§ 11 The discriminant

Note that the group S_n contains a normal subgroup of index 2, namely A_n, the group of even permutations. Let's compute the extension of K corresponding to this subgroup.

Suppose that a degree n polynomial $f(x)$ splits as $\prod_{i=1}^{n}(x-\alpha_i)$ in its splitting field. Suppose all α_i are distinct (true if f is irreducible). The group S_n acts by permuting the roots (and $\mathrm{Gal}(f/K)$ is a subgroup of S_n).

We define $\Delta(f)=\prod_{i>j}(\alpha_i-\alpha_j)$.

Lemma 11.1 Suppose $\theta \in \mathrm{Gal}(f/K) \subseteq S_n$. Then

$$\theta(\Delta(f)) = \begin{cases} \Delta(f) & \text{if } \theta \text{ is an even permutation} \\ -\Delta(f) & \text{if } \theta \text{ is an odd permutation} \end{cases}$$

Proof. This is an equivalent definition of even/odd. ⊠

Define the *discriminant*, $D(f)$, to be $\Delta(f)^2$. Then note that $\theta(D(f)) = D(f)$ for all $\theta \in \mathrm{Gal}(f/K)$ by the lemma. It follows that $D(f)$ lies in K, as it is fixed by every element of the Galois group (using Theorem 12.3).

Corollary 11.2 Let $f \in K[x]$ have only simple roots, and let L denote a splitting field. Regard $G = \mathrm{Gal}(f/K)$ as a subgroup of S_n. Then the subfield of L corresponding to the subgroup $G \cap A_n$ is $K[\Delta(f)]$. In particular,

$$G \subseteq A_n \iff \Delta(f) \in K \iff D(f) \text{ is a square in } K.$$

Proof. As f has distinct roots, $\Delta(f) \neq 0$, and so the lemma shows that $\theta(\Delta(f)) = \Delta(f)$ if and only if $\theta \in A_n$. Thus $G \cap A_n$ is the subgroup of G corresponding to $K[\Delta(f)]$, and so

$$G \subseteq A_n \iff K[\Delta(f)] = K \iff \Delta(f) \in K.$$

⊠

Thus the Galois group $\mathrm{Gal}(f/K)$ of a polynomial f of degree d is contained in A_d, not just S_d, if and only if its discriminant is a square in K.

Corollary 11.3 Suppose $f \in K[x]$ is an irreducible cubic equation. Then

$$\mathrm{Gal}(f/K) = \begin{cases} A_3 & \text{if } D(f) \text{ is a square} \\ S_3 & \text{if not} \end{cases}$$

Proof. Let α be a root of f. As f is irreducible, it is the minimal polynomial of α. By Theorem 2.2, $[K(\alpha):K]=3$. But if L is the splitting field of f, $L \supseteq K(\alpha)$, so we conclude that $3|[L:K]$ by Theorem 2.3. Also, L/K is Galois (it's a splitting field), so $|\mathrm{Gal}(L/K)| = [L:K]$. Finally, the Galois group may be regarded as a subgroup of S_3, a group of order 6. It follows that $\mathrm{Gal}(f/K)$ is either all of S_3, or it is a subgroup of order 3 – the only such subgroup is $A_3 = \langle(1\ 2\ 3)\rangle$. By Corollary 11.2, the Galois group is A_3 precisely when $D(f)$ is a square, and is S_3 if not. $\boxtimes$

By an Exercise, the cubic $f(x) = x^3 + ax + b$ has $D(f) = -(4a^3 + 27b^2)$.

Remark 11.4 An explicit computation (or use Maple!) shows that a quartic has the same discriminant as its resolvent cubic.

Remark 11.5 We can now classify Galois groups of irreducible quartics. As the quartic is irreducible, then its Galois group is a transitive subgroup of S_4. These subgroups are known; there are 5 possibilities, namely, S_4, A_4, D_4, V_4 and C_4.

We also know that if its discriminant is a square, then its Galois group is a transitive subgroup of A_4 and must therefore be either A_4 or V_4 (the other groups all contain 4-cycles, so cannot be contained in A_4). Otherwise, its Galois group is not contained in A_4, so is one of S_4, D_4 or C_4.

Also, if its resolvent cubic is irreducible, adjoining the roots of the resolvent cubic leads to an extension of degree divisible by 3. This was the first step in constructing the splitting field of the quartic. It follows that the Galois group of the quartic must be of order divisible by 3, so must be one of S_4 or A_4. Otherwise the Galois group will be one of D_4, V_4 or C_4.

We therefore have the following classification:

$D(f)$ square?	res. cubic irred.?	Galois group
Yes	Yes	A_4
No	Yes	S_4
Yes	No	V_4
No	No	D_4 or C_4

In fact, we can distinguish between these latter two possibilities – the Galois group is D_4 if the quartic remains irreducible over the splitting field of the cubic, and is C_4 if not. In general, however, it is usually easier to compute these by hand.

We have seen examples of all of these occurring earlier in the course, or on example sheets, for polynomials over $\mathbb{Q}$. In Exercise 25, we saw that $x^4 + 8x + 12$ has irreducible resolvent cubic, but its discriminant is 576^2. Thus its Galois group is A_4. However, $x^4 + 8x - 12$ has irreducible resolvent cubic and discriminant which is not a square, so its Galois group is S_4. We have just seen that $x^4 - 10x^2 + 1$ has splitting field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, so has Galois group V_4. Another example is provided by $x^4 + 1$, which is the cyclotomic polynomial λ_8 – recall that the Galois group of λ_n over $\mathbb{Q}$ was $U(\mathbb{Z}_n)$. We see that $U(\mathbb{Z}_8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ and that this is a group isomorphic to V_4. In §6, we found that the Galois group of $x^4 - 2$ was D_4.

Finally, the fifth cyclotomic polynomial $\lambda_5 = x^4 + x^3 + x^2 + x + 1$ has Galois group $U(\mathbb{Z}_5) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, which is cyclic of order 4.

Thus all five possible transitive subgroups of S_4 can occur as Galois groups of polynomials over $\mathbb{Q}$. More generally, it is conjectured that any finite group may be realised as the Galois group of some polynomial over $\mathbb{Q}$. This question is known as the "Inverse Galois Problem", and is the subject of much current research.