Resolvents

Let K be the splitting field of a polynomial

$$f(x) = x^n - a_1x^{n-1} + a_2x^{n-2} - \pm a_n$$

over F, and let $\alpha_1, ..., \alpha_n$ be the roots of f in K, which we assume to be distinct. We wish to determine the Galois group G. By its operation on the roots, G embeds as a subgroup of the symmetric group $S_n = \mathcal{G}$, and the problem is to determine this subgroup:

Which permutations of the roots come from F-automorphisms of K?

The method we discuss here computes some auxiliary polynomials called *resolvents*, and asks whether or not they have roots in F. Our question can be answered by such computations, in principle.

To help keep track of things, we use the substitution homomorphism

$$F[u_1, ..., u_n] \to K$$

which sends $u_i \rightsquigarrow \alpha_i$. The coefficients a_i of f are obtained by substitution from the elementary symmetric functions: $a_i = s_i(\alpha)$.

Let $p_1(u_1, ..., u_n)$ be a polynomial with coefficients in F. The symmetric group $\mathcal{G}$ operates on the polynomial ring $F[u_1, ..., u_n]$; let its orbit under the action of $\mathcal{G}$ be $\{p_1, ..., p_r\}$.

For example, if $p_1 = u_1u_2$, the orbit of p_1 consists of the products u_iu_j with $i \neq j$.

Lemma. *Let $\{p_1, ..., p_r\}$ be the orbit of a polynomial $p_1(u_1, ..., u_n)$ for the operation of permuting the variables. Let $f(y_1, ..., y_r)$ be a symmetric polynomial in some variables $y_1, ..., y_r$. Then $f(p_1, ..., p_r)$ is a symmetric polynomial in $u_1, ..., u_n$.*

Proof. A permutation of $u_1, ..., u_n$ permutes the orbit $\{p_1, ..., p_r\}$. The corresponding permutation of $y_1, ..., y_r$ fixes the symmetric polynomial f. □

We expand the polynomial $\gamma(x) = (x - p_1) \cdots (x - p_r)$.
Its coefficients are elementary symmetric functions in $p_1, ..., p_r$, so they are also symmetric functions of u, and can be written in terms of the elementary symmetric functions $s_i(u)$, say

$$s_j(p_1, ..., p_r) = q_j(s_1, ..., s_n),$$

where $s_i = s_i(u)$. We make the substitution $u_i = \alpha_i$. Let

$$\beta_j = p_j(\alpha_1, ..., \alpha_n),$$

and let

$$g(x) = (x - \beta_1) \cdots (x - \beta_r) = x^r - b_1x^{r-1} + b_2x^{r-2} + \cdots \pm b_r.$$

The coefficients of g are obtained by the same substitution into $q_j(s_1, ..., s_n)$, so $b_j = q_j(a_1, ..., a_n)$. Therefore $g(x)$ has coefficients in F.

A permutation z of the set $\{u_1, ..., u_n\}$ defines some more permutations:

(a) Since the α_i are distinct, z can equally well be thought of as a permutation of the set $\{\alpha_1, ..., \alpha_n\}$.
(b) z induces a permutation $\widetilde{z}$ of the set $\{p_1, ..., p_r\}$.
(c) Provided that the β_j are distinct, $\widetilde{z}$ can be used to permute $\{\beta_1, ..., \beta_r\}$.

Our notation will be that z sends $u_i \rightsquigarrow zu_i$. Then $\widetilde{z}(p_j(u_1, ..., u_n)) = p_j(zu_1, ..., zu_n)$, which is another one of the polynomials $\{p_1, ..., p_k\}$, say p_ℓ. Assuming that β_j are distinct, we substitute $u_i = \alpha_i$:

$$\widetilde{z}(\beta_j) = \widetilde{z}(p_j(\alpha_1, ..., \alpha_n)) = p_j(z\alpha_1, ..., z\alpha_n) = \beta_\ell.$$

Lemma. *Assume that the β_j are distinct. Let σ be an F-automorphism of K, and let z be the permutation of the roots $\{\alpha_1, ..., \alpha_n\}$ it defines. Then the permutation $\widetilde{z}$ of $\{\beta_1, ..., \beta_r\}$ determined by z is the one defined by σ too.*

Proof. $\widetilde{z}(\beta_j) = p_j(z\alpha_1, ..., z\alpha_n) = p_j(\sigma\alpha_1, ..., \sigma\alpha_n) = \sigma(p_j(\alpha_1, ..., \alpha_n)) = \sigma(\beta_j)$. □

If G is not the whole symmetric group $\mathcal{G}$, there is no reason to suppose that the set $\{\beta_1, ..., \beta_r\}$ forms a single G-orbit in K, and if not, then $g(x)$ will be reducible. We ask: What could we conclude if one of the elements β_j happened to be in F?

Let $\mathcal{H}_j$ be the stabilizer of the polynomial p_j for the operation of $\mathcal{G}$. It is a general property of group operations that the $\mathcal{H}_j$ are *conjugate subgroups* of $\mathcal{G}$, because the polynomials p_j form one orbit.

Theorem. *With the notation as above, suppose that $\beta_1, ..., \beta_r$ are distinct elements of K. Then $\beta_j \in F$ if and only if G is a subgroup of $\mathcal{H}_j$.*

Proof. The theorem follows from the fact that F is the fixed field K^G. Let σ be an F-automorphism of K, let z denote the be the permutation of $\{u_1, ..., u_n\}$ which corresponds to the permutation induced by σ on $\{\alpha_1, ..., \alpha_n\}$, and let $\widetilde{z}$ be the permutation of $\{p_j\}$ induced by z.

We apply the lemma. Because the β_j are distinct, σ fixes β_j if and only if $\widetilde{z}$ fixes u_j, and this happens if and only if $z \in \mathcal{H}_j$. Then $\beta_j \in F$ if and only if β_j is fixed by all $\sigma \in G$, which is true if and only if $G \subset \mathcal{H}_j$. □

Since G is the smallest subgroup of $\mathcal{G}$ in which it is contained, knowing which subgroups of $\mathcal{G}$ contain G determines the group. We need only find suitable resolvents.

Example. The *resolvent cubic* is, aside from the discriminant, the most important resolvent of a quartic equation. It determines whether or not the order of the Galois group is divisible by 3.

Let $n = 4$, and $p_1 = u_1u_2 + u_3u_4$. The orbit contains the three elements p_1, $p_2 = u_1u_3 + u_2u_4$, and $p_3 = u_1u_4 + u_2u_3$. The resolvent cubic is the polynomial

$$\gamma(x) = x^3 - s_1(p)x^2 + s_2(p)x - s_3(p).$$

We compute the coefficients of γ: $s_1(p) = u_1u_2 + (\textit{orbit sum}) = s_2$. Next,

$$s_2(p) = (u_1u_2 + u_3u_4)(u_1u_3 + u_2u_4) + ... \qquad \text{(a sum of 12 terms).}$$

We note that one term is $u_1^2u_2u_3$ and that the orbit of this monomial has order 12. Therefore

$$s_2(p) = u_1^2u_2u_3 + (\textit{orbit sum}).$$

We set the last variable to zero, obtaining

$$s_2(p)^\circ = u_1^2u_2u_3 + u_1u_2^2u_3 + u_1u_2u_3^2 = s_1^\circ s_3^\circ.$$

We note that $s_1s_3 = (u_1 + \cdots)(u_1u_2u_3 + \cdots)$ is a sum of 16 terms, and 12 of them make up the orbit of $u_1^2u_2u_3$, which is $s_2(p)$. Therefore $s_1s_3 = s_2(p) + 4s_4$, and $s_2(p) = s_1s_3 - 4s_4$. Similarly, one finds that $s_3(p) = s_3^2 - 4s_2s_4 + s_1^2s_4$. So

$$\gamma(x) = x^3 - s_2x^2 + (s_1s_3 - 4s_4)x - (s_3^2 - 4s_2s_4 + s_1^2s_4), \qquad s_i = s_i(u).$$

For example, the polynomial $f(x) = x^4 - 6x + 2$ is irreducible over $\mathbb{Q}$, by the Eisenstein criterion. Here $s_1 = s_2 = 0$, $s_3 = 6$, and $s_4 = 2$. So $s_1(p) = 0$, $s_2(p) = -8$, and $s_3(p) = 36$. The resolvent cubic is

$$g(x) = x^3 - 8x - 36,$$

which has no integer root, hence is irreducible over $\mathbb{Q}$. Since it has roots in the splitting field K of f, the degree $[K : F]$ is divisible by 3.