I.K. Discriminants, cubics, and quartics

We now embark on the systematic computation of Galois groups for specific polynomials, starting with low degree. Suppose that $\mathrm{char}(K) \neq 2$, and let $f \in K[x]$ be monic of degree n, with splitting field L and Galois group $G := \mathrm{Gal}_K(f) := \mathrm{Aut}(L/K)$. Let $\alpha_1, \ldots, \alpha_n$ denote the roots $\mathcal{R}_f \subset L$ (with possible repetitions), and recall from I.G.17 that G acts transitively on $\mathcal{R}_f \iff f$ is irreducible.

I.K.1. DEFINITION. The **discriminant** of f is $\Delta := \delta^2$, where

$$\delta := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j) \quad \in \quad L$$

Note that δ depends on a choice of ordering of the α_i, but Δ does not.

If f is separable, then the α_i are distinct, L/K is Galois, and Δ is G-invariant (since G just permutes the roots). Otherwise, there is a repeated root and Δ is obviously 0. So we see that

$$\Delta \in K \tag{I.K.2}$$

always holds. In fact, there are formulas (for any n) for Δ in terms of (polynomials in) the coefficients of f. So computationally speaking, Δ actually precedes δ; and for this reason I will sometimes write $\sqrt{\Delta}$ instead of δ.

I.K.3. THEOREM. (i) $\Delta = 0 \implies$ *f has a repeated root in L.*
(ii) $\Delta \neq 0$ *and* $\sqrt{\Delta} \in K \implies G \leq \mathfrak{A}_n$.
(iii) $\Delta \neq 0$ *and* $\sqrt{\Delta} \notin K \implies G \not\leq \mathfrak{A}_n$ *and* $K(\delta) = \mathrm{Inv}(G \cap \mathfrak{A}_n)$.

PROOF. If $\Delta \neq 0$, then f is separable and L/K Galois. Consider $\sigma \in G \leq \mathfrak{S}_n$ as a permutation of the roots: by (slight) abuse of notation, $\sigma(\alpha_i) = \alpha_{\sigma(i)}$. Since the number of inversions[35] in a permutation has the same parity as the number of transpositions,

$$\sigma(\delta) = \textstyle\prod_{i<j}(\alpha_{\sigma(i)} - \alpha_{\sigma(j)}) = \mathrm{sgn}(\sigma)\delta. \tag{I.K.4}$$

[35]These are pairs (i, j) for which $i < j$ but $\sigma(i) > \sigma(j)$. To see the equality mod 2, note that each transposition changes the number of inversions by an odd number.

If $\delta \in K(= \mathrm{Inv}(G))$, then δ is G-invariant and (I.K.4) forces $G \leq \ker(\mathrm{sgn}) = \mathfrak{A}_n$.

On the other hand, if $\delta \notin K$, then it isn't G-invariant and (again by (I.K.4)) some $\sigma \in G$ has $\mathrm{sgn}(\sigma) = -1$. By (I.K.2), $m_\delta = x^2 - \Delta$ and $[K(\delta){:}K] = 2$. Applying the FTGT to $[G{:}G \cap \mathfrak{A}_n] = 2$ yields $[\mathrm{Inv}(G \cap \mathfrak{A}_n){:}K] = 2$; since $\delta \in \mathrm{Inv}(G \cap \mathfrak{A}_n)$ ((I.K.4) again), we get $K(\delta) = \mathrm{Inv}(G \cap \mathfrak{A}_n)$. $\square$

Clearly it would be useful to be able to compute Δ. Consider the $n \times n$ Vandermonde matrix $M = (\alpha_j^{i-1})_{i,j,=1,\ldots,n}$. This clearly has $\det(M) = \delta$; and so

$$\text{(I.K.5)} \qquad \Delta = \det(M^t M) = \det((\lambda_{i+j-2})_{i,j,=1,\ldots,n}), \quad \lambda_k := \textstyle\sum_{\ell=1}^n \alpha_\ell^k,$$

where the λ_k are the Newton symmetric polynomials $s_k(\underline{\alpha})$ in the roots. Recalling that these may be expressed in terms of the elementary symmetric polynomials $e_k(\underline{\alpha})$, which (up to $(-1)^k$) are just the coefficients of f, we see a route to general formulas.

I.K.6. EXAMPLE. Let's start with quadratics: $f(x) = x^2 + a_1 x + a_0 = (x - \alpha_1)(x - \alpha_2)$. Then $\lambda_1 = \alpha_1 + \alpha_2 = -a_1$ and $\lambda_2 = \alpha_1^2 + \alpha_2^2 = (\alpha_1 + \alpha_2)^2 - 2\alpha_1\alpha_2 = a_1^2 - 2a_0$. The resulting discriminant

$$\Delta = \begin{vmatrix} 2 & -a_1 \\ -a_1 & a_1^2 - 2a_0 \end{vmatrix} = 2a_1^2 - 4a_0 - a_1^2 = a_1^2 - 4a_0$$

should look pretty familiar.

Cubics.

Turning to $f(x) = x^3 + a_2 x^2 + a_1 x + a_0$, the linear substitution $x = y - \frac{1}{3}a_2$ yields

$$g(y) = y^3 - py - q, \text{ with } p = \tfrac{1}{3}a_2^2 - a_1 \text{ and } q = \tfrac{1}{3}a_1 a_2 - \tfrac{2}{27}a_2^3 - a_0.$$

Since this merely translates all roots by $\frac{a_2}{3}$, it doesn't affect the discriminant, the splitting field, or the Galois group, but greatly simplifies the computation.

Now write λ_k and e_k for the (Newton and elementary) symmetric polynomials in the roots α_i of g; we have $e_1 = \alpha_1 + \alpha_2 + \alpha_3 = 0$,

$e_2 = -p$ and $e_3 = q$. By Newton's identities we have

$$\begin{aligned}
\lambda_1 &= e_1 = 0, \\
\lambda_2 &= e_1^2 - 2e_2 = 2p, \\
\lambda_3 &= e_1^3 - 3e_1e_2 + 3e_3 = 3q, \text{ and} \\
\lambda_4 &= e_1^4 - 4e_1^2e_2 + 4e_1e_3 + 2e_2^2 = 2p^2,
\end{aligned}$$

which yield the discriminant

$$\Delta = \begin{vmatrix} 3 & 0 & 2p \\ 0 & 2p & 3q \\ 2p & 3q & 2p^2 \end{vmatrix} = 4p^3 - 27q^2. \tag{I.K.7}$$

Assuming that $\mathrm{char}(K) \neq 2, 3$, f is separable (cf. (I.E.6)); and assuming f irreducible, $\Delta \neq 0$. Moreover, G acts transitively, so is either $\mathfrak{A}_3 \cong \mathbb{Z}_3$ or $\mathfrak{S}_3$. By Theorem I.K.3, we have

$$G \cong \mathbb{Z}_3 \iff (\delta =)\, \sqrt{\Delta} \in K; \tag{I.K.8}$$

and in either case, $[L{:}K(\delta)] = 3$ and $\mathrm{Aut}(L/K(\delta)) \cong \mathbb{Z}_3$.

To enclose L/K in a root tower, first adjoin a cube root of unity ζ to K, followed by δ; note that $L(\zeta)/K$ is a SFE (for $(x^3-1)g(x)$) hence Galois. The tower of extensions $K \subset K(\delta) \subset L \subset L(\zeta)$ evidently has total degree 3, 6, or 12; this forces $L(\zeta)/K(\delta,\zeta)$ to be of order 3 hence cyclic (with generator σ). By I.J.19, $L(\zeta) = K(\delta,\zeta,\theta)$ where $\theta^3 \in K(\delta,\zeta)$; and so our root tower is

$$K \subset K(\zeta) \subset K(\zeta,\delta) \subset K(\zeta,\delta,\theta) = L(\zeta).$$

In fact, the proof of I.J.19 gives a formula for the cube root: we must take $\theta = \theta_+ := \alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3$, since then applying σ sends $\alpha_1 \mapsto \alpha_2 \mapsto \alpha_3 \mapsto \alpha_1 \implies \theta_+ \mapsto \zeta^2\theta_+ \implies \theta_+^3 \mapsto \theta_+^3 \implies \theta_+^3 \in K(\zeta,\delta)$. Writing $\theta_- := \alpha_1 + \zeta^2\alpha_2 + \zeta\alpha_3$, we evidently have $\sigma(\theta_-) = \zeta\theta_-$, and so $\theta_-^3, \theta_+\theta_- \in K(\zeta,\delta)$ as well.

We can use this to compute the roots α_i of g. First observe that

$$\theta_+\theta_- = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + (\zeta+\zeta^2)(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = \lambda_2 - e_2 = 3p,$$

while

$$\theta_+^3 + \theta_-^3 = (\alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3)^3 + (\alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3)^3 + (\underbrace{\alpha_1 + \alpha_2 + \alpha_3}_{0})^3$$
$$= 3(\alpha_1^3 + \alpha_2^3 + \alpha_3^3) + 18\alpha_1\alpha_2\alpha_3$$
$$= 3\lambda_3 + 18e_3 = 9q + 18q = 27q.$$

Therefore

$$(y - \theta_+^3)(y - \theta_-^3) = y^2 - (\theta_+^3 + \theta_-^3)y + (\theta_+\theta_-)^3 = y^2 - 27qy + 27p^3,$$

which by (I.K.7) and the quadratic formula yields

$$\theta_\pm^3 = \tfrac{27}{2}q \pm \tfrac{3}{2}\sqrt{-3\Delta} = \tfrac{27}{2}q \pm \tfrac{3}{2}(2\zeta + 1)\delta. \tag{I.K.9}$$

Finally, solving the linear system

$$\begin{cases} \alpha_1 + \alpha_2 + \alpha_3 &= 0 \\ \alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3 &= \theta_+ \\ \alpha_1 + \zeta^2\alpha_2 + \zeta\alpha_3 &= \theta_- \end{cases}$$

for the roots gives (up to reordering)

(I.K.10)

$$\alpha_1 = \tfrac{1}{3}(\theta_+ + \theta_-), \quad \alpha_2 = \tfrac{1}{3}(\zeta^2\theta_+ + \zeta\theta_-), \quad \alpha_3 = \tfrac{1}{3}(\zeta\theta_+ + \zeta^2\theta_-),$$

which together with (I.K.9) and (I.K.7) constitute *Cardano's formulas*, published in 1545. In fact, Cardano's book also contained a method for solving quartics by radicals.

Quartics. Continuing to assume $\mathrm{char}(K) \neq 2, 3$, consider $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, and again make a linear substitution $x = y - \frac{a_3}{4}$ to replace this by $g(y) = y^4 + py^2 + qy + r$. Assuming f irreducible ($\implies \Delta \neq 0$), we know that $G := \mathrm{Gal}_K(f)$ is a transitive subgroup of $\mathfrak{S}_4$, hence limited to the possibilities $\mathfrak{S}_4$, $\mathfrak{A}_4$, D_4, V_4, and $\mathbb{Z}_4$. We see right away from Theorem I.K.3 that

- if $\delta \in K$, then $G \cong \mathfrak{A}_4$ or V_4, while
- if $\delta \notin K$, then $G \cong \mathfrak{S}_4$, D_4 or $\mathbb{Z}_4$.

To go further, we need to consider the cubic resolvent of g and *its* splitting field, starting with the latter.

Recall that $V_4 = \{\mathbf{1}, (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup of $\mathfrak{S}_4$, so that $H := V_4 \cap G \trianglelefteq G$. (In fact $H = V_4$ unless $G = \langle (1234) \rangle \cong \mathbb{Z}_4$, in which case $H = \mathbb{Z}_2$.) Inside our splitting field L for g, consider then $M := \mathrm{Inv}(H)$, with $\mathrm{Aut}(L/M) \cong H \leq V_4$ and

$$\mathrm{Aut}(M/K) \cong G/H \cong G/(G \cap V_4) \cong GV_4/V_4 \leq \mathfrak{S}_4/V_4 \cong \mathfrak{S}_3,$$

which certainly suggests that M/K should be the SFE of a cubic polynomial.

To determine M, write $g(y) = \prod_{i=1}^4 (y - \alpha_i)$, with $\sum_i \alpha_i = 0$. Taking $\beta_{ij} := \alpha_i + \alpha_j$, their squares

$$\beta_{12}^2 = -\beta_{12}\beta_{34}, \;\; \beta_{13}^2 = -\beta_{13}\beta_{24}, \;\; \text{and} \;\; \beta_{14}^2 = -\beta_{14}\beta_{23}$$

are evidently fixed by V_4, and so belong to M. Conversely, if σ is a permutation of roots fixing these squares, then $\sigma \in V_4$. So

$$\mathrm{Aut}(L/M) \leq \mathrm{Aut}(L/K(\beta_{12}^2, \beta_{13}^2, \beta_{14}^2)) \leq H = \mathrm{Aut}(L/M)$$

forces both $\leq$'s to be $=$'s, and $M = K(\beta_{12}^2, \beta_{13}^2, \beta_{14}^2)$.

One then computes

$$\begin{cases} \beta_{12}^2 + \beta_{13}^2 + \beta_{14}^2 = -2\sum_{i<j} \alpha_i\alpha_j = -2p, \\ \beta_{12}^2\beta_{13}^2 + \beta_{12}^2\beta_{14}^2 + \beta_{13}^2\beta_{14}^2 = p^2 - 4r, \\ \beta_{12}\beta_{13}\beta_{14} = -q \;\; (\implies \;\; \beta_{12}^2\beta_{13}^2\beta_{14}^2 = q^2), \end{cases}$$

which obviously belong to K, making M the splitting field of the **cubic resolvent**

(I.K.11) $$F(z) := z^3 + 2pz^2 + (p^2 - 4r)z - q^2 \; \in \; K[x]$$

of g. By Cardano's formula, we can construct the roots $\beta_{12}^2, \beta_{13}^2, \beta_{14}^2$ of F by taking square and cube roots. Then we obtain $\beta_{12}, \beta_{13}, \beta_{14}$ by taking further square roots (signs compatible with $\beta_{12}\beta_{13}\beta_{14} = -q$). Adjoining these to M yields L, since we now obtain the roots

$$\begin{cases} \alpha_1 = \frac{1}{2}(\beta_{12} + \beta_{13} + \beta_{14}), & \alpha_2 = \frac{1}{2}(\beta_{12} - \beta_{13} - \beta_{14}), \\ \alpha_3 = \frac{1}{2}(-\beta_{12} + \beta_{13} - \beta_{14}), & \alpha_4 = \frac{1}{2}(-\beta_{12} - \beta_{13} + \beta_{14}) \end{cases}$$

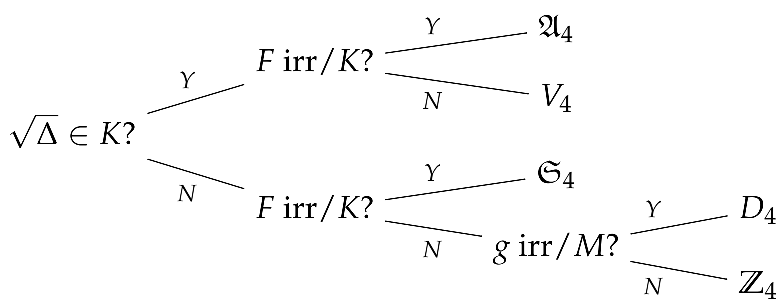
of g by "solving the linear system" as before. Incorporating the cube root of unity ζ, we therefore have the desired root tower: adjoin ζ to K, then the square root of the discriminant of (I.K.11), then the cubic radical θ for (I.K.11), which gets us to $M(\zeta)$; finally, adjoining the square roots β_{1j} of elements of $M(\zeta)$ gets us to $L(\zeta)$.

Going back to the possibilities for the Galois group G of g (and f), we have the following table[36]

G	G/H	H	g irr$/M$?	F irr$/K$?	$\sqrt{\Delta} \in K$?	SFEs of F & g
$\mathfrak{S}_4$	$\mathfrak{S}_3$	V_4	Y	Y	N	$K \overset{6}{—} M \overset{4}{—} L$
$\mathfrak{A}_4$	$\mathbb{Z}_3$	V_4	Y	Y	Y	$K \overset{3}{—} M \overset{4}{—} L$
D_4	$\mathbb{Z}_2$	V_4	Y	N	N	$K \overset{2}{—} M \overset{4}{—} L$
V_4	$\{1\}$	V_4	Y	N	Y	$K \overset{1}{=} M \overset{4}{—} L$
$\mathbb{Z}_4$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	N	N	N	$K \overset{2}{—} M \overset{2}{—} L$

which leads for instance to the decision diagram

(I.K.12)



However, one can often avoid computing Δ by finding the roots of the resolvent and/or g and making use of the right-hand column of the table instead.

I.K.13. EXAMPLE. Consider $f(x) = x^4 + 4x + 2\,(= g(x))$ over $K = \mathbb{Q}$. This is irreducible by Eisenstein. Computing $\Delta = 256r^3 - 27q^4 = 16^2(2^3 - 3^3)$, we find that $\sqrt{\Delta} \notin \mathbb{Q}$. The resolvent is $F(z) =$

[36] In order to make effective use of this, we need to know the discriminant. One can show that Δ is given by $256r^3 - 128p^2r^2 + 144pq^2r - 27q^4 + 16p^4r - 4p^3q^2$. The standard method (for any monic polynomial) is to compute the resultant of g and g', which is a (in this case 7×7) determinant constructed from coefficients of the two polynomials.

$z^3 - 8z - 16$, which is "equivalent" to $\frac{1}{8}F(2z) = z^3 - 2z - 2$, hence irreducible (again by Eisenstein). So the Galois group is $\mathfrak{S}_4$.

For practice, you might try to find G for $x^4 - 2x - 1$, $x^4 + 4x^2 + 2$, and $x^4 - 10x^2 + 4$.