

Galois Theory by Calculator
Thomas W. Mattman
California State University, Chico

(Revised) Abstract:

Using Computer Algebra Systems, students can easily calculate the Galois groups of most rational polynomials up to degree seven. Although there are several techniques available, we will focus on a method which involves factoring resolvent polynomials. To illustrate the method, we investigate the Galois groups of $x^5 - 5x + 12$ and $x^5 + 2$.

These slides are available at
<http://www.csuchico.edu/~tm108/>

Context: $f(x)$ an irreducible polynomial with rational coefficients of degree n less than 7.

We wish to find $G = \text{Gal}(f)$.

Note: If instead, $f = p_1 \cdot p_2$, and

$$\text{Split}(p_1) \cap \text{Split}(p_2) = \mathbb{Q},$$

then

$$\text{Gal}(f) = \text{Gal}(p_1) \oplus \text{Gal}(p_2).$$

However, in general, finding the Galois group of a composite polynomial is difficult.

Since f is irreducible, the Galois group G acts transitively on the roots α_i of f and therefore is a transitive subgroup of S_n .

We can identify G by its orbit-lengths when acting on subsets of roots. For $n \leq 5$, it is enough to look at sets and sequences of two roots.

The Discriminant: Let,

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

Δ^2 is the discriminant of f and

$$G \subset A_n \Leftrightarrow \Delta \in \mathbb{Q}.$$

On the other hand, if $G \not\subset A_n$, there's a $\sigma \in G$ which takes Δ to $-\Delta$, i.e. the action of G on $\{\Delta, -\Delta\}$ has one orbit of length two.

The resolvent polynomial associated to $\{\Delta, -\Delta\}$ is

$$(x - \Delta)(x + \Delta).$$

It factors iff $G \subset A_n$.

Moral: The orbit-length partition is the same as the factorization shape of the associated resolvent.

Example 1: $f(x) = x^5 - 5x + 12$. The discriminant (use the Maple command “discrim”) is $64000000 = 2^{12}5^6$, so $G \subset A_n$.

The two-set resolvent polynomial is

$$\begin{aligned}
 T_2(x) &= (x - \alpha_1\alpha_2)(x - \alpha_1\alpha_3)(x - \alpha_1\alpha_4)(x - \alpha_1\alpha_5)(x - \alpha_2\alpha_3) \times \\
 &\quad (x - \alpha_2\alpha_4)(x - \alpha_2\alpha_5)(x - \alpha_3\alpha_4)(x - \alpha_3\alpha_5)(x - \alpha_4\alpha_5) \\
 &= x^{10} + 5x^8 - 25x^6 - 288x^5 - 125x^4 - 720x^3 + 20736 \\
 &= (x^5 + 5x^4 + 5x^3 - 35x^2 - 120x - 144) \times \\
 &\quad (x^5 - 5x^4 + 25x^3 - 65x^2 + 120x - 144)
 \end{aligned}$$

We see that $G = Z_5$ or $G = D_5$. To distinguish between the two, we use the two sequence resolvent:

$$\begin{aligned}
 Q_2(x) &= (x - (\alpha_1 + 2\alpha_2))(x - (\alpha_1 + 2\alpha_3)) \cdots (x - (\alpha_5 + 2\alpha_4)) \\
 &= x^{20} - 20x^{16} - 936x^{15} + \dots + 3308303536 \\
 &= (x^{10} + 20x^8 + \dots + 16876)(x^{10} - 20x^8 + \dots + 196036)
 \end{aligned}$$

Therefore, $G = D_5$, the dihedral group of order 10.

Example 2: $f(x) = x^5 + 2$

The discriminant is $50000 = 2^4 5^5$, so $G \not\subset A_n$.

The two-set resolvent is $T_2(x) = x^{10} - 8x^5 + 16$.

However, T_2 has repeated roots. Indeed,

$$\gcd(T_2(x), T_2'(x)) = x^5 - 4.$$

To find the true orbit-lengths on two-sets, we need a $T_2(x)$ without repeated roots.

Use the Tschirnhaus transformation $x \rightarrow x + 1$:

$$g(x) = (x + 1)^5 + 2 = x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 3$$

G , the Galois group of f , is the same as the Galois group of g .

Both the two set resolvent and the two sequence resolvent of g are irreducible. So G is either F_{20} or else S_5 .

To distinguish between these two, we consider the action of G on sets of the form $\{\{i, j\}, \{k, l\}\}$. In other words we use the resolvent polynomial

$$\begin{aligned}
 R(x) &= (x - (\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)^2)(x - (\alpha_1 + \alpha_2 - \alpha_3 - \alpha_5)^2) \times \\
 &\quad (x - (\alpha_1 + \alpha_2 - \alpha_4 - \alpha_5)^2)(x - (\alpha_1 + \alpha_3 - \alpha_2 - \alpha_4)^2) \times \\
 &\quad \dots \\
 &\quad (x - (\alpha_2 + \alpha_4 - \alpha_3 - \alpha_5)^2)(x - (\alpha_2 + \alpha_5 - \alpha_3 - \alpha_4)^2) \\
 &= (x^5 - 12500)(x^{10} + 30500x^5 + 50000)
 \end{aligned}$$

Since the resolvent polynomial R is not irreducible, G is not S_n .

Therefore $G = F_{20}$.