Galois at 200

A Lecture Presented at Fq10, Ghent, Belgium, 2011

Michael Rosen, Brown University

Évariste Galois was one of the greatest mathematicians of all times. The outlines of his short, tragic life are well known (at least to mathematicians). He was born on October 25, 1811 in the village of Bourg-la-Reine on the outskirts of Paris. He died in a duel on May 31, 1832 at the age of twenty. His monumental contributions to mathematics were developed between the ages of sixteen and twenty. It is not my intention to review his life's story. A short overview can be obtained from the entry "*Évariste Galois*" at Wikipedia.com. For a fuller version see Leopold Infeld, *Whom the Gods Love: The Story of Evariste Galois*, or the more recent and scholarly account of Laura Toti Rigatelli, *Evariste Galois*.

Instead of going over the details of his life, I wish to illustrate the beauty of the mathematical ideas he developed by proving in some detail one of his brilliant, but little known theorems. It is my hope that the beauty, originality, and depth of his contributions will shine forth.

Before beginning, let me recall two of his papers. The first, entitled *Sur la théorie des nombres*, was published in 1830. Here he develops in systematic fashion the theory of finite fields. This was the first time the theory had appeared in print. For many years, in his honor, the name "Galois field" was used instead of "finite field". The whole presentation of the subject in his memoire is remarkably modern.

The second paper I want to call to your attention is *Memoire sur les conditions de resolubilité des equations par radicaux*. In this paper he lays out the foundations of the theory which now bears his name. Although submitted three times it did not appear in his lifetime. Twice it was lost and once it was rejected. Years later, at the urging of Galois' friends, the eminent mathematician Liouville found and read the neglected manuscript. Finding the work entirely sound, he published it in his famous journal, Journal de Mathématique Pure et Appliquées. This was in 1846, fourteen years after Galois' death. Once published the mathematical world took little time to recognize its worth. The repercussions and developments of Galois' theory continue to this day.

For a translation and detailed discussion of this memoir (and much else) see the book of Harold M. Edwards, *Galois Theory*.

Galois associates a finite group of permutations G_f to a polynomial equation $f(x) = 0$. He shows that the equation is solvable in radicals if and only if G_f is a solvable group. It should be noted that before Galois even the notion of a normal subgroup of a group was not known. He defined it and also defined what it means for a group of permutations to be solvable. A subgroup H of a group G is normal, according to Galois, if its set of left cosets is equal to its set of right cosets. This is easily seen to be equivalent to the usual definition. He calls a finite group solvable if and only if there exists a series of subgroups

$$(e) \subset G_1 \subset G_2 \subset \ldots \subset G_{t-1} \subset G_t = G \ ,$$

where each G_i is a normal subgroup of G_{i+1} and for all i, $[G_{i+1} : G_i]$ is prime. Note that this definition avoids talking about quotient groups. The notion of a quotient group does not seem to occur in Galois' works.

As an application of his general theory, Galois states the following, which is the last theorem in his memoir.

Theorem A. *In order for an irreducible equation of prime degree to be solvable in radicals, it is necessary and sufficient that once any two roots are known, the others can be deduced from them rationally.*

This result is not as well known as it deserves to be. My main purpose is to present the proof and an application. For clarity, I will use modern notation and ways of doing Galois theory. However, I will attempt to avoid using any tools that were unavailable to Galois.

Let $f(x) \in k[x]$, where k is a field of characteristic zero. We assume that $f(x)$ has no repeated factors. Suppose that $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of $f(x)$ in some extension field of k. Set $L = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Then, L/k is a Galois extension. Let $G = \mathrm{Gal}(L/k)$ be its Galois group. G acts on the set of roots, i.e. if $\sigma \in G$ then $\sigma\alpha_i = \alpha_{\pi(i)}$ where $\pi \in S_n$, the symmetric group on n letters. The map $\rho : G \to S_n$ which takes σ to π is a monomorphism. The image of ρ, $G_f \subseteq S_n$, is what Galois calls the group attached to $f(x)$. Note that $f(x)$ is irreducible if and only if G_f is a transitive subgroup of S_n.

Here is a reformulation of Theorem A.

Theorem B. *Suppose $f(x)$ is irreducible of prime degree p. Then, $f(x) = 0$ is solvable in radicals if and only if for all $1 \leq i, j \leq p$ with $i \neq j$, we have $k(\alpha_1, \alpha_2, \ldots, \alpha_p) = k(\alpha_i, \alpha_j)$.*

Using Galois theory we can easily translate this into a statement about groups.

Theorem C. *Let p be a prime, and $G \subseteq S_p$ a transitive subgroup. Then, G is solvable if and only if the only element of G which has two or more fixed points is e, the identity permutation.*

We now proceed to the proof of Theorem C.

Proposition 1. *Suppose $G \subseteq S_n$ is transitive. Let N be a normal subgroup of G. All the orbits of N have the same number of elements, m say. The number m divides n.*

Proof. Let i be an integer between 1 and n and H_i the isotropy subgroup of i in G. The number of elements in the N orbit of i is $[N : N \cap H_i]$. Let j be another integer between 1 and n. Since G is transitive, there is a $\sigma \in G$ such that $\sigma(i) = j$. One easily sees that $H_j = \sigma H_i \sigma^{-1}$. Since N is normal, it follows that $N \cap H_i$ is conjugate to $N \cap H_j$, from which it follows that the N orbit of i has the same number of elements as the N orbit of j.

Since $\{1, 2, \ldots, n\}$ is the disjoint union of the orbits of N each of which has m elements, we see that m divides n.

Corollary. *Suppose that $n = p$, a prime, and that N is not (e). Then, N acts transitively.*

Proof. The number m of elements in an N orbit must be bigger than 1. Otherwise, every element of N fixes every integer between 1 and p, i.e. $N = (e)$. By the Proposition, m divides p implying $m = p$. Thus, N is transitive.

Proposition 2. *Suppose p is a prime and $G \subseteq S_p$ is transitive and solvable. By definition, there is a tower of subgroups G_i, $i = 0, 1, \ldots, t$, such that $G_0 = (e)$, G_i normal in G_{i+1}, $[G_{i+1} : G_i] = p_i$, a prime, and $G_t = G$. We must have $p_1 = p$, i.e. G_1 is a cyclic subgroup of order p.*

Proof. Since $G_{t-1} \neq (e)$ is normal in G, and G is transitive, it follows from the above Corollary that G_{t-1} is transitive. Since G_{t-1} is transitive and $G_{t-2} \neq (e)$ is normal in G_{t-1}, it follows that G_{t-2} is transitive. Proceeding inductively down the tower we find that G_1 is transitive. Since G_1 is transitive, its order p_1 is divisible by p. Thus $p_1 = p$.

Let τ' be a generator of G_1. Since τ' has order p it must be a p-cycle. Conjugating G if necessary by an element of S_p, we can assume that $\tau' = (1, 2, 3, \ldots, p)$.

At this point Galois makes use of a very clever idea. Instead of the set $\{1, 2, \ldots, p\}$, he lets the set being acted on be $\{\bar{0}, \bar{1}, \ldots, \overline{p-1}\} = \mathbb{Z}/p\mathbb{Z}$. This has a group structure! Our cycle $(1, 2, 3, \ldots, p)$ becomes the translation $\tau(x) = x + \bar{1}$. From now on we drop the bars and write $\{0, 1, \ldots, p-1\} = \mathbb{Z}/p\mathbb{Z}$ and allow modular arithmetic modulo p. Galois introduces the group $A(1, p)$ of affine transformations $x \to ax + b$, where $a \in (\mathbb{Z}/p\mathbb{Z})^*$ and $b \in \mathbb{Z}/p\mathbb{Z}$. This is a group of order $p(p-1)$. There are two important subgroups; the subgroup of translations $x \to x + b$ and the subgroup of dilations $x \to ax$ of orders p and $p-1$ respectively. The subgroup of translations is the cyclic group generated by τ which we denote by $< \tau >$. It will play a major role.

Lemma. *Every element of $A(1, p)$ not in $< \tau >$ has order dividing $p - 1$.*

Proof. Here is a sharper form of the Lemma. Let $T(x) = ax + b$ with $a \neq 1$. Then, the order of T in $A(1, p)$ is equal to the order of a in $(\mathbb{Z}/p\mathbb{Z})^*$. We leave this as an exercise for the reader.

Corollary. *$< \tau >$ is a normal subgroup of $A(1, p)$.*

Proof. For any $\sigma \in A(1, p)$ we have $\sigma\tau\sigma^{-1}$ has order p which implies, by the Lemma, that $\sigma\tau\sigma^{-1} \in < \tau >$.

Proposition 3. *If $\lambda \in S_p$ and $\lambda\tau\lambda^{-1} \in A(1, p)$, then $\lambda \in A(1, p)$.*

Proof. Since $\lambda\tau\lambda^{-1}$ has order p, it must be in $< \tau >$ by the above Lemma. Thus, $\lambda\tau\lambda^{-1} = \tau^a$ for some $a \in (\mathbb{Z}/p\mathbb{Z})^*$. From $\lambda\tau = \tau^a\lambda$ we find $\lambda(x + 1) = \lambda(x) + a$. By an obvious induction, we find $\lambda(x + r) = \lambda(x) + ar$ for all $r \in \mathbb{Z}/p\mathbb{Z}$. Set $x = 0$ and we find $\lambda(r) = ar + \lambda(0)$. This shows that $\lambda \in A(1, p)$.

We are now in a position to prove Theorem C. We break the proof up into two parts corresponding to the "if and only if" parts of the statement.

Proof of Theorem C, Part 1

We will assume G is solvable and show G is conjugate within S_p to a subgroup of $A(1, p)$. We will deduce the fixed point property from this.

Since G is solvable, we have a normal series

$$(e) \subset G_1 \subset G_2 \subset \ldots \subset G_{t-1} \subset G_t = G \ .$$

By assumption, G_i is normal in G_{i+1} and $[G_{i+1} : G_i]$ is prime. By Proposition 2 and the folllowing remarks, we can assume $G_1 =< \tau >$ where $\tau(x) = x + 1$. If $\lambda \in G_2$, we have $\lambda\tau\lambda^{-1} \in G_1 =< \tau >$ since G_1 is normal in G_2. This shows that $\lambda\tau\lambda^{-1} \in A(1, p)$ so by Proposition 3, $\lambda \in A(1, p)$. It follows that $G_2 \subseteq A(1, p)$. Now, let $\lambda \in G_3$. Then, $\lambda\tau\lambda^{-1} \in G_2$ since $\tau \in G_2$ and G_2 is normal in G_3. Thus, $\lambda\tau\lambda^{-1} \in A(1, p)$ and, again invoking Proposition 3, we see that $\lambda \in A(1, p)$. Since this is true for all $\lambda \in G_3$ it follows that $G_3 \subseteq A(1, p)$. Proceeding in this manner up the chain we deduce that $G \subseteq A(1, p)$.

We now show that the only element of G with two or more fixed points is the identity e. Let $\sigma \in G$. Since $G \subseteq A(1, p)$, we see $\sigma(x) = ax + b$ for suitable a and b. Suppose $i \neq j$ and both i and j are fixed points of σ. Then, $ai + b = i$ and $aj + b = j$. Subtracting these equations yields $a(i - j) = i - j$. It follows that $a = 1$ and $b = 0$. This shows $\sigma = e$, as asserted.

Proof of Theorem C, Part 2

We now suppose that $G \subset S_p$ is transitive and has the property that the only element in G with two or more fixed points is e, the identity. We will show that these properties imply that G is solvable.

In the proof we need the fact that $A(1, p)$ is solvable. From a modern point of view this is clear since $< \tau >$ is a cyclic normal subgroup with cyclic quotient group. However, Galois did not seem to have the idea of a quotient group, so here is a sketch of a proof that does not use this notion. Let T and D denote the subgroups of $A(1, p)$ of translations and dilations respectively. T is cyclic of order p and D is cyclic of order $p - 1$. Since T is a normal subgroup (see the Corollary to the Lemma) it follows that A(1,p) is the semi-direct product of T and D. Since D is cyclic, one easily constructs a series of subgroups $(e) \subset D_1 \subset D_2 \subset \ldots \subset D_{m-1} \subset D_m = D$ where for all i, $[D_{i+1} : D_i]$ is prime. Then,

$$(e) \subset T \subset D_1T \subset D_2T \subset \ldots \subset D_{m-1}T \subset D_mT = A(1, p) \ .$$

is a normal series with the index at each step being a prime number. This shows $A(1, p)$ is solvable.

Since G is transitive, its order is divisible by p and it follows that G contains a p-cycle. By conjugating G be a suitable element of S_p we can assume the p-cycle is $(1, 2, 3, \ldots, p)$. Then, changing the notation as in the discussion after Proposition 2, we can assume $\tau \in G$ where $\tau(x) = x + 1$. We will show that all the elements in G of order p are in $< \tau >$. Let's assume for the moment that this has been done. It follows that $< \tau >$ is a normal subgroup of G. Then, for all $\lambda \in G$ we have $\lambda\tau\lambda^{-1} \in < \tau > \subset A(1, p)$. By Proposition 3, $\lambda \in A(1, p)$. It follows that $G \subseteq A(1, p)$ and since we have shown $A(1, p)$ is solvable, it follows that G is solvable.

One can invoke the Sylow theorems in order to show $< \tau >$ contains all the elements on G of order p. These theorems had not yet been discovered during Galois lifetime, so we prefer to give a proof which does not use them.

Let S be the set of pairs (k, l) where $0 \leq k, l \leq p - 1$ and $k \neq l$. This set has $p(p - 1)$ elements. Let $(i, j) \in S$ and map G into S by sending σ to $(\sigma(i), \sigma(j))$. If $(\sigma(i), \sigma(j)) = (\rho(i), \rho(j))$, then $\rho^{-1}\sigma$ has two fixed points, namely i and j. By assumption, this implies $\rho^{-1}\sigma = e$, i.e. $\rho = \sigma$. This shows our map is one to one, so $|G| \leq p(p - 1)$.

Now, suppose there is a $\theta \in G$ of order p which is not in $< \tau >$. Then, $< \theta > \cap < \tau >= (e)$ and it follows that $< \theta >< \tau >$ has p^2 elements. This cannot happen since $|G| \leq p(p-1)$. The proof is complete.

Here is a useful theorem of Kronecker which he proved without knowing the result of Galois that we have just proved.

Theorem. *Let $f(x) \in \mathbb{Q}[x]$ be irreducible and solvable of prime degree. If $f(x) = 0$ has two real roots, then all of its roots are real.*

This is immediate from Theorem B, since of α_i and α_j are real, then every element of the field $\mathbb{Q}(\alpha_i, \alpha_j)$ is real. Thus, all the roots are real.

As a concrete application, consider the integral polynomial $f(x) = x^q - apx - p \in \mathbb{Z}[x]$. Assume $a \geq 2$ and that q and p are both positive primes with $q \geq 5$. By the Eisenstein criterion, $f(x)$ is irreducible. Using calculus to plot its graph one easily shows there are exactly three real roots. By Kronecker's result, we see that the Galois group of this polynomial is not solvable.

The night before he was mortally wounded in a duel, Galois wrote a long letter to his friend Auguste Chevalier in which he outlines his ideas and to which he attached three manuscripts. About this letter Hermann Weyl commented, "This letter, if judged by the novelty and profundity of the ideas it contained, is perhaps the most substantial piece of writing in the whole literature of mankind". This may or may not strike us as exaggerated, but it certainly shows the immense respect held by one of the greatest mathematicians of the twentieth century for the young genius Évariste Galois whose bicentennial we celebrate this year. His life was tragically short, but his influence only increases as time goes by.