29. Symmetric polynomials and computing Galois groups

This worksheet attempts to address two questions from past classes:

(1) "Is there an algorithm to compute Galois groups?" and
(2) What is the relationship between symmetries of polynomials and Galois symmetries?

It will be important to remain a careful distinction between formal polynomials, and those polynomials evaluated at specific algebraic numbers. I'll use capital letters for the former, and for the fields that contain them, and lower case letters for the latter.

Let $f(x) = x^n - e_1 x^{n-1} + e_2 x^{n-2} - \cdots \pm e_n$ be a separable polynomial in $\mathbb{Q}[x]$, let $r_1, \ldots, r_n$ be the roots of f in $\mathbb{C}$ and let $\ell = \mathbb{Q}(r_1, \ldots, r_n)$. So we identify $Gal(\ell/\mathbb{Q})$ with a subgroup of S_n.

Let $L = \mathbb{Q}(R_1, \ldots, R_n)$ and let K be the field of symmetric rational functions in L, so $K = \mathbb{Q}(E_1, \ldots, E_n)$ where the E_j are the elementary symmetric polynomials, so $\prod(x - R_j) = x^n - E_1 x^{n-1} + E_2 x^{n-2} - \cdots \pm E_n$.

Let $H \in \mathbb{Q}[R_1, \ldots, R_n]$. Let Γ be the subgroup $\{\gamma \in S_n : H(R_1, \ldots, R_n) = H(R_{\gamma(1)}, \ldots, R_{\gamma(n)})\}$. As an example, if $H = R_1^2 R_2 + R_2^2 R_3 + R_3^2 R_1$, then $\Gamma = \langle (123) \rangle$. Let h be the complex number $H(r_1, \ldots, r_n)$.

Problem 29.1. Suppose that $\mathrm{Gal}(\ell/\mathbb{Q}) \subseteq \Gamma$. Show that $h \in \mathbb{Q}$.

Problem 29.2. Suppose that, for $\sigma \not\in \Gamma$, we have $H(r_1, \ldots, r_n) \neq H(r_{\sigma(1)}, \ldots, r_{\sigma(n)})$. Then show that $h \in \mathbb{Q}$ if and only if $\mathrm{Gal}(\ell/\mathbb{Q}) \subseteq \Gamma$.

So, we can test whether $\mathrm{Gal}(\ell/\mathbb{Q})$ is contained in a particular subgroup of S_n by testing whether or not $H(r_1, \ldots, r_n) \in \mathbb{Q}$, subject to needing the extra hypothesis that, if $H(R_1, \ldots, R_n) \neq H(R_{\sigma(1)}, \ldots, R_{\sigma(n)})$ then $H(r_1, \ldots, r_n) \neq H(r_{\sigma(1)}, \ldots, r_{\sigma(n)})$.

The next problems discuss two approaches to teach whether $h \in \mathbb{Q}$. As our running example, we will look at the cubics $x^3 - 4x - 1$ and $x^3 + x^2 - 2x - 1$ and test whether their Galois groups are contained in the subgroup $\langle (123) \rangle$ of S_3. We'll look at the polynomial $H(R_1, R_2, R_3) = R_1^2 R_2 + R_2^2 R_3 + R_3^2 R_1$ which, indeed, has symmetry group $\langle (123) \rangle$.

First approach

Problem 29.3. Suppose that all the e_j (the coefficients of $f(x)$) are integers and let $H \in \mathbb{Z}[R_1, \ldots, R_n]$. Show that $h \in \mathbb{Q}$ if and only if $h \in \mathbb{Z}$.

This is useful, because it means that we can just compute $h(r_1, \ldots, r_n)$ to enough numerical accuracy to determine whether or not it is an integer.

Example: We have $x^3 - 4x - 1 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ and $x^3 + x^2 - 2x - 1 = (x - \beta_1)(x - \beta_2)(x - \beta_3)$ where $(\alpha_1, \alpha_2, \alpha_3) = (-1.8608, -0.2541, 2.1149)$ and $(\beta_1, \beta_2, \beta_3) = (-1.8019, -0.4450, 1.2470)$. We compute

$$\alpha_1^2 \alpha_2 + \alpha_2^2 \alpha_3 + \alpha_3^2 \alpha_1 = -9.066 \qquad \beta_1^2 \beta_2 + \beta_2^2 \beta_3 + \beta_3^2 \beta_1 = -4.000.$$

Thus, in the first case, the Galois group cannot be contained in $\langle (123) \rangle$ and, in the second, it is highly likely to be.

Second approach

$$G(x) = \prod_{\sigma \in \Gamma \backslash S_n} \Big(x - H(R_{\sigma(1)}, \ldots, R_{\sigma(n)}) \Big).$$

Here the product if over cosets of $\Gamma \backslash S_n$, choosing one element from each coset.

Problem 29.4. Explain why the product is well defined, independent of the choice of element from each coset.

Problem 29.5. Show that the coefficients of G lie in $\mathbb{Q}[E_1, \ldots, E_n]$ (this is just quoting a very old problem).

Let $g(x)$ be the polynomial in $\mathbb{Q}[x]$ that we get by evaluating the coefficients of G at $E_j = e_j$.

Problem 29.6. Show that h is a root of g. Conclude that, if $\mathrm{Gal}(\ell/\mathbb{Q}) \subseteq \Gamma$, then g has a rational root.

Problem 29.7. Suppose g has a rational root of multiplicity 1. Show that there is some $\sigma \in S_n$ such that $\mathrm{Gal}(\ell/\mathbb{Q}) \subseteq \sigma \Gamma \sigma^{-1}$.

Our running example: We have

$$(x - R_1^2 R_2 - R_2^2 R_3 - R_3^2 R_1)(x - R_2^2 R_1 - R_3^2 R_2 - R_1^2 R_3) = x^2 - (E_1 E_2 - 3E_3)x + (E_2^3 - 6E_1 E_2 E_3 + E_1^3 E_3).$$

Evaluating $E_1 E_2 - 3E_3$ and $E_2^3 - 6E_1 E_2 E_3 + E_1^3 E_3$ at the coefficients of our two example cubics gives: $x^2 + 3x - 55$ and $x^2 - x - 12$ respectively. The first does not have a rational root and the second does, so the splitting field of the first cubic does not have Galois group contained in $\langle (123) \rangle$ and the second does. In approach, all computations are done with rational numbers, so there is no fear of round off error. However, the computations are much larger, and you have to deal with the complication of finding an S_n-conjugate of the correct group rather than the group itself.

Example – the alternating group: Homework problem 9.4 was an example of this approach: Let $\Delta = \prod_{i<j}(R_i - R_j)$ and let $\Phi = \Delta^2$, so Φ is a symmetric polynomial. The symmetry group of Δ is A_n, and the minimal polynomial of Δ is $x^2 - \Phi$, so we get that $\mathrm{Gal}(\ell/\mathbb{Q}) \subset A_n$ if and only if $\Phi(r_1, \ldots, r_n)$ is a square. The polynomial Φ is called the ***discriminant***.

Example – constructibility of roots of quartics: Let Γ be the subgroup $\langle (12), (34), (13)(24) \rangle$ of S_4; this is a 2-Sylow subgroup. We have

$$(y - R_1 R_2 - R_3 R_4)(y - R_1 R_3 - R_2 R_4)(y - R_1 R_4 - R_2 R_3) = y^3 - E_2 y^2 + (E_1 E_3 - E_4)y - (E_1^3 + E_1^2 E_4 - 4E_2 E_4).$$

Let ℓ be the splitting field of a quartic $x^4 - e_1 x^3 + e_2 x^2 - e_3 x + e_4$. Then $\mathrm{Gal}(\ell/\mathbb{Q})$ is contained in a conjugate of Γ if and only if $\mathrm{Gal}(\ell/\mathbb{Q})$ is a 2-group (by the second Sylow theorem). And Γ is a 2-group if and only if the roots of $x^4 - e_1 x^3 + e_2 x^2 - e_3 x + e_4$ are constructible. So we deduce that the roots of $x^4 - e_1 x^3 + e_2 x^2 - e_3 x + e_4$ are constructible if and only if $y^3 - e_2 y^2 + (e_1 e_3 - e_4)y - (e_1^3 + e_1^2 e_4 - 4e_2 e_4)$ has a rational root.