Scratchwork: Galois Theory, Symmetric Polynomials, Geometry

How to find the Galois group of a cubic equation?
$x^3 + ax^2 + bx + c = (x - r_1)(x - r_2)(x - r_3) = x^3 - (r_1 + r_2 + r_3)x^2 + (r_1r_2 + r_2r_3 + r_3r_1)x - r_1r_2r_3 = 0$

Symmetric function identities

- $r_1 + r_2 + r_3 = r_1 + r_2 + r_3$
- $r_1r_2 + r_2r_3 + r_1r_3 = \frac{1}{2}\big[(r_1 + r_2 + r_3)^2 - (r_1^2 + r_2^2 + r_3^2)\big]$
- $r_1r_2r_3 = (r_1 + r_2 + r_3)^3 - 2(r_1^3 + r_2^{+} r_3^3) + (r_1 + r_2 + r_3)(r_1^2 + r_2^2 + r_3^2)$

Ex $x^3 - x + 1 = 0$ over $\mathbb{Q}$. So the Galois group is S_3. What are the automorphisms?[1]

Ex $x^3 - (2 + i)x + 5 = 0$ over $\mathbb{Q}(i)$. Is this a cyclic extension? Maybe we can write a 2×2 matrix equation:

$$X^3 - \begin{bmatrix} 2 & 1 \\ -1 & 2 \end{bmatrix} X + \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix} = 0 \quad \text{with} \quad X = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

The Galois group G might be all of S_3 or just $C_3 \simeq A_3$. Perhaps this is why they call it a G-module.

$$M = \{r_1^2r_2^2, r_2^2r_3^2, r_1^2r_3^2\} \text{ then } \dim M \leq 3$$

Can we show the dimension is less than three using these relations?

- $r_1 + r_2 + r_3 = 0$
- $r_1r_2 + r_2r_3 + r_3r_1 = -1$
- $r_1r_2r_3 = -1$

Where do symmetric function identities come from? The permutation group on three elements has three group representations, $\ydiagram{3}$ or $\ydiagram{2,1}$ or $\ydiagram{1,1,1}$. There are several kinds of symmetic polynomials, **elementary symmetric polynomials** and **complete symmetric polynomials** and **power sum symmetric polynomials**. Our Galois Theory example seems to give the elementary symmetric polynomials.

$$s(\ydiagram{3,1}) = s_{(2,1,1)} = \frac{1}{\Delta}\begin{vmatrix} x_1^4 & x_2^4 & x_3^4 \\ x_1^2 & x_2^2 & x_3^2 \\ x_1 & x_2 & x_3 \end{vmatrix} = x_1x_2x_3(x_1 + x_2 + x_3)$$

? Do prime numbers over $\mathbb{Z}$ such as 5 or 23 factor in $\mathbb{Q}[x]/(x^3 - x - 1)$. Find explicit factorizations.

References

[1] Henri Cohen **Computational Number Theory in Relation with L-Functions** `arXiv:1809.10904`

[1] The map $x \mapsto ?$ that take polynomial to itself.