\begin{array}{ccc} {\color{red}\alpha_1+\alpha_2} & {\color{blue}\alpha_1+\alpha_3} & {\color{teal}\alpha_1+\alpha_4} \\ {\color{teal}\alpha_2+\alpha_3} & {\color{blue}\alpha_2+\alpha_4} & {\color{red}\alpha_3+\alpha_4} \end{array}$$

- That is, the *orbit-length partition* of $R_{p,f}$'s roots under V_4 is $\{2,2,2\}$.

Using the orbit-length partition

- The following table gives the orbit-length partitions of $x_1 + x_2$ under the five transitive subgroups of S_4 (up to relabeling indices):

S_4	A_4	D_4	V_4	C_4
$\{6\}$	$\{6\}$	$\{4, 2\}$	$\{2, 2, 2\}$	$\{4, 2\}$

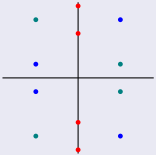
- Thus $\mathrm{Gal}(f)$ is either D_4 or C_4.

Trying a new resolvent polynomial

- With $p \coloneqq x_1 - x_2$ we find that

$$\begin{aligned} R_{p,f}(y) &= y^{12} + 5y^{10} + 15y^8 + 25y^6 - 50y^4 + 125 \\ &= (y^4 + 5y^2 + 5)(y^4 + 5y + 5)(y^4 - 5y + 5) \end{aligned}$$

and we find the orbits of $R_{p,f}$'s roots under $\mathrm{Gal}(f)$ to be:



- Thus the orbit-length partition of $x_1 - x_2$ under $\mathrm{Gal}(f)$ is $\{4, 4, 4\}$.

Using the orbit-length partition

- The following table gives the orbit-length partitions of $x_1 - x_2$ under the five transitive subgroups of S_4 (up to relabeling indices):

S_4	A_4	D_4	V_4	C_4
$\{12\}$	$\{12\}$	$\{8,4\}$	$\{4,4,4\}$	$\{4,4,4\}$

- Thus $\mathrm{Gal}(f)$ is either V_4 or C_4. Comparing with our previous result, we find that $\mathrm{Gal}(f)$ is C_4.

In general

- The orbit-length partition of small linear polynomials under $\mathrm{Gal}(f)$ is often enough to completely distinguish $\mathrm{Gal}(f)$.

A general algorithm

- To determine if $\mathrm{Gal}(f) \subseteq G$ one can select p which is fixed by exactly the permutations in G (i.e., $G = \mathrm{stab}(p)$). For example, one can take

$$p \coloneqq \sum_{\sigma \in G} x_{\sigma(1)} x_{\sigma(2)}^2 x_{\sigma(3)}^3 \cdots x_{\sigma(n)}^n.$$

- $R_{p,f}$ has a linear factor if and only if

$$\mathrm{Gal}(f) \subseteq \mathrm{stab}(p(\alpha_1, \ldots, \alpha_n))$$

  for some ordering of the α_i.

A general algorithm (cont'd)

- Find all transitive subgroups $G \subseteq S_n$ and work your way through the subgroup lattice by testing if $\mathrm{Gal}(f) \subseteq G$ as necessary.
- For example, the subgroup lattice of S_4 is:

$$
\begin{tikzcd}[arrows=-]
 & & S_4 \arrow[dl] \arrow[dr] & \\
 & D_4 \arrow[dl] \arrow[dr] & & A_4 \arrow[dl] \\
C_4 & & V_4 &
\end{tikzcd}
$$