Galois Theory - Finding Galois Groups

Abigail Tan
March 25, 2023

Some of these notes are based on Keith Conrad's blurbs.
We write G for $\mathrm{Gal}(f/K)$. The main basic results that will be used are as follows:

Proposition 1. The polynomial $f \in K[X]$ is irreducible if and only if $\mathrm{Gal}(f/K)$ is transitive.
Proof. Let $x \in L$ (a splitting field for f) be a root of f. Then $\mathrm{Orb}_{\mathrm{Gal}(f/K)}(x)$ is the set of roots of $m_{x,K}$. Then $m_{x,K} = f$ iff f is irreducible, since $m_{x,K}|f$. But $m_{x,K} = f$ iff every root of f is in the orbit of x, i.e. $\mathrm{Gal}(f,K)$ acts transitively on roots of f. $\square$

Remark. If $G \subset S_n$ is transitive, then n divides $|G|$. (This holds because of orbit-stabiliser). Additionally, $\mathrm{Disc}(f) \neq 0$ if and only if f is separable.

Proposition 2. If $\mathrm{char}\, K \neq 2$, then the fixed field of $G \cap A_n$ is $K(\Delta)$ (where $\mathrm{Disc}(f) = \Delta^2$), and $\mathrm{Gal}(f/K) \subset A_n$ if and only if $\mathrm{Disc}(f)$ is a square in K.
Proof. Let $\pi \in S_n$, then $\prod_{1\leq i<j\leq n}(T_{\pi(i)} - T_{\pi(j)}) = \mathrm{sgn}(\pi)\prod_{1\leq i<j\leq n}(T_i - T_j)$ so for $\sigma \in G$, $\sigma(\Delta) = \mathrm{sgn}(\sigma)\Delta$. Since $\Delta \neq 0$, this implies $\Delta \in K \iff G \subset A_n$ and Δ lies in $L^{G\cap A_n}$. Since $[L^{G\cap A_n} : K] = (G : G\cap A_n) = 1$ if $G \subset A_n$ and 2 otherwise, we have $L^{G\cap A_n} = K(\Delta)$. $\square$

The following result finds the Galois group of an irreducible cubic.

Theorem 3. Let $\mathrm{char}\, K \neq 2$. Let $f \in K[X]$ be a separable, irreducible cubic. Then

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

Proof. The Galois group G is transitive since f is irreducible. The only transitive subgroups of S_3 are S_3 and A_3, and G is contained in A_3 iff $\mathrm{Disc}(f)$ is a square in K, by Prop. 2. $\square$

Definition 4 (Resolvent cubic). Let $f(X) = X^4 + aX^3 + bX^2 + cX + d$. Then the resolvent cubic of f, $R_3(X)$, is defined as $R_3(X) = X^3 - bX^2 + (ac - 4d)X - (a^2d + c^2 - 4bd)$.

Remark. These are derived from taking $f(X) = (X - r_1)(X - r_2)(X - r_3)(X - r_4)$ and finding $R_3(X) := (X - (r_1r_2 + r_3r_4))(X - (r_1r_3 + r_2r_4))(X - (r_1r_4 + r_2r_3))$.

Theorem 5. The Galois groups of monic irreducible quartics f can be classified as follows.

$\mathrm{Disc}(f)$	resolvent cubic $R_3(X)$	$\mathrm{Gal}(f/K)$
not square	irred.	S_4
square	irred.	A_4
not square	red.	D_8 or C_4
square	red.	V

Some additional results can distinguish between D_8 and C_4 in certain cases.

Proposition 6. Let $f \in \mathbb{Q}[X]$ be an irreducible quartic. If $G = C_4$, then $\mathrm{Disc}(f) > 0$. (Hence, if $\mathrm{Disc}(f) < 0$ is not a square and $R_3(X)$ is reducible, then $G = D_8$, by Theorem 5).
Proof. If $G = C_4$, then the splitting field for f over $\mathbb{Q}$ has degree 4. Any root of f generates an extension of degree 4, so a field generated by one root contains all the other roots. Therefore f has either 0 or 4 real roots. The result follows from writing roots as complex conjugate pairs. □

Rather than quoting Theorem 5, the following example uses the ideas that are used in proving that theorem directly.

Example 7. Find the Galois group of $f(X) = X^4 - X - 1$ over $\mathbb{Q}$.
Solution. Note f is irreducible mod 2, so is irreducible over $\mathbb{Q}$. We find $R_3(X) = X^3 + 4X - 1$ is also irreducible over $\mathbb{Q}$ (by the rational root theorem, the fact that neither of ± 1 are roots is a sufficient condition), so the splitting field L of f over $\mathbb{Q}$ contains a cubic subfield $\mathbb{Q}(r_1 r_2 + r_3 r_4)$. By correspondence, the order of $\mathrm{Gal}(f/\mathbb{Q})$ is a multiple of 3. Also, since L is a splitting field for f, we have $\mathbb{Q}(r_1) \subset L$ and $[\mathbb{Q}(r_1) : \mathbb{Q}] = 4$ so $|\mathrm{Gal}(f/K)|$ is also a multiple of 4.
We've shown $|\mathrm{Gal}(f/K)|$ is a multiple of 12 so it is A_4 or S_4, but f has discriminant -283, a non-square, so the Galois group is not in A_4, so is S_4.

Theorem 8 (Full classification of Galois groups for irreducible quartics). Let char $K \neq 2$ and $f \in K[X]$ be an irreducible quartic. Then $G = \mathrm{Gal}(f/K)$ is as follows.

$\mathrm{Disc}(f)$ in K	$R_3(X)$ in $K[X]$	$(a^2 - 4(b - r'))\mathrm{Disc}(f)$ and $(r'^2 - 4d)\mathrm{Disc}(f)$	G
not square	irred.		S_4
square	irred.		A_4
not square	root $r' \in K$	at least one is not square in K	D_8
not square	root $r' \in K$	both square in K	C_4
square	red.		V