Galois Theory: Projects

January 27, 2013

Only the last of these topics requires a knowledge of Galois theory, although all of them are related to the course in some way. As you can see, they are very different in character – indeed, the material in the first, second, third and fourth projects dates from the 17th, 18th, 19th and 20th century, respectively. The first two are easier, and are described clearly and thoroughly in the references given, while the third, though described very well in both references, is hard, and the fourth is somewhat complicated. I will take all this into account, so **choose a project you like**. We'll find some way of dealing with conflicts, should they arise. The aim is to have 2 people to each project: you are each required to read and understand the proof(s), and each of you should present something in class.

The fundamental theorem on symmetric polynomials

The theorem states that every symmetric polynomial $p(x_1, \ldots, x_n)$ in n variables can be expressed as a polynomial $P(s_1, \ldots, s_n)$ in the *elementary symmetric polynomials*

$$\begin{aligned} s_1(x_1, \ldots, x_n) &= \sum x_i \\ s_2(x_1, \ldots, x_n) &= \sum_{\cdots} x_i x_j \\ s_n(x_1, \ldots, x_n) &= x_1 x_2 \cdots x_n. \end{aligned}$$

There is a proof by induction in Chapter 6 of Stillwell's book (Exercise 6.5.1), and a proof using Galois theory in Chapter 9 (Exercise 9.3.4). Present whichever proof you like.

The result goes back to Newton and Girard, and is a cornerstone of classical Galois theory. Galois used it to prove the primitive element theorem, *Lemme III* of his memoir. This proof is also part of the project. Edwards [1] contains an expanded version of Galois' sketch.

[1] H.M. Edwards, Galois Theory, Springer-Verlag, 1984.

[2] H.M. Edwards, Galois for 21st-century readers, *Notices of the American Mathematical Society* **59** (2012), 912–923.

[3] P.M. Neumann, Review of *Galois Theory* by Harold M. Edwards, *American Mathematical Monthly* **93** (1986), 407–411.

[4] P.M. Neumann, The mathematical writings of Évariste Galois, European Mathematical Society, 2011.

The construction of the regular heptadecagon

The constructions of the equilateral triangle and regular pentagon appear in Euclid's Elements (in Books I and IV, respectively). The next major advance was made in 1796 by Gauss, who proved that it is possible to construct the regular seventeen-sided polygon. All these constructions are with *straightedge and compass* (see Section 1.2 of Stillwell's book for a precise definition). Gauss was so proud of his discovery that he requested that a regular seventeen-sided polygon be inscribed on his tombstone.

The relevant Galois theory is described in Section 9.8 of Stillwell's book; for the construction itself, see Chapter 5 of Hardy and Wright [1], or Chapter 19 of Stewart [2].

[1] G.H. Hardy and E.M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, 2008.

[2] I.N. Stewart, Galois Theory, Chapman and Hall, 2004.

The transcendence of π

The three great construction problems of antiquity were to square the circle, duplicate the cube, and trisect the angle, with straightedge and compass. All three are impossible. The second and third were shown to be so by Wantzel in 1837, while the first is rendered impossible by a little field theory (which I will cover in class) and the transcendence of π. This last fact was finally established by Lindemann in 1882, with an astonishing proof. Ian Stewart wrote that all mathematicians should see it at least once in their lives, while Felix Klein wrote in 1893:

> The problem has thus been reduced to such simple terms that the proofs for the transcendency of e and π should henceforth be introduced into university teaching everywhere.

Stewart's book [2] contains the whole proof, while Klein's lecture [1] gives a good overview of the argument. The proof itself uses the fundamental theorem on symmetric polynomials, but is otherwise unrelated to Galois Theory (as far as I know). I've included it as a project because I share the sentiments above.

[1] F. Klein, The transcendency of the numbers e and π, in *Lectures on Mathematics*, AMS Chelsea Publishing, 2000.

[2] I.N. Stewart, Galois Theory, Chapman and Hall, 2004.

Computing the Galois group of a quartic

If $p \in \mathbb{Q}[x]$ is an irreducible quartic with splitting field $F \subset \mathbb{C}$, then $\mathrm{Gal}(F : \mathbb{Q})$ is isomorphic to a transitive subgroup of S_4. There are 5 such subgroups, so how do we tell, given the coefficients of p, which one is the Galois group? Galois' memoir itself actually contains an algorithm (or a sketch of one), but the paper below provides a simpler method.

[1] L. Kappe and B. Warren, An elementary test for the Galois group of a quartic polynomial, *American Mathematical Monthly* **96** (1989), 133–137.
