Galois Theory for Beginners

John Stillwell

Galois theory is rightly regarded as the peak of undergraduate algebra, and the modern algebra syllabus is designed to lead to its summit, usually taken to be the unsolvability of the general quintic equation. I fully agree with this goal, but I would like to point out that most of the equipment supplied—in particular normal extensions, irreducible polynomials, splitting fields and a lot of group theory—is unnecessary. The biggest encumbrance is the so-called "fundamental theorem of Galois theory." This theorem, interesting though it is, has little to do with polynomial equations. It relates the subfield structure of a normal extension to the subgroup structure of its group, and can be proved without use of polynomials (see, e.g., the appendix to Tignol [6]). Conversely, one can prove the unsolvability of polynomial equations without knowing about normality of field extensions or the Galois correspondence between subfields and subgroups.

The aim of this paper is to prove the unsolvability by radicals of the quintic (in fact of the general nth degree equation for $n \geq 5$) using just the fundamentals of groups, rings and fields from a standard first course in algebra. The main fact it will be necessary to know is that if ϕ is a homomorphism of group G onto group G' then $G' \cong G/\ker\phi$, and conversely, if $G/H \cong G'$ then H is the kernel of a homomorphism of G onto G'. The concept of Galois group, which guides the whole proof, will be defined when it comes up. With this background, a proof of unsolvability by radicals can be constructed from just three basic ideas, which will be explained more fully below:

1. Fields containing n indeterminates can be "symmetrized".
2. The Galois group of a radical extension is solvable.
3. The symmetric group S_n is not solvable.

When one considers the number of mathematicians who have worked on Galois theory, it is not possible to believe this proof is really new. In fact, all proofs seem to contain steps similar to the three just listed. Nevertheless, most of the standard approach had to be stripped away before the present proof became visible. I read the books of Edwards [2], Tignol [6], Artin [1], Kaplansky [3], MacLane and Birkhoff [5] and Lang [4], taught a course in Galois theory, and then discarded 90% of what I had learned.

I wish to thank my students, particularly Mark Kisin, for helpful suggestions and discussions which led to the writing of this paper. I am also grateful to the referee for several improvements.

THE GENERAL EQUATION OF DEGREE n. The goal of classical algebra was to express the roots of the general nth degree equation

$$(*) \qquad x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

in terms of the coefficients $a_0, \ldots, a_{n-1}$, using a finite number of operations $+, -, \times, \div$ and radicals $\sqrt{\ }, \sqrt[3]{\ }, \ldots$. For example, the roots x_1, x_2 of the general quadratic equation

$$x^2 + a_1 x + a_0 = 0$$

are expressed by the formula

$$x_1, x_2 = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0}}{2}.$$

Formulas for the roots of general cubic and quartic equations are also known, using cube roots as well as square roots. We say that these equations are *solvable by radicals*.

The set of elements obtainable from $a_0, \ldots, a_{n-1}$ by $+, -, \times, \div$ is the *field* $\mathbb{Q}(a_0, \ldots, a_{n-1})$. If we denote the roots of $(*)$ by $x_1, \ldots, x_n$, so that

$$(x - x_1) \cdots (x - x_n) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

then $a_0, \ldots, a_{n-1}$ are polynomial functions of $x_1, \ldots, x_n$ called the *elementary symmetric functions*:

$$a_0 = (-1)^n x_1 x_2 \ldots x_n, \ldots, a_{n-1} = -(x_1 + x_2 + \cdots + x_n).$$

The goal of solution by radicals is then to *extend* $\mathbb{Q}(a_0, \ldots, a_{n-1})$ *by adjoining radicals* until a field containing the roots $x_1, \ldots, x_n$ is obtained. For example, the roots x_1, x_2 of the quadratic equation lie in the extension of $\mathbb{Q}(a_0, a_1) = \mathbb{Q}(x_1 x_2, x_1 + x_2)$ by the radical

$$\sqrt{a_1^2 - 4a_0} = \sqrt{(x_1 + x_2)^2 - 4x_1 x_2} = \sqrt{(x_1 - x_2)^2} = \pm(x_1 - x_2).$$

In this case we get $\mathbb{Q}(x_1, x_2)$ itself as the radical extension $\mathbb{Q}(a_0, a_1, \sqrt{a_1^2 - 4a_0})$, though in other cases a radical extension of $\mathbb{Q}(a_0, \ldots, a_{n-1})$ containing $x_1, \ldots, x_n$ is larger than $\mathbb{Q}(x_1, \ldots, x_n)$. In particular, the solution of the cubic equation gives a radical extension of $\mathbb{Q}(a_0, a_1, a_2)$ which includes imaginary cube roots of unity as well as x_1, x_2, x_3.

In general, adjoining an element α to a field F means forming the closure of $F \cup \{\alpha\}$ under $+, -, \times, \div$ (by a non-zero element), i.e., taking the intersection of all fields containing $F \cup \{\alpha\}$. The adjunction is called *radical* if some positive integer power α^m of α equals an element $f \in F$, in which case α may be represented by the radical expression $\sqrt[m]{f}$. The result $F(\alpha_1)(\alpha_2) \ldots (\alpha_k)$ of successive adjunctions is denoted by $F(\alpha_1, \ldots, \alpha_k)$ and if each adjunction is radical we say $F(\alpha_1, \ldots, \alpha_k)$ is a *radical extension of* F.

It is clear from these definitions that a radical extension E of $\mathbb{Q}(a_0, \ldots, a_{n-1})$ containing $x_1, \ldots, x_n$ is also a radical extension of $\mathbb{Q}(x_1, \ldots, x_n)$, since $a_0, \ldots, a_{n-1} \in \mathbb{Q}(x_1, \ldots, x_n)$. Thus we also have to study radical extensions of $\mathbb{Q}(x_1, \ldots, x_n)$. The most important property of $\mathbb{Q}(x_1, \ldots, x_n)$ is that it is *symmetric* with respect to $x_1, \ldots, x_n$, in the sense that any permutation σ of $x_1, \ldots, x_n$ extends to a bijection σ of $\mathbb{Q}(x_1, \ldots, x_n)$ defined by

$$\sigma f(x_1, \ldots, x_n) = f(\sigma x_1, \ldots, \sigma x_n)$$

for each rational function f of $x_1, \ldots, x_n$. Moreover, this bijection σ obviously satisfies

$$\sigma(f+g) = \sigma f + \sigma g,$$

$$\sigma(fg) = \sigma f \cdot \sigma g,$$

and hence is an *automorphism* of $\mathbb{Q}(x_1, \dots, x_n)$.

A radical extension E of $\mathbb{Q}(x_1, \dots, x_n)$ is not necessarily symmetric in this sense. For example, $\mathbb{Q}(x_1, \dots, x_n, \sqrt{x_1})$ contains a square root of x_1, but not of x_2, hence there is no automorphism exchanging x_1 and x_2. However, we can restore symmetry by adjoining $\sqrt{x_2}, \dots, \sqrt{x_n}$ as well. The obvious generalization of this idea gives a way to "symmetrize" any radical extension E of $\mathbb{Q}(x_1, \dots, x_n)$:

Theorem 1. *For each radical extension E of $\mathbb{Q}(x_1, \dots, x_n)$ there is a radical extension $\overline{E} \supseteq E$ with automorphisms σ extending all permutations of $x_1, \dots, x_n$.*

Proof: For each adjoined element, represented by radical expression $e(x_1, \dots, x_n)$, and each permutation σ of $x_1, \dots, x_n$, adjoin the element $e(\sigma x_1, \dots, \sigma x_n)$. Since there are only finitely many permutations σ, the resulting field $\overline{E} \supseteq E$ is also a radical extension of $\mathbb{Q}(x_1, \dots, x_n)$.

This gives a bijection (also called σ) of $\overline{E}$ sending each $f(x_1, \dots, x_n) \in \overline{E}$ (a rational function of $x_1, \dots, x_n$ and the adjoined radicals) to $f(\sigma x_1, \dots, \sigma x_n)$, and this bijection is obviously an automorphism of $\overline{E}$, extending the permutation σ. ■

The reason for wanting an automorphism σ extending each permutation of $x_1, \dots, x_n$ is that $a_0, \dots, a_{n-1}$ are fixed by such permutations, and hence so is every element of the field $\mathbb{Q}(a_0, \dots, a_{n-1})$. If $E \supseteq F$ are any fields, the automorphisms σ of E fixing all elements of F form what is called the *Galois group of E over F*, $\mathrm{Gal}(E/F)$. This concept alerts us to the following corollary of Theorem 1:

Corollary. *If E is a radical extension of $\mathbb{Q}(a_0, \dots, a_{n-1})$ containing $x_1, \dots, x_n$ then there is a further radical extension $\overline{E} \supseteq E$ such that* $\mathrm{Gal}(\overline{E}/\mathbb{Q}(a_0, \dots, a_{n-1}))$ *includes automorphisms σ extending all permutations of $x_1, \dots, x_n$.*

Proof: This is immediate from Theorem 1 and the fact that a radical extension of $\mathbb{Q}(a_0, \dots, a_{n-1})$ containing $x_1, \dots, x_n$ is also a radical extension of $\mathbb{Q}(x_1, \dots, x_n)$. ■

THE STRUCTURE OF RADICAL EXTENSIONS. So far we know that a solution by radicals of the general nth degree equation $(*)$ entails a radical extension of $\mathbb{Q}(a_0, \dots, a_{n-1})$ containing $x_1, \dots, x_n$, and hence a radical extension $\overline{E}$ with the symmetry described in the corollary above. This opens a route to prove *non-existence* of such a solution by learning enough about $\mathrm{Gal}(\overline{E}/\mathbb{Q}(a_0, \dots, a_{n-1}))$ to show that such symmetry is lacking, at least for $n \geq 5$. In the present section we shall show that the Galois group $\mathrm{Gal}(F(\alpha_1, \dots, \alpha_k)/F)$ of any radical extension has a special structure, called *solvability*, inherited from the structure of $F(\alpha_1, \dots, \alpha_k)$. Then in the next section we shall show that this structure is indeed incompatible with the symmetry described in the corollary. To simplify the derivation of this structure, we shall show that certain assumptions about the adjunction of radicals α_i can be made without loss of generality.

First, we can assume that each radical α_i adjoined is a pth root for some *prime* p. E.g., instead of adjoining $\sqrt[6]{\alpha}$ we can adjoin first $\sqrt{\alpha} = \beta$, then $\sqrt[3]{\beta}$. Second, if α_i

is a pth root we can assume that $F(\alpha_1, \dots, \alpha_i)$ contains no pth roots of unity not in $F(\alpha_1, \dots, \alpha_{i-1})$ unless α_i itself is a pth root of unity. If this is not the case initially we simply adjoin a pth root of unity $\zeta \neq 1$ to $F(\alpha_1, \dots, \alpha_{i-1})$ *before* adjoining α_i (in which case $F(\alpha_1, \dots, \alpha_{i-1}, \zeta)$ contains all the pth roots of unity: $1, \zeta, \zeta^2, \dots, \zeta^{p-1}$). With both these modifications the final field $F(\alpha_1, \dots, \alpha_k)$ is the same, and it remains the same if the newly adjoined roots ζ are included in the list $\alpha_1, \dots, \alpha_k$. Hence we have:

Any radical extension $F(\alpha_1, \dots, \alpha_k)$ is the union of an ascending tower of fields

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k = F(\alpha_1, \dots, \alpha_k)$$

where each $F_i = F_{i-1}(\alpha_i)$, α_i is the p_i-th root of an element in F_{i-1}, p_i is prime, and F_i contains no p_i-th roots of unity not in F_{i-1} unless α_i is itself a p_i-th root of unity.

Corresponding to this tower of fields we have a descending tower of groups

$$\mathrm{Gal}(F_k/F_0) = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_k = \mathrm{Gal}(F_k/F_k) = \{\mathbf{1}\}$$

where $G_i = \mathrm{Gal}(F_k/F_i) = \mathrm{Gal}(F_k/F_{i-1}(\alpha_i))$ and $\mathbf{1}$ denotes the identity automorphism. The containments are immediate from the definition of $\mathrm{Gal}(E/B)$, for any fields $E \supseteq B$, as the group of automorphisms of E fixing each element of B. As B increases to E, $\mathrm{Gal}(E/B)$ must decrease to $\{\mathbf{1}\}$. The important point is that the step from G_{i-1} to its subgroup G_i, reflecting the adjunction of the p_i-th root α_i to F, is "small" enough to be describable in group-theoretic terms: *G_i is a normal subgroup of G_{i-1}, and G_{i-1}/G_i is abelian*, as we shall now show.

To simplify notation further we set

$$E = F_k,\ B = F_{i-1},\ \alpha = \alpha_i,\ p = p_i,$$

so the theorem we want is:

Theorem 2. *If $E \supseteq B(\alpha) \supseteq B$ are fields with $\alpha^p \in B$ for some prime p, and if $B(\alpha)$ contains no pth roots of unity not in B unless α itself is a pth root of unity, then* $\mathrm{Gal}(E/B(\alpha))$ *is a normal subgroup of* $\mathrm{Gal}(E/B)$ *and* $\mathrm{Gal}(E/B)/\mathrm{Gal}(E/B(\alpha))$ *is abelian.*

Proof: By the homomorphism theorem for groups, it suffices to find a homomorphism of $\mathrm{Gal}(E/B)$, with kernel $\mathrm{Gal}(E/B(\alpha))$, into an abelian group (i.e., onto a subgroup of an abelian group, which of course is also abelian). The obvious map with kernel $\mathrm{Gal}(E/B(\alpha))$ is *restriction to $B(\alpha)$*, $|_{B(\alpha)}$, since by definition

$$\sigma \in \mathrm{Gal}(E/B(\alpha)) \Leftrightarrow \sigma|_{B(\alpha)} \text{ is the identity map.}$$

The homomorphism property,

$$\sigma'\sigma|_{B(\alpha)} = \sigma'|_{B(\alpha)}\sigma|_{B(\alpha)} \quad \text{for all } \sigma', \sigma \in \mathrm{Gal}(E/B),$$

is automatic provided $\sigma|_{B(\alpha)}(b) \in B(\alpha)$ for each $b \in B(\alpha)$, i.e. provided $B(\alpha)$ is closed under each $\sigma \in \mathrm{Gal}(E/B)$.

Since σ fixes B, $\sigma|_{B(\alpha)}$ is completely determined by the value $\sigma(\alpha)$. If α is a pth root of unity ζ then

$$(\sigma(\alpha))^p = \sigma(\alpha^p) = \sigma(\zeta^p) = \sigma(1) = 1,$$

hence $\sigma(\alpha) = \zeta^i = \alpha^i \in B(\alpha)$, since each pth root of unity is some ζ^i. If α is not a root of unity then

$$(\sigma(\alpha))^p = \sigma(\alpha^p) = \alpha^p \quad \text{since} \quad \alpha^p \in B,$$

hence $\sigma(\alpha) = \zeta^j \alpha$ for some pth root of unity ζ, and $\zeta \in B$ by hypothesis, so again $\sigma(\alpha) \in B(\alpha)$. Thus $B(\alpha)$ is closed as required.

This also implies that $|_{B(\alpha)}$ maps $\mathrm{Gal}(E/B)$ into $\mathrm{Gal}(B(\alpha)/B)$, so it now remains to check that $\mathrm{Gal}(B(\alpha)/B)$ is abelian. If α is a root of unity then, as we have just seen, each $\sigma|_{B(\alpha)} \in \mathrm{Gal}(B(\alpha)/B)$ is of the form σ_i, where $\sigma_i(\alpha) = \alpha^i$, hence

$$\sigma_i \sigma_j(\alpha) = \sigma_i(\alpha^j) = \alpha^{ij} = \sigma_j \sigma_i(\alpha).$$

Likewise, if α is not a root of unity then each $\sigma|_{B(\alpha)} \in \mathrm{Gal}(B(\alpha)/B)$ is of the form σ_i where $\sigma_i(\alpha) = \zeta^i \alpha$, hence

$$\sigma_i \sigma_j(\alpha) = \sigma_i(\zeta^j \alpha) = \zeta^{i+j}\alpha = \sigma_j \sigma_i(\alpha)$$

since $\zeta \in B$ and therefore ζ is fixed. Hence in either case $\mathrm{Gal}(B(\alpha)/B)$ is abelian. ■

The property of $\mathrm{Gal}(F(\alpha_1, \dots, \alpha_k)/F)$ implied by this theorem, that it has subgroups $\mathrm{Gal}(F(\alpha_1, \dots, \alpha_k)/F) = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_k = \{1\}$ with each G_i normal in G_{i-1} and G_{i-1}/G_i abelian, is called *solvability* of $\mathrm{Gal}(F(\alpha_1, \dots, \alpha_k)/F)$.

NON-EXISTENCE OF SOLUTIONS BY RADICALS WHEN $n \geq 5$. As we have said, this amounts to proving that a radical extension of $\mathbb{Q}(a_0, \dots, a_{n-1})$ does not contain $x_1, \dots, x_n$ or, equivalently, $\mathbb{Q}(x_1, \dots, x_n)$. We have now reduced this problem to proving that the symmetry of the hypothetical extension $\overline{E}$ containing $x_1, \dots, x_n$, given by the corollary to Theorem 1, is incompatible with the solvability of $\mathrm{Gal}(\overline{E}/\mathbb{Q}(a_0, \dots, a_{n-1}))$, given by Theorem 2. Our proof looks only at the effect of the hypothetical automorphisms of $\overline{E}$ on $x_1, \dots, x_n$, and hence it is really about the *symmetric group* S_n of all permutations of $x_1, \dots, x_n$. In fact, we are adapting a standard proof that S_n is not a solvable group, given by Milgram in his appendix to Artin [1].

Theorem 3. *A radical extension of* $\mathbb{Q}(a_0, \dots, a_{n-1})$ *does not contain* $\mathbb{Q}(x_1, \dots, x_n)$ *when* $n \geqslant 5$.

Proof: Suppose on the contrary that E is a radical extension of $\mathbb{Q}(a_0, \dots, a_{n-1})$ which contains $\mathbb{Q}(x_1, \dots, x_n)$. Then E is also a radical extension of $\mathbb{Q}(x_1, \dots, x_n)$ and by the corollary to Theorem 1 there is a radical extension $\overline{E} \supseteq E$ such that $G_0 = \mathrm{Gal}(\overline{E}/\mathbb{Q}(a_0, \dots, a_{n-1}))$ includes automorphisms σ extending all permutations of $x_1, \dots, x_n$.

By Theorem 2, G_0 has a decomposition

$$G_0 \supseteq G_1 \supseteq \cdots \supseteq G_k = \{1\}$$

where each G_{i+1} is a normal subgroup of G_i and G_{i-1}/G_i is abelian. We now show that this is contrary to the existence of the automorphisms σ.

Since G_{i-1}/G_i is abelian, G_i is the kernel of a homomorphism of G_{i-1} onto an abelian group, and therefore

$$\sigma, \tau \in G_{i-1} \Rightarrow \sigma^{-1}\tau^{-1}\sigma\tau \in G_i.$$

We use this fact to prove by induction on i that, if $n \geq 5$, each G_i contains automorphisms σ extending all 3-cycles (x_a, x_b, x_c). This is true for G_0 by hypothesis, and when $n \geq 5$ the property persists from G_{i-1} to G_i because

$$(x_a, x_b, x_c) = (x_d, x_a, x_c)^{-1}(x_c, x_e, x_b)^{-1}(x_d, x_a, x_c)(x_c, x_e, x_b)$$

where a, b, c, d, e are distinct. Thus if there are at least five indeterminates x_j, there are σ in each G_i which extend arbitrary 3-cycles (x_a, x_b, x_c), and this means in particular that $G_k \neq \{1\}$. This contradiction shows that $\mathbb{Q}(x_1, \ldots, x_n)$ is not contained in any radical extension of $\mathbb{Q}(a_0, \ldots, a_{n-1})$ when $n \geq 5$. ∎

REFERENCES

1. E. Artin, *Galois Theory*, Notre Dame, 1965.
2. H. M. Edwards, *Galois Theory*, Springer-Verlag, New York, 1984.
3. I. Kaplansky, *Fields and Rings*, University of Chicago Press, 1969.
4. S. Lang, *Undergraduate Algebra*, Springer-Verlag, New York, 1987.
5. S. MacLane & G. Birkhoff, *Algebra*, 2nd ed, Collier Macmillan, New York, 1979.
6. J.-P. Tignol, *Galois' Theory of Algebraic Equations*, Longman, New York, 1988.

Department of Mathematics
Monash University
Clayton 3168
Australia

PICTURE PUZZLE
(from the collection of Paul Halmos)

This famous topologist was usually considered more scary than scared.
(see page 86.)