A Note on Galois Theory

HAROLD M. EDWARDS

GALOIS' tragic marginal note *..Il y a quelque chose à compléter dans cette démonstration. Je n'ai pas le temps,*" gives the impression that there is a serious gap in his memoir on the solution of equations. As I stated in my book *Galois Theory,* I believe that the only gap in GALOIS' eyes (in the eyes of his contemporaries the entire memoir was so terse as to be virtually unintelligible) was that the proposition being proved had been changed but the proof had not:

> "The famous statement 'I haven't the time' occurs in a marginal note Galois made probably on the night before the duel, with regard to the proof of his Proposition II, which he said needed to be 'completed'. Although his proof appears wrong at first because he adjoins *one* root r of an equation and then uses *other* roots of the equation, and although Liouville found it necessary to circumvent Galois' proof entirely, I believe now that the proof given in § 44 is very close to what Galois had in mind, and that the marginal note was merely prompted by the fact that he had *changed the statement of the Proposition,* and realized that the proof needed to be amended accordingly. (In fact, the Proposition, as stated, is false. The index of the subgroup need not be 1 or p when p is not prime – it must simply be a divisor of p.)" ([E, pp. ix–x])

The "proof Galois had in mind" is not explained in the book (it is divided among the text, pp. 59–61, the exercises, number 6 in the 6th set, and the answers to the exercises), and some readers have had difficulty proving Proposition II by an argument analogous to the one in my § 44. Therefore, I would like to explain in detail what I believe GALOIS' proof to have been.

Prior to Proposition II, GALOIS has constructed in a quite concrete form the group now known as the GALOIS group of an equation. Briefly, his construction is as follows.

Let the given equation be $f(x) = 0$, where f is a polynomial of degree m with coefficients in a given field K. (In our terminology, GALOIS appears to assume the field K under consideration to be a field obtained from the rational numbers by a finite number of algebraic and/or transcendental adjunctions.) GALOIS asserts that if $a, b, c, \dots$ are the m roots of f then there exist (provided f has no multiple roots) integers $A, B, C, \ldots,$ such that the $m!$ "values" obtained by permuting $a, b, c, \ldots,$ in the "function" $Aa + Bb + Cc + \ldots$ are distinct. In speaking of these "values" Galois tacitly assumes the existence of a splitting field of f, that is, assumes there is a domain in which the operations of arithmetic can be carried out which contains the coefficient field K and contains m roots of f. As far as I know, nothing in Galois' works permits us to guess what view he took of this basic assumption. However, granted the existence of a splitting field, it is easily shown, along lines I indicate in my book, that, indeed, integers $A, B, C, \ldots,$ can be chosen so that $AS(a) + BS(b) + CS(c) + \ldots$ assumes $m!$ distinct values in the splitting field when S ranges over all permutations of the roots $a, b, c, \ldots$ of f (§ 32). The polynomial $F(X) = \Pi(X - V^{(i)})$, where $V^{(i)}$ ranges over these $m!$ values, is a polynomial with coefficients in K (a symmetric function in the roots of a polynomial $f(x)$ can be expressed as a rational function in the coefficients of $f(x)$). Since $V = Aa + Bb + Cc + \ldots$ is a root of $F(X)$, it is a root of some factor of $F(X)$ irreducible over K, say $G(V) = 0$ where $G(X)$ is a factor of $F(X)$ irreducible over K.

Given $G(X)$, one can *construct explicitly* a splitting field of f. This concrete and computational description of the splitting field seems to me to lie at the heart of Galois theory. The construction is simply to adjoin one root of G to K (see § 34 for a full explanation of this construction), which gives a splitting field of f by virtue of Galois' Lemma III:

> "When the function V is chosen as indicated above, it will have the property that all the roots of the given equation can be expressed as rational functions of V."

In other words, the roots $a, b, c, \ldots,$ of f in the splitting field are all contained in the subfield $K(V)$ generated by V. My explication of Galois' proof of Lemma III is in § 37. In his review of the book, Peter M. Neumann wrote of this explication: "Edwards feels that Galois was right and he gives a line of argument that undoubtedly completes the proof. But to do this he has to read very much more than is there into what Galois actually wrote, and I find his justification rather far-fetched" ([N, p. 411]). Since my objective in the present paper is similar to my objective in § 37, and since I want to persuade the reader that I am not "reading very much more than is there into what Galois actually wrote," I would like to review Galois' proof of Lemma III before going on to Proposition II.

Galois would surely have taken it as known that a symmetric polynomial in the roots of a monic polynomial g can be expressed as a polynomial in the coefficients of g. Therefore, any symmetric polynomial in the roots $b, c, \ldots$ of $f(x)$ other than a can be expressed as a polynomial in the coefficients of $f(x)/(x - a)$ (assuming, as we may without loss of generality, that $f(x)$ is monic). Therefore, any symmetric polynomial in $b, c, \ldots,$ can be expressed as a polynomial in a. (If $f(x) = x^m + px^{m-1} + qx^{m-2} + rx^{m-3} + \ldots$ then $f(x)/(x-a) = x^{m-1} + Px^{m-2} + Qx^{m-3} + Rx^{m-4} + \ldots$ where $P = a + p$, $Q = a^2 + pa + q$, $R = a^3 + pa^2 + qa + r$, *etc.*, so the coefficients of $f(x)/(x - a)$ are polynomials in a.) Galois applies this observation to the product

$$\Pi(X - Aa - BS(b) - CS(c) - \ldots),$$

where the product is over all permutations S of $b, c, \ldots,$ to write it in the form $F(X, a)$. Then F is a polynomial in two variables with coefficients in K for which $F(V, a) = 0$. On the other hand, since the relation $F(X, a) = \Pi(X - Aa - BS(b) - CS(c) - \ldots)$ is derived using just the assumption that a is a root of $f(x)$ and $b, c, \ldots,$ are the other roots, one clearly has $F(X, b) = \Pi(X - Ab - BS(a) - CS(c) - \ldots)$, where the product is over all permutations S of $a, c, \ldots$. Therefore, by the choice of V, $F(V, b) \neq 0$. Since the same is true of $c, \ldots,$ *the only common root of $f(x)$ and $F(V, x)$ is a.* Galois observes this property of a and concludes without further argument that a can be expressed as a rational function of V. The argument, surely, is that when the Euclidean algorithm is used to find the greatest common divisor of $f(x)$ and $F(V, x)$, regarding both as polynomials in x with coefficients in the field $K(V)$, the result is a polynomial with coefficients in $K(V)$ with the single root a. Therefore, a is the root of a linear polynomial with coefficients in $K(V)$, which implies $a \in K(V)$.

Although Galois wastes no words, every idea in the proof of Lemma III just given is clearly indicated in his proof:

> En effet, soit
>
> $$V = \phi(a, b, c, d, \ldots),$$
>
> ou bien
>
> $$V - \phi(a, b, c, d, \ldots) = 0.$$
>
> Multiplions entre elles toutes les équations semblables, que l'on obtient en permutant dans celles-ci toutes les lettres, la première seulement restant fixe; il viendra l'expression suivante:
>
> $$(V - \phi(a, b, c, d, \ldots))\ (V - \phi(a, c, b, d, \ldots))\ (V - \phi(a, b, d, c, \ldots)) \ldots,$$
>
> symétrique en b, c, d, etc., ..., laquelle pourra, par conséquent, s'écrire en fonction de a. Nous aurons donc une équation de la forme
>
> $$F(V, a) = 0.$$
>
> Or je dis que de la on peut tirer la valeur de a. Il suffit pour cela de chercher la solution commune a cette équation et a la proposée. Cette solution est la seule commune: car on ne peut avoir, par example,
>
> $$F(V, b) = 0$$
>
> sans quoi, cette équation ayant un facteur commun avec l'équation semblable, l'une des fonctions $\phi(a, \ldots)$ serait égale a l'une des fonctions $\phi(b, \ldots)$; ce qui est contre l'hypothése.
>
> Il suit de la que a s'exprime en fonction rationelle de V, et il en est de même des autres racines. [G, p. 49]

(This proof applies to any $V = \phi(a, b, c, \ldots)$, not just to one of the special form $V = Aa + Bb + Cc + \ldots$ Galois seems to make a slight slip when he speaks of *les équations semblables*, since he doubtless means the polynomials $V - \phi(Sa, Sb, Sc, \ldots)$, where S is a permutation of the roots with $Sa = a$, and these are not equations at all; however, he seems often to use "equation" to mean "polynomial", as, for example, in the first paragraphs of the memoir, where he speaks of "factors" of an equation.)

The irreducible polynomial $G(X)$ not only describes the splitting field of $f(x)$ (adjoin one root of $G(X)$ to K), it also describes the GALOIS group of $f(x)$ over K in the following way. Since $G(X)$ by construction is a factor of $F(X) = \Pi(X - V^{(i)})$ irreducible over K, $G(X)$ is equal to the product of a subset of the factors $X - V^{(i)}$, say $G(X) = (X - V)(X - V')(X - V'') \dots (X - V^{(n-1)})$. Each $V^{(i)}$ is of the form $V^{(i)} = AS(a) + BS(b) + CS(c) + \dots$ for a unique permutation S of the roots $a, b, c, \dots$, with V corresponding to the identity permutation. The set of these permutations as $V^{(i)}$ ranges over the roots of $G(X)$ is what GALOIS calls the group of the equation whose roots are $a, b, c, \dots$ It is not difficult to show that they form a group in the modern sense of the word. Moreover, the permutations of the roots that are obtained in this way are precisely those that are obtained by restricting *automorphisms of the splitting field which leave elements of K fixed* to the roots $a, b, c, \dots$. Today it is usual to regard the GALOIS group as being the group of automorphisms of the splitting field which leave elements of K fixed. GALOIS' view differs very little if at all from the modern view. For GALOIS, an element of the splitting field is "a function of the roots" (see part 1 of his demonstration of Proposition I). As such, it can be expressed as a rational function of V. Changing V to V' in this rational function is the same as changing a to $S(a)$, b to $S(b)$, etc., in the original function of the roots, where $V' = AS(a) + BS(b) + \dots$; that is, changing V to V' gives an automorphism of the splitting field which agrees with S on the roots $a, b, \dots$ (see also GALOIS' Lemma IV).

With the group of an equation so defined, and with its basic property described in Proposition I, GALOIS continues:

"Proposition II.

"Theorem. If one adjoins to a given equation the root r of an auxiliary irreducible equation [of prime degree p]

"(1) one of two things will happen: either the group of the equation will not be changed; or it will be partitioned into p groups, each belonging to the given equation respectively when one adjoins each of the roots of the auxiliary equation;

"(2) these groups will have the remarkable property that one will pass from one to the other in applying the same substitution of letters to all the permutations of the first." (My translation, quoted from Appendix A of my book.)

The words "of prime degree p" were stricken in GALOIS' last-minute revision. It is unthinkable that GALOIS intended by this deletion to *weaken* Proposition II, but this is what he did, because the deletion left p undefined in (1) and robbed (1) of any statement connecting the number of "groups" to the degree of the auxiliary equation; in fact, with the deletion, Proposition II no longer provides the information needed in the proof of Proposition V. I conclude that GALOIS meant to revise Proposition II to state what he undoubtedly knew to be true, namely, that the number of "groups" divides the degree of the auxiliary equation. Whether he meant p in (1) to be, as I said in the passage quoted above, the degree of the auxiliary equation, or whether he meant it to be the number of "groups", is beside the point. In either case, I still believe that the "*quelque chose à compléter*" is the proof of the (corrected) generalization of Proposition II to the case in which the degree of the auxiliary equation is not necessarily prime.

When K is extended to $K(r)$ by the adjunction of a single root r of an auxiliary equation $g(x) = 0$, the polynomial $G(X)$, which is irreducible over K, may factor. Let H be the monic factor of G irreducible over $K(r)$ of which V is a root. Since H has coefficients in $K(r)$, and since elements of $K(r)$ can be expressed as polynomials in r with coefficients in K, H can be expressed in the form $H = H(X, r)$ of a polynomial in X and r with coefficients in K. As follows directly from its definition, the GALOIS group of $f(x)$ over $K(r)$ contains $\deg_X H(X, r)$ permutations, and they correspond to those $V^{(i)}$ which satisfy $H(V^{(i)}, r) = 0$.

Similarly, any root r' of $g(x) = 0$ gives an extension $K(r')$ of K and $H(X, r')$ is a factor of $G(X)$ irreducible over $K(r')$ (as follows easily from GALOIS' Lemma I), so the GALOIS group of $f(x)$ over $K(r')$ contains $\deg_X H(X, r)$ permutations and they correspond to those $V^{(i)}$ which satisfy $H(V^{(i)}, r') = 0$. The original case of Proposition II, part (1) (namely, the case $p =$ prime) states, in essence, that $G(X)$ is the product of the $H(X, r')$ over all p roots r' of $g(x) = 0$. In the brief proof GALOIS gives of Proposition II in the case $p =$ prime, he simply states this as a fact; what argument he had in mind can only be conjectured. The factorization of $G(X)$ into factors of the form $H(X, r^{(i)})$ in the general case can be found as follows.

Note first that *two of the polynomials $H(X, r^{(i)})$ which have a root in common are identical.* For the proof of this lemma, let H be as above, let L be a splitting field of both $f(x)$ and $g(x)$, and let $r, r', r'', \ldots, r^{(p-1)}$ be the roots of g in L. All the polynomials under discussion have their coefficients in L. In his proof of part (2) of Proposition II, GALOIS states, with a clear indication of a proof included as a footnote, that if V is a root of $H(X, r)$ and if $\phi(V)$ is another (any root of $G(X)$ can be written in the form $\phi(V)$ where ϕ is a polynomial with coefficients in K) and if V' is a root of $H(V, r')$, then $\phi(V')$ is another root of $H(V, r')$. When $V = V'$, this says that if $H(X, r)$ and $H(X, r')$ have one root in common then every root of $H(X, r)$ is a root of $H(X, r')$. Since $H(X, r)$ and $H(X, r')$ have the same degree and are monic, the lemma follows.

As was noted above, for each root $r^{(i)}$ of g, $H(X, r^{(i)})$ is a factor of $G(X)$ (over $K(r^{(i)})$). Therefore, every root of $H(X, r^{(i)})$ is a root of $G(X)$. Let $h(X) = \Pi_i H(X, r^{(i)})$. Then $h(X)$ has coefficients in K (its coefficients are symmetric in the $r^{(i)}$) and its roots (it factors into linear, monic factors over L) are roots of $G(X)$. Since $G(X)$ is irreducible over K, and both $h(X)$ and $G(X)$ are monic, it follows that $h(X) = G(X)^k$ for some integer k. Any root V of G is a root of multiplicity k of the right hand side, so it is a root of multiplicity k of the left hand side. But $h(X)$ is a product of factors $H(X, r^{(i)})$ which have distinct roots (they are irreducible over $K(r^{(i)})$), so each V is a root of exactly k of these factors. It was just shown that two factors which have a root in common are identical, so it follows that the factors $H(X, r^{(i)})$ of $h(X)$ are equal in sets of k. If one takes a representative factor from each set, one obtains a set of p/k factors whose product is a monic polynomial, call it $P(X)$, whose roots are the roots of $G(X)$, each with multiplicity 1. Therefore, $P(X) = G(X)$. In short, *$G(X)$ is the product of the distinct polynomials $H(X, r^{(i)})$.* Moreover, *the number j of these factors divides p* because $j = p/k$.

Part (1) of Proposition II follows readily. The factorization of $G(X)$ just established partitions the roots of $G(X)$ into j subsets, where j divides p, and each subset corresponds to a root of g (in fact, to k roots of g, where $k = p/j$). Each subset describes the GALOIS group of the given equation over a $K(r^{(i)})$ in the same way that the roots of $G(X)$ describe its GALOIS group over K. (That GALOIS calls these subsets "groups" shows that he is not using the word entirely in the modern sense; a group in the modern sense cannot, of course, be partitioned into groups.) While I admit that this argument goes beyond what is explicitly contained in GALOIS' memoir — the proof has been "completed" slightly — I contend that it is not at all far-fetched to say that this proof is the sort of "completion" GALOIS had in mind.

Dr. JESPER LÜTZEN has pointed out an error in my translation of the proof of Proposition II. In the original version (p = prime) GALOIS said that $G(X)$ was $H(X, r) \cdot H(X, r') \cdot H(X, r'') \ldots$, "$r, r', r'', \ldots$ *étant les diverses valeurs de* r." In his revision, he changed "*les diverses*" to "*d'autres.*" Neither version is correctly translated by my phrase "the other values of r." The original version could perhaps be translated "the various values of r", and the revised version "certain values of r."

Dr. LÜTZEN has also challenged my statement, quoted above, that "Liouville found it necessary to circumvent Galois' proof entirely." On reconsideration, I agree with him, and I retract the statement. It was based on a too hasty reading of LIOUVILLE's note on the case p = prime published by BOURGNE & AZRA [G, p. 492]. Dr. LÜTZEN has made available to me preprints of portions of his forthcoming biography of LIOUVILLE [L], including transcriptions of and analyses of LIOUVILLE's notes on the case where p is not prime. These show clearly that LIOUVILLE's understanding of Proposition II was far better than I had thought.

It is worth noting that the above explication of Proposition II leads to an immediate proof of Proposition III, about which GALOIS in his haste said only "*On trouvera la démonstration.*" Adjoining *all* roots of g to K can be accomplished by adjoining a single root of a single irreducible auxiliary equation, call it g_1. (Indeed, GALOIS has shown that adjoining all roots of f is the same as adjoining one root of G, so it is only necessary to apply this construction to g instead of f and let g_1 be the resulting G.) For such an auxiliary equation, $K(r^{(i)})$ is the same for all i, because every root of g_1 can be expressed rationally in terms of every other. Since it was shown above that the "groups" into which the original group is partitioned by the adjunction of a root r of g_1 are presentations of the GALOIS groups of the given equation over the various fields $K(r^{(i)})$, and since these various fields coincide, it follows that, as groups of substitutions of the roots of the given equation, these groups are all the same, which is Proposition III.

Bibliography

[E] EDWARDS, HAROLD M., *Galois Theory*, Springer-Verlag, New York, 1984.

[G] GALOIS, ÉVARISTE, *Écrits et Mémoires Mathématiques*, R. BOURGNE & J.-P. AZRA, Eds., Gauthier-Villars, Paris, 1962.

[L] LÜTZEN, JESPER, *Joseph Liouville: Master of Pure and Applied Mathematics*, Springer-Verlag, to appear.

[N] NEUMANN, PETER M., Review of *Galois Theory* by HAROLD M. EDWARDS, American Mathematical Monthly, **93** (1986) pp. 407–411.

Courant Institute of
Mathematical Sciences
New York University

(Received October 25, 1989)