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 \( \text{char}(K) \neq 2 \), and let \( f \in K[x] \) be monic of degree \( n \), with splitting field \( L \) and Galois group \( G := \text{Gal}_K(f) := \text{Aut}(L/K) \). Let \( \alpha_1, \ldots, \alpha_n \) denote the roots \( R_f \subset L \) (with possible repetitions), and recall from I.G.17 that \( G \) acts transitively on \( R_f \iff f \) is irreducible.

I.K.1. Definition. The \textbf{discriminant} of \( f \) is \( \Delta := \delta^2 \), where

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

Note that \( \delta \) depends on a choice of ordering of the \( \alpha_i \), but \( \Delta \) does not.

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

(I.K.2) \( \Delta \in K \)

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

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 \( K(\delta) = \text{Inv}(G \cap \mathfrak{A}_n) \).

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,

(I.K.4) \( \sigma(\delta) = \prod_{i<j}(\alpha_{\sigma(i)} - \alpha_{\sigma(j)}) = \text{sgn}(\sigma)\delta. \)

\(^{35}\)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 $\delta \in K = \text{Inv}(G)$, then $\delta$ is $G$-invariant and (I.K.4) forces $G \leq \ker(\text{sgn}) = \mathfrak{A}_n$.

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 $\text{sgn}(\sigma) = -1$. 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 $[\text{Inv}(G \cap \mathfrak{A}_n):K] = 2$; since $\delta \in \text{Inv}(G \cap \mathfrak{A}_n)$ (I.K.4) again), we get $K(\delta) = \text{Inv}(G \cap \mathfrak{A}_n)$. □

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

\[(I.K.5) \quad \Delta = \det(M^tM) = \det((\lambda_{i+j-2})_{i,j=1,...,n}), \quad \lambda_k := \sum_{\ell=1}^n \alpha^k_\ell,
\]

where the $\lambda_k$ are the Newton symmetric polynomials $s_k(\alpha)$ in the roots. Recalling that these may be expressed in terms of the elementary symmetric polynomials $e_k(\alpha)$, 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: $f(x) = x^2 + a_1x + a_0 = (x - \alpha_1)(x - \alpha_2)$. 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 $f(x) = x^3 + a_2x^2 + a_1x + a_0$, the linear substitution $x = y - \frac{1}{3}a_2$ yields

$$
g(y) = y^3 - py - q, \quad \text{with } p = \frac{1}{3}a_2^2 - a_1 \quad \text{and } q = \frac{1}{3}a_1a_2 - \frac{2}{27}a_2^3 - a_0.
$$

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 $\lambda_k$ and $e_k$ for the (Newton and elementary) symmetric polynomials in the roots $\alpha_i$ 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

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

which yield the discriminant

$$\begin{vmatrix}
3 & 0 & 2p \\
0 & 2p & 3q \\
2p & 3q & 2p^2
\end{vmatrix} = 4p^3 - 27q^2.$$  

Assuming that 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 $A_3 \cong \mathbb{Z}_3$ or $S_3$. By Theorem I.K.3, we have

$$G \cong \mathbb{Z}_3 \iff (\delta =) \sqrt{\Delta} \in K;$$

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

To enclose $L/K$ in a root tower, first adjoin a cube root of unity $\zeta$ to $K$, followed by $\delta$; 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 $\sigma$). By I.J.19, $L(\zeta) = K(\delta, \zeta, \theta)$ where $\theta^3 \in K(\delta, \zeta)$; and so our root tower is

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

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 $\sigma$ sends $\alpha_1 \mapsto \alpha_2 \mapsto \alpha_3 \mapsto \alpha_1 \mapsto \theta_+ \mapsto \zeta^2\theta_+ \mapsto \theta^3_+ \mapsto \theta_+ \in K(\zeta, \delta)$. Writing $\theta_- := \alpha_1 + \zeta^2\alpha_2 + \zeta\alpha_3$, we evidently have $\sigma(\theta_-) = \zeta\theta_-$, and so $\theta_+\theta_- \in K(\zeta, \delta)$ as well.

We can use this to compute the roots $\alpha_i$ 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
\[ \theta^3_+ + \theta^3_- = (a_1 + \zeta a_2 + \zeta^2 a_3)^3 + (a_1 + \zeta a_2 + \zeta^2 a_3)^3 + (a_1 + a_2 + a_3)^3 \]
\[ = 3(a_1^3 + a_2^3 + a_3^3) + 18a_1a_2a_3 \]
\[ = 3\lambda_3 + 18e_3 = 9q + 18q = 27q. \]

Therefore
\[ (y - \theta^3_+)(y - \theta^3_-) = y^2 - (\theta^3_+ + \theta^3_-)y + (\theta^3_+ \theta^-)^3 = y^2 - 27qy + 27p^3, \]
which by (I.K.7) and the quadratic formula yields
\[ (\text{I.K.9}) \quad \theta^3_\pm = \frac{27}{2}q \pm \frac{3}{2}\sqrt{-3\Delta} = \frac{27}{2}q \pm \frac{3}{2}(2\zeta + 1)\delta. \]

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)
\[ (\text{I.K.10}) \quad \alpha_1 = \frac{1}{3}(\theta_+ + \theta_-), \quad \alpha_2 = \frac{1}{3}(\zeta^2\theta_+ + \zeta\theta_-), \quad \alpha_3 = \frac{1}{3}(\zeta\theta_+ + \zeta^2\theta_-), \]
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 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 \(G := \text{Gal}_K(f)\) is a transitive subgroup of \(S_4\), hence limited to the possibilities \(S_4, A_4, D_4, V_4,\) and \(Z_4\). We see right away from Theorem I.K.3 that
- if \(\delta \in K\), then \(G \cong A_4\) or \(V_4\), while
- if \(\delta \notin K\), then \(G \cong S_4, D_4\) or \(Z_4\).

To go further, we need to consider the cubic resolvent of \(g\) and its splitting field, starting with the latter.
Recall that $V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup of $S_4$, so that $H := V_4 \cap G \leq G$. (In fact $H = V_4$ unless $G = ((1234)) \cong Z_4$, in which case $H = Z_2$.) Inside our splitting field $L$ for $g$, consider then $M := \text{Inv}(H)$, with $\text{Aut}(L/M) \cong H \leq V_4$ and

$$\text{Aut}(M/K) \cong G/H \cong G/(G \cap V_4) \cong GV_4/V_4 \leq S_4/V_4 \cong S_3,$$

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

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

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

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

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

One then computes

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

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

(I.K.11) \hspace{1cm} 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 $\zeta$, we therefore have the desired root tower: adjoin $\zeta$ to $K$, then the square root of the discriminant of (I.K.11), then the cubic radical $\theta$ for (I.K.11), which gets us to $M(\zeta)$; finally, adjoining the square roots $\beta_{1j}$ 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:\footnote{In order to make effective use of this, we need to know the discriminant. One can show that $\Delta$ is given by $256r^3 - 128p^2r^2 + 144pq^2r - 27q^4 = 16^2(2^3 - 3^3)$, we find that $\sqrt{\Delta} \notin \mathbb{Q}$. The resolvent is $F(z) =$}

<table>
<thead>
<tr>
<th>$G$</th>
<th>$G/H$</th>
<th>$H$</th>
<th>$g$ irr/M?</th>
<th>$F$ irr/K?</th>
<th>$\sqrt{\Delta} \in K$?</th>
<th>SFEs of $F$ &amp; $g$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathfrak{A}_4$</td>
<td>$\mathcal{S}_3$</td>
<td>$V_4$</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>$K \frac{6}{2} M \frac{4}{2} L$</td>
</tr>
<tr>
<td>$A_4$</td>
<td>$Z_3$</td>
<td>$V_4$</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>$K \frac{3}{2} M \frac{4}{2} L$</td>
</tr>
<tr>
<td>$D_4$</td>
<td>$Z_2$</td>
<td>$V_4$</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>$K \frac{2}{2} M \frac{4}{2} L$</td>
</tr>
<tr>
<td>$V_4$</td>
<td>{1}</td>
<td>$V_4$</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>$K \frac{1}{2} M \frac{4}{2} L$</td>
</tr>
<tr>
<td>$Z_4$</td>
<td>$Z_2$</td>
<td>$Z_2$</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>$K \frac{2}{2} M \frac{2}{2} L$</td>
</tr>
</tbody>
</table>

which leads for instance to the decision diagram

(I.K.12)

$$
\begin{array}{ccc}
\sqrt{\Delta} \in K? & F \text{ irr/} K? & \mathfrak{A}_4 \\
\downarrow & \downarrow & \downarrow \\
Y & Y & V_4 \\
N & N & \mathcal{S}_4 \\
\end{array}
\begin{array}{ccc}
F \text{ irr/} K? & g \text{ irr/} M? & D_4 \\
\downarrow & \downarrow & \downarrow \\
Y & Y & Z_4 \\
N & N & \end{array}
$$

However, one can often avoid computing $\Delta$ 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 $\Delta = 256r^3 - 128p^2r^2 + 144pq^2r - 27q^4 = 16^2(2^3 - 3^3)$, we find that $\sqrt{\Delta} \notin \mathbb{Q}$. The resolvent is $F(z) =$

\footnote{In order to make effective use of this, we need to know the discriminant. One can show that $\Delta$ is given by $256r^3 - 128p^2r^2 + 144pq^2r - 27q^4 = 16^2(2^3 - 3^3)$, we find that $\sqrt{\Delta} \notin \mathbb{Q}$. The resolvent is $F(z) =$}
\[ z^3 - 8z - 16, \text{ which is "equivalent" to } \frac{1}{8} F(2z) = z^3 - 2z - 2, \text{ hence irreducible (again by Eisenstein). So the Galois group is } \mathfrak{S}_4. \]

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