Galois group of cubic

Definition 1. If $f(x) \in k[x]$, the *Galois group of* $f(x)$ is the Galois group $\mathrm{Gal}(K/k)$ of a splitting field K of $f(x)$.

Theorem 1. *For $f(x) \in k[x]$, the Galois group of $f(x)$ permutes the set of roots of $f(x)$. Therefore, if the roots of $f(x)$ are $\alpha_1, \ldots, \alpha_n \in K$, the Galois group of $f(x)$ is isomorphic to a subgroup of S_n.*

Proof. $K = k(\alpha_1, \ldots, \alpha_n)$, so any automorphism σ of K fixing k is determined by the image of each α_i. But σ must take each α_i to some α_j (where possibly $i = j$), since σ is a homomorphism of K and thus $f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = 0$. Thus σ permutes the roots of $f(x)$ and is determined by the resulting permutation. □

We now restrict our attention to the case $k = \mathbb{Q}$. If $f(x) \in \mathbb{Q}[x]$ is a cubic, its Galois group is a subgroup of S_3. We can then use the knowledge of the group structure of S_3 to anticipate the possible Galois groups of a cubic polynomial. There are six subgroups of S_3, and the three subgroups of order 2 are conjugate. This leaves four essentially different subgroups of S_3: the trivial group, the group $\langle (1,2) \rangle$ that consists of a single transposition, the group $A_3 = \langle (1,2,3) \rangle$, and the full group S_3. All four of these groups can in fact appear as the Galois group of a cubic.

Let K be a splitting field of $f(x)$ over $\mathbb{Q}$.

If $f(x)$ splits completely in $\mathbb{Q}$, then $K = \mathbb{Q}$ and so the Galois group of $f(x)$ is trivial. So any cubic (in fact, a polynomial of any degree) that factors completely into linear factors in $\mathbb{Q}$ will have trivial Galois group.

If $f(x)$ factors into a linear and an irreducible quadratic term, then $K = \mathbb{Q}(\sqrt{D})$, where D is the discriminant of the quadratic. Hence $[K : \mathbb{Q}] = 2$ and the order of $\mathrm{Gal}(K/\mathbb{Q})$ is 2, so $\mathrm{Gal}(K/\mathbb{Q}) \cong \langle 1, 2 \rangle \cong \mathbb{Z}/2\mathbb{Z}$; the nontrivial element of the Galois group takes each root of the quadratic to its complex conjugate (i.e. it maps $\sqrt{D} \mapsto -\sqrt{D}$). Thus any cubic that has exactly one rational root will have Galois group isomorphic to $\langle 1, 2 \rangle \cong \mathbb{Z}/2\mathbb{Z}$.

The Galois groups A_3 and S_3 arise when considering irreducible cubics. Let $f(x)$ is irreducible with roots r_1, r_2, r_3. Since f is irreducible, the roots are distinct. Thus $\mathrm{Gal}(K/\mathbb{Q})$ has at least 3 elements, since the image of r_1 may be any of the three roots. Since $\mathrm{Gal}(K/\mathbb{Q}) \subset S_3$, it follows that $\mathrm{Gal}(K/\mathbb{Q}) \cong A_3$ or $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$ and thus by the fundamental theorem of Galois theory that $[K : \mathbb{Q}] = 3$ or 6.

Now, the discriminant of f is

$$D = \prod_{i<j} (r_i - r_j)^2$$

This is a symmetric polynomial in the r_i. The coefficients of $f(x)$ are the elementary symmetric polynomials in the r_i: if $f(x) = x^3 + ax^2 + bx + c$, then

$$\begin{aligned} c &= r_1 r_2 r_3 \\ b &= -(r_1 r_2 + r_1 r_3 + r_2 r_3) \\ a &= r_1 + r_2 + r_3 \end{aligned}$$

Thus D can be written as a polynomial in the coefficients of f, so $D \in \mathbb{Q}$. $D \neq 0$ since $f(x)$ is irreducible and therefore has distinct roots; also clearly $\sqrt{D} \in K$ and thus $\mathbb{Q}(r_1, \sqrt{D}) \subset K$. If $f(x) = x^3 + ax^2 + bx + c$, then its discriminant D is $18abc + a^2b^2 - 4b^3 - 4a^3c - 27c^2$ (see the article on the discriminant for a longer discussion).

If $\sqrt{D} \notin \mathbb{Q}$, it follows that $\sqrt{D}$ has degree 2 over $\mathbb{Q}$, so that $[\mathbb{Q}(r_1, \sqrt{D}) : \mathbb{Q}] = 6$. Hence $K = \mathbb{Q}(r_1, \sqrt{D})$, so we can derive the splitting field for f by adjoining any root of f and the square root of the discriminant. This can happen for either positive or negative D, clearly. Note in particular that if $D < 0$, then $\sqrt{D}$ is imaginary and thus K is not a real field, so that f has one real and two imaginary roots. So any cubic with only one real root has Galois group S_3.

If $\sqrt{D} \in \mathbb{Q}$, then any element of $\mathrm{Gal}(K/\mathbb{Q})$ must fix $\sqrt{D}$. But a transposition of two roots does not fix $\sqrt{D}$ - for example, the map

$$r_1 \mapsto r_2, \qquad r_2 \mapsto r_1, \qquad r_3 \mapsto r_3$$

takes

$$\sqrt{D} = (r_1 - r_2)(r_1 - r_3)(r_2 - r_3) \mapsto (r_2 - r_1)(r_2 - r_3)(r_1 - r_3) = -\sqrt{D}$$

Then $\mathrm{Gal}(K/\mathbb{Q})$ does not include transpositions and so it must in this case be isomorphic to A_3. Thus $[K:\mathbb{Q}] = 3$, so $K = \mathbb{Q}(r_1) = \mathbb{Q}(r_1, \sqrt{D})$ since $\sqrt{D} \in \mathbb{Q}$. This proves:

Theorem 2. *Let $f(x) \in \mathbb{Q}[x]$ be an irreducible cubic and K its splitting field. Then if α is any root of f,*

$$K = \mathbb{Q}(\alpha, \sqrt{D})$$

where D is the discriminant of f. Thus if $\sqrt{D}$ is rational, $[K:\mathbb{Q}] = 3$ and the Galois group is isomorphic to A_3, otherwise $[K:\mathbb{Q}] = 6$ and the Galois group is isomorphic to S_3.

Note that one consequence of all of this is that any irreducible cubic with three real roots must have Galois group A_3 (and thus any irreducible cubic with Galois group S_3 must have two complex roots), but the converse does not hold.

One way of looking at the above analysis is that for a "general" polynomial of degree n, the Galois group is S_n. If the Galois group of some polynomial is not S_n, there must be algebraic relations among the roots that restrict the available set of permutations. In the case of a cubic whose discriminant is a rational square, this relation is that $\sqrt{D}$, which is a polynomial in the roots, must be preserved.

Example 1 $f(x) = x^3 - 6x^2 + 11x - 6$. By the rational root test, this polynomial has the three rational roots $1, 2, 3$, so it factors as $f(x) = (x-1)(x-2)(x-3)$ over $\mathbb{Q}$. Its Galois group is therefore trivial.

Example 2 $f(x) = x^3 - x^2 + x - 1$. Again by the rational root test, this polynomial factors as $(x-1)(x^2+1)$, so its Galois group has two elements, and a splitting field K for f is derived by adjoining the square root of the discriminant of the quadratic: $K = \mathbb{Q}(\sqrt{-1})$. The nontrivial element of the Galois group maps $\sqrt{-1} \leftrightarrow -\sqrt{-1}$.

Example 3 $f(x) = x^3 - 2$. This polynomial has discriminant $-108 = -3 \cdot 6^2$. This is not a rational square, so the Galois group of f over $\mathbb{Q}$ is S_3, and the splitting field for f is $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-108}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$. This is in agreement with what we already know, namely that the cube roots of 2 are

$$\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$$

where $\omega = \frac{-1+\sqrt{-3}}{2}$ is a primitive cube root of unity.

Example 4 $f(x) = x^3 - 4x + 2$. This is irreducible since it is Eisenstein at 2 (or by the rational root test), and its discriminant is 202, which is not a rational square. Thus the Galois group for this polynomial is also S_3; note, however, that f has three real roots (since $f(0) > 0$ but $f(1) < 0$).

Example 5 $f(x) = x^3 - 3x + 1$. This is also irreducible by the rational root test. Its discriminant is 81, which is a rational square, so the Galois group for this polynomial is A_3. Explicitly, the roots of $f(x)$ are

$$r_1 = 2\cos(2\pi/9), r_2 = 2\cos(8\pi/9), r_3 = 2\cos(14\pi/9)$$

and we see that

$$\cos(14\pi/9) = \cos(4\pi/9) = 2\cos^2(2\pi/9) - 1$$
$$\cos(8\pi/9) = 2\cos^2(4\pi/9) - 1$$

Let's consider an automorphism of K sending r_1 to r_3, i.e. sending $\cos(2\pi/9) \mapsto \cos(14\pi/9)$. Given the relations above, it is clear that this mapping uniquely determines the image of r_3 as well, since

$$r_3 = 2\cos^2(2\pi/9) - 1 \mapsto 2\cos^2(4\pi/9) - 1 = r_2$$

and thus we see how the relation imposed by the discriminant actually manifests itself in terms of restrictions on the permutation group.