GALOIS THE HECK IS GOING ON?
JUNE

RAYMOND FRIEND

Abstract. What good is Group Theory? These are the fruits of your labor, young undergraduate.

Contents

1. Introduction

This paper was another excruciatingly difficult one on which to focus, because I did not realize I wanted to write on this subject until after having read most of the material! From scouring MASS lecture notes to searching Wikipedia for basic definitions to watching YouTube for ten hours just to find a "succinct" way to prove some lemmas, I have tried my best to discern between the seven various versions of *solvability*. I may have inadvertantly avoided some important details such as providing alternate definitions to a solvable group or perhaps mentioning that some extension of a field required ample roots of unity for a proof to be valid, but it is pretty close to the truth.

2. Manifestools

Definition 2.1. A subgroup $H \leq G$ is *normal* if and only if conjugation by G fixes H, or

$$H \triangleleft G \qquad \text{iff} \qquad ghg^{-1} \in H \text{ for all } g \in G, h \in H.$$

Definition 2.2. A group G is *solvable* if it has a finite series of subgroups

$$1 = G_0 \leq G_1 \leq ... \leq G_n = G$$

such that $G_i \triangleleft G_{i+1}$ and G_{i+1}/G_i is abelian for $0 \leq i < n$.

We have two isomorphism theorems as well.

Date: June 28, 2017.

Lemma 2.3. *If $H \lhd G$ and $A \leq G$, then*

$$H \cap A \lhd A \qquad \text{and} \qquad \frac{A}{H \cap A} = \frac{HA}{H}.$$

If we further have the properties that $H \leq A \lhd G$, then

$$H \lhd A, \qquad A/H \lhd G/H, \qquad \text{and} \qquad \frac{G/H}{A/H} = \frac{G}{A}.$$

Now we wish to use our lemma to prove some facts about solvability.

Theorem 2.4. *If G is a group and $H \leq G$ and $N \lhd G$, then*

(1) *G is solvable implies H is solvable;*
(2) *G is solvable implies G/N is solvable;*
(3) *G/N and N are solvable imply G is solvable.*

Proof. (1) We have by G solvable that there exists G_i satisfying the conditions in the definition of solvable. Let $H_i = G_i \cap H$. Then the tower $1 = H_0 \lhd H_1 \lhd ... \lhd H_n = H$ is a normal series. We wish to show the abelian property too. Notice by use of the first isomorphism theorem,

$$\frac{H_{i+1}}{H_i} = \frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{G_i \cap (G_{i+1} \cap H)} \simeq \frac{G_i(G_{i+1} \cap H)}{G_i} \leq \frac{G_{i+1}}{G_i}.$$

The quotient H_{i+1}/H_i is a subgroup of the abelian G_{i+1}/G_i, so it too is abelian. So H is solvable.

(2) We have by G solvable that there exists G_i satisfying the conditions in the definition of solvable. Using the fact that the product of two normal subgroups is still a normal subgroup, we have G_iN is normal; but $GN = G$. Then take each subgroup in the series and quotient by N to get

$$N/N = G_0N/N \lhd G_1N/N \lhd ... \lhd G_nN/N = G/N.$$

By the previous lemma,

$$\frac{G_{i+1}N/N}{G_iN/N} = \frac{G_{i+1}N}{G_iN} = \frac{G_{i+1}(G_iN)}{G_iN} \simeq \frac{G_{i+1}}{G_{i+1} \cap (G_iN)}$$
$$\simeq \frac{G_{i+1}/G_i}{(G_{i+1} \cap (G_iN))/G_i} \leq \frac{G_{i+1}}{G_i} \text{ abelian.}$$

(3) We have two series $1 = N_0 \lhd N_1 \lhd ... \lhd N_m = N$ and $N/N = G_0/N \lhd G_1/N \lhd ... \lhd G_n/N = G/N$. We can construct the series

$$1 = N_0 \lhd N_1 \lhd ... \lhd N_m = N = G_0 \lhd G_1 \lhd ... \lhd G_n = G.$$

This is a normal series because the quotients N_{i+1}/N_i are abelian, and

$$\frac{G_{i+1}}{G_i} \simeq \frac{G_{i+1}/N}{G_i/N} \text{ abelian.}$$

□

Now we can move on to establishing some of the facts that will help in coming to a contradiction on the solvability of all polynomials.

Definition 2.5. Group G is *simple* if and only if its only normal subgroups are 1 and G.

For example, for any prime p, the cyclic group $\mathbb{Z}_p$ or $\mathbb{Z}/p\mathbb{Z}$ is simple, but since $1 \triangleleft \mathbb{Z}_p$ is a normal series with an abelian quotient congruent to $\mathbb{Z}_p$, it is also solvable. Actually, all non-abelian, simple groups are not solvable, and every *perfect* group (or a group equal to its own commutator subgroup) is not solvable.

Theorem 2.6. *A solvable group G is simple if and only if it is cyclic of prime order.*

Proof. Suppose G is simple. Then we have G_i satisfying the given criteria. Deleting any repeats we may find in that series, we get the minimal $G_{i+1} \neq G_i$. Thus, G_{n-1} is a proper subgroup of G, but since G is simple, $G_{n-1} = 1$ and $G = G_n/G_{n-1}$ is abelian, yet every subgroup of G is normal and every element of G generates a cyclic group. Since G does not have any nontrivial proper subgroups, it must be the case that G is cyclic of prime order. Obviously, a cyclic group of prime order is simple. □

Proposition 2.7. *The symmetric group S_n is solvable for $n < 5$.*

Proof. The smallest symmetric groups S_1 and S_2 are trivially solvable. Also, one can check that the subgroup $\langle (123) \rangle \simeq \mathbb{Z}_3$ is of index 2 in S_3 and is, therefore, normal. Hence, we have the composition series

$$1 \triangleleft \langle (123) \rangle \triangleleft S_3,$$

with the quotients $\mathbb{Z}_2$ and $\mathbb{Z}_3$ respectively, so S_3 is solvable. Finally, consider A_4, a subgroup of index 2 in S_4, so $A_4 \triangleleft S_4$. Now let $\mathbb{V} = \{1, (12)(34), (13)(24), (14)(23)\}$, the Klein group. $\mathbb{V} \triangleleft S_4$, so $\mathbb{V} \triangleleft A_4$. Furthermore, since $\#A_4 = 12$ and $\#\mathbb{V} = 4$, it must be that $A_4/\mathbb{V} \simeq \mathbb{Z}_3$. And since $A_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, we see that we have the following composition series for S_4:

$$1 \triangleleft \mathbb{Z}_2 \triangleleft \mathbb{V} \triangleleft A_4 \triangleleft S_4,$$

with the abelian quotients $\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_2$ respectively, meaning S_4 is solvable. □

Theorem 2.8. *For $n \geq 5$, the alternating group A_n is simple.*

Corollary 2.9. *The symmetric group S_n is not solvable for $n \geq 5$.*

Proof. We know a subgroup of a solvable group is solvable, so if S_n is solvable, so is A_n. But A_n is simple, so it is cyclic of prime order. However, $|A_n| = \frac{n!}{2}$ which is not prime for $n \geq 5$. □

Notice A_n is generated by 3-cycles $(abc) = (ac)(ab)$. This is a standard fact. A sketch of the proof is as follows: show every product of two transpositions is a product of 3-cycles; since A_n is the set of every product of an even number of transpositions, we will have proven the statement. Take σ, τ transpositions that switch a common element $a \in \{1, ..., n\}$. Then they are of the form $\sigma = (ab), \tau = (ac)$, so $\sigma\tau = (ab)(ac) = (acb)$. Now suppose σ and τ transpose distinct elements. Then $\sigma = (ab), \tau = (cd)$, and $\sigma\tau = (ab)(cd) = (dac)(abd)$. A direct corollary of this fact is that A_n is generated by m-cycles for any odd number $3 \leq m \leq n$, based on the identity

$$(a_1 a_2 a_3) = (a_2 a_1 a_3 a_4 ... a_m)(a_m a_{m-1} ... a_4 a_3 a_2 a_1).$$

Proposition 2.10. *Consider nontrivial $1 \neq N \triangleleft A_n$.*

(1) If N contains a 3-cycle then it contains all 3 cycles, so $N = A_n$.

(2) N contains a 3-cycle.

Proof. (1) Without loss of generality, suppose N contains the cycle (123). We will show for any $k > 3$ that $(32k) \in A_n$. Notice, since N is a normal subgroup, we have in particular that

$$(32k)^{-1}(123)(32k) = (1k2) \implies (1k2) \in N.$$

Squaring, we get $(1k2)^2 = (12k) \in N$ for all $k > 3$. If $n > 3$, then let $a, b \geq 3$. The permutation $(1a)(1b)$ is even so exists in A_n. By closure under conjugation of N,

$$((1a)(1b))^{-1}(12k)((1a)(1b)) = (abk) \in N.$$

(2) The second part requires a case-by-case proof that I will omit but is standard.

□

Proof of Theorem 2.8. Any nontrivial normal subgroup of A_n is exactly A_n, meaning A_n is trivial. □

3. Galois' Up? Radical!

Suppose that E is an extension of the field F, written also as E/F. The extension E/F is said to be *normal* if every irreducible polynomial over F either has no root in E or splits into linear factors in E. The extension E/F is said to be *separable* if for all $\alpha \in E$, the minimal polynomial of α over F is a separable polynomial (i.e. the minimal polynomial is square-free over E). Together, normality and separability are equivalent to E/F being a *Galois extension.*

Definition 3.1. An automorphism of E/F is defined to be an automorphism (isomorphism from E to E) of E that fixes F pointwise. The set of all automorphisms of E/F forms a group with the operation of function composition, called $\mathrm{Aut}(E/F)$. If E/F is a Galois extension, then $\mathrm{Aut}(E/F)$ is called the *Galois group* of E over F, and is denoted by $\mathrm{Gal}(E/F)$.

There are multiple options for conditions we can assume for the remainder of this paper, including the simpler condition: let $char F = 0$. But we could also assume that all extensions we consider are separable and their degrees are not divisible by their characteristic.

Definition 3.2. Let E/F be a finite field extension.

- The extension E/F is called *solvable* if there exists a Galois extension D/F containing E with a solvable Galois group.
- The extension E/F is *solvable in radicals* if there exists a tower

$$F = D_0 \subset D_1 \subset ... \subset D_r$$

such that $E \subset D_r$ and such that $D_i = D_{i-1}(\sqrt[n_i]{a_i})$ for some $a_i \in D_{i-1}$.

Now we aim to establish an equivalence between these two notions of solvability.

Theorem 3.3. *E/F is solvable if and only if it is solvable in radicals.*

Proof. All fields in this proof will be subfields of the fixed algebraic closure of F. So let E/F be solvable. Then let D/F be the Galois extension containing E with a solvable Galois group G of order n. Let $F(\zeta_n)$ be the splitting field of $x^n - 1$, with ζ_n being the n-th root of unity, a solution to the polynomial. In the figure below, consider the first diagram of fields. From the following lemma, $D(\zeta_n)/F(\zeta_n)$ is a

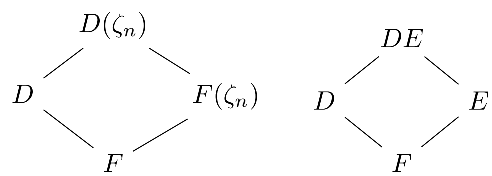


FIGURE 1. Field Extension Diagrams

Galois extension and its Galois group H is isomorphic to $\mathrm{Gal}(D/(D \cap F(\zeta_n))) \leq G$. So H is solvable.

Lemma 3.4. *Let $D \subset \overline{F}$ be a finite Galois extension of F and let $E \subset \overline{F}$ be any finite extension of F. With view of the second diagram above, the composite field DE is Galois over E and the Galois group Gal(DE/E) is isomorphic to Gal$(D/(D \cap E))$.*

A cyclic tower of subgroups $H = H_1 \supset H_2 \supset ... \supset H_r = 1$ gives rise to a tower of subfields

$$F(\zeta_n) = J_1 \subset ... \subset J_r = D(\zeta_n),$$

where $J_i = D(\zeta_n)^{H_i}$. By the main theorem of Galois theory, $D(\zeta_n)/J_i$ is Galois with a Galois group H_i. Since H_{i+1} is normal in H_i, J_{i+1}/J_i is a Galois extension with Galois group H_i/H_{i+1}, which is cyclic. Since J_{i+1}/J_i is a cyclic extension of degree $d \mid n$ (by Lagrange theorem), and J_i contains n-th roots of unity, we can apply a theorem (4.3.1 of Tevelev) showing on each step $J_{i+1} = J_i(\alpha)$ where some power of α belongs to J_{i-1}. Thus, E/F is solvable in radicals.
Conversely, we can suppose E/F is solvable in radicals, i.e. E is contained in a field D that admits a tower

$$F \subset D_1 \subset ... \subset D_r = D$$

such that one each step $D_i = D_{i-1}(\alpha)$ where $\alpha^k \in D_{i-1}$ for some k. Let n be the least common multiple of all of the k's that appear. Consider the tower of fields

$$F \subset F(\zeta_n) \subset D_1(\zeta_n) \subset ... \subset D_r(\zeta_n) = M,$$

where each consecutive embedding is Galois with and abelian Galois group on the first step and a cyclic Galois group for the remaining steps. However, M/F is not necessarily Galois. Let $g_1, ..., g_k : M \to \overline{F}$ be the list of all embeddings over F, where g_1 is the identity. Each of the embeddings $g_1(M) \subset \overline{F}$ has the same property as above: in the corresponding tower

$$F \subset g_i(F(\zeta_n)) \subset g_i(D_1(\zeta_n)) \subset ... \subset g_i(M),$$

each consecutive embedding is Galois with an abelian Galois group. Notice that the composite field $\mathcal{M} = g_1(M) \cdots g_k(M)$ is Galois over F and admits a tower of field extensions:

$$F \subset g_1(M) \subset g_1(M)g_2(M) \subset ... \subset g_1(M) \cdots g_k(M) = \mathcal{M}.$$

Consider the i-th step of this tower

$$N \subset N g_i(M),$$

where $N = g_1(M) \cdots g_{i-1}(M)$. We can refine this inclusion of fields by taking a composite of the tower for F above with N. By the lemma, each consecutive embeddings in this tower is Galois with an abelian Galois group. By the main theorem of Galois theory, this tower of subfields of $\mathcal{M}$ corresponds to an abelian filtration of $\mathrm{Gal}(\mathcal{M}/F)$. Therefore this group is solvable. □

For some polynomial $f \in F[x]$, we call it solvable if its Galois group is solvable, and solvable in radicals if for any root β of $f(x)$ in $\overline{F}$, there exists a tower

$$F = D_0 \subset ... \subset D_r$$

such that $\beta \in D_r$ and such that $D_i = D_{i-1}(\sqrt[n_i]{a_i})$ for some $a_i \in D_{i-1}$. By the theorem, these two notions are equivalent.

Proposition 3.5. *Any polynomial $f(x) \in \mathbb{Q}[x]$ of degree less than 5 is solvable in radicals.*

Proof. Without loss of generality, we may consider only irreducible polynomials of degree less than 5, since all reducible polynomials are products of irreducible ones. Assume f is monic as well. Let E be the splitting field of f and let $a_1, ..., a_n$ be the roots of f in $\overline{\mathbb{Q}}$. Then any $\mathbb{Q}$-automorphism of E consists simply in permuting the a_i, so we see that $\mathrm{Gal}(E/\mathbb{Q})$ is a subgroup of S_n. Since any subgroup of a solvable group is solvable and an irreducible polynomial is $\mathbb{Q}[x]$ is solvable by radicals if and only if the Galois group of its splitting field is solvable, we see that general f is solvable if and only if S_n is solvable (assuming some f can obtain Galois group S_n for each n). We already proved that S_1, S_2, S_3, and S_4 are solvable groups. Therefore, f is solvable in radicals. □

However, S_5 is not solvable, because the only

4. Still Abel to Do It without Galois

When Abel published his first proof of the theorem that the general equation of the fifth degree cannot be solved in radicals in 1824, he had little to use from Galois theory, since Galois was only thirteen years old at the time. I will present his formulations as well.

Recall if F is a field and $f \in F[x]$ is monic, then let

$$f(x) = (x - x_1)(x - x_2) \cdots (x - x_n)$$

in some extension field of F, called the splitting field of f over F: $E = F(x_1, x_2, ..., x_n)$. A finite algebraic extension D/F is called a radical tower over F if there is a series of intermediate fields

$$F = D_0 \subset D_1 \subset ... \subset D_m = D$$

such that for each $0 \leq i \leq m$, $D_{i+1}\left(\sqrt[p_i]{\alpha_i}\right)$ where p_i is prime and $\alpha_i \in D_i^\times$. For a polynomial f to solvable in radicals, there must exist a radical tower D/F such that $E \subset D$. We may restrict our attention to irreducible, monic polynomials, whose splitting field to which we may assign a Galois group G_f. These are certain transitive subgroups of the group of permutations of the roots of $f(x)$.

Definition 4.1 (Alternative Solvable Group)**.** Finite group G is solvable if there is a sequence of subgroups

$$(e) = G_0 \subset G_1 \subset ... \subset G_m = G$$

such that G_i is normal in G_{i+1} and $p_{i+1} = [G_{i+1} : G_i]$ is prime for $0 \leq i < m$.

Theorem 4.2 (Galois)**.** *Polynomial $f \in F[x]$ is solvable in radicals if and only if the Galois group of E/F is solvable.*

Let F be a field of characteristic zero, and let $s_1, s_2, ..., s_n$ be algebraically independent over F. Set $F' = F(s_1, s_2, ..., s_3)$. Now let the general equation of degree n over F' be

$$f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^n s_n \in F'[x].$$

If $f(x) = (x - \theta_1)(x - \theta_2) \cdots (x - \theta_n)$ in some extension E/F', then E is a splitting field for $f(x)$ over F'. Generally, the roots $x_1, ..., x_n$ are algebraically independent over F', and each s_i is an elementary symmetric function of the x_j:

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots + x_n \\ s_2 &= x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n \\ &\vdots \\ s_i &= \sum_{1 \leq k_1 < ... < k_i \leq n} \prod_{j=1}^{i} x_{k_j} \\ &\vdots \\ s_n &= x_1 x_2 \cdots x_n. \end{aligned}$$

Each permutation of the x_i induces an automorphism of E which leaves F' fixed pointwise; and the only elements of E fixed by all such automorphisms are the elements of F'. Thus, E/F' is a Galois extension with Galois group isomorphic to S_n, or S_n is the Galois group of the general equation of degree n over k. Abel, Ruffini, Vandermonde, Lagrange, and the like had all of this to work with, but were missing the notion of a normal subgroup, so could not formulate a solvable group.

Theorem 4.3 (Abel)**.** *Let $f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^n s_n$ be the general equation of degree n over F'. If $n \geq 5$, then this equation is not solvable in radicals.*

Proof. Abel proceeded with two steps to his proof.

- *Claim 1*: If E is contained in a radical tower D over F', then E/F' is itself a radical tower.
- *Claim 2*: If $n \geq 5$, then E/F' is not a radical tower.

Actually, Abel restricted himself to proving Claim 2 only when $n = 5$. Abel's noteworthy contributions mostly came from his proof of Claim 1, which Ruffini likely thought was inessential. First, let us denote that for an element $\sigma \in S_n$

$$(\sigma f)(x_1, ..., x_n) = f(x_{\sigma(1)}, ..., x_{\sigma(n)}).$$

Now define these two quantities (determinant and its square root)

$$\delta = \prod_{i<j}(x_i - x_j) \qquad \text{and} \qquad \Delta = \delta^2.$$

We notice for some $\sigma \in S_n$, $\sigma\delta = \pm\delta$. The sign on δ changes for each transposition in σ, so A_n preserves δ while its opposite coset $(12)A_n$ flips the sign of δ.

(1) Let us list a few Lemmas that will aid our proof. The proofs of each lemma exist in the Rosen source.

Lemma 4.4. *Let F be a field containing a primitive q-th root of unity. If $a \in F^\times$ is not a q-th power, then the polynomial $x^q - a$ is irreducible. If α is a root of $x^q - a = 0$ then every $\gamma \in F(\alpha)$ can be written in the form*

$$\gamma = a_0 + a_1\alpha + \cdots + a_{q-1}\alpha^{q-1}$$

where each $a_i \in F$.

Lemma 4.5. *Assume that $x^q - a \in F[x]$ is irreducible and that α is a root. Let γ be an element of $F(\alpha) \setminus F$. Then there is a $\beta \in F(\alpha)$ such that $\beta^q \in F$ and*

$$\gamma = b_0 + b_1\beta + \cdots + b_{q-1}\beta^{q-1}$$

where each $b_i \in F$.

Lemma 4.6. *Let q be a prime. Then for each integer i,*

$$1 + \zeta_q^i + \zeta_q^{2i} + \cdots + \zeta_q^{(q-1)i} = \begin{cases} 0 & \text{if } q \text{ does not divide } i, \\ q & \text{if } q \text{ divides } i. \end{cases}$$

Lemma 4.7. *Consider the extension E/F'. Let $y \in E$. Then the irreducible polynomial for y over F' splits into linear factors in $E[x]$.*

Now this lemma is the final one, containing the crux of the argument.

Lemma 4.8. *Let L/F' be an extension field, q a prime, and $a \in L$ and element such that $x^q - a \in L[x]$ is irreducible. Let α be a root of $x^q - a = 0$. Set $M = L(\alpha) \cap E$ and $M_0 = L \cap E$. If $M \neq M_0$, then M/M_0 is a radical extension. More precisely, there is a $\beta \in M$ such that $\beta^q \in \mathcal{M}_0$ and β generates M over M_0.*

Now suppose that L/F' is a radical tower and that $E \subseteq L$. We have

$$F' = L_0 \subset L_1 \subset ... \subset L_m = L$$

where $L_{i+1} = L_i\left(\sqrt[q_i]{a_i}\right)$, q_i being a prime, and $a_i \in L_i$. Now consider the tower

$$F' = L_0 \cap E \subseteq L_1 \cap E \subseteq ... \subseteq L_{m-1} \cap E \subseteq E.$$

If $L_{i+1} \cap E = L_i \cap E$ there is nothing that need be said. Otherwise, then the previous lemma shows that $L_{i+1} \cap E/L_i \cap E$ is a radical extension of degree q_i. Thus, after eliminating equalities, we see E as a radical tower over F'.

(2) Suppose $F' = F'_0 \subset F'_1 \subset ... \subset F'_n = E$ is a radical tower. Then there is a prime p and an element $a \in F'^\times$ such that $F'_1 = F(\sqrt[p]{a})$. We will show that $p = 2$ and that $a = b^2\Delta$ where $b \in F'^\times$ and Δ is the symmetric function defined before. Thus, F'_1 will be uniquely determined and is the field $F(\sqrt{\Delta})$.

Set $\alpha = \sqrt[p]{a}$ and let $\tau \in S_n$ be a transposition. Applying τ we get $\tau(\alpha)^p = a$, which implies $(\tau(\alpha)/\alpha)^p = 1$, so $\tau(\alpha) = \zeta_p \alpha$, where $\zeta_p^p = 1$. Applying τ again achieves $\alpha = \tau(\zeta_p \alpha) = \zeta_p^2 \alpha$. Either $\tau(\alpha) \neq \alpha$ for some transposition τ and $p = 2$, or α is fixed by all transpositions. However, if α is always fixed, then we contradict $\alpha \in F'$, since all of S_n is generated by transpositions and S_n should only fix roots of f in E/F'. Thus, $\tau(\alpha) = \pm\alpha$ for all transpositions, thus all $\sigma \in S_n$. We know every 3-cycle is a square, i.e. $(abc) = (acb)^2$, so $A_n(\alpha) = \alpha$. Since it is true for one, $\tau(\alpha) = -\alpha$ for all transpositions. This is a property shared by δ. So α/δ is fixed by all transpositions and so also by all elements of S_n. Let $b = \alpha/\delta \in F$, and so

$$a = \alpha^2 = b^2\delta^2 = b^2\Delta,$$

showing $F_1' = F'(\sqrt{b^2\Delta}) = F'(\sqrt{\Delta})$.

Knowing this, we can prove that F_1 has no radical extension in E. Suppose $c \in F_1'^{\times}$, and $F_2' = F_1'(\sqrt[q]{c})$ for prime q. Set $\gamma = \sqrt[q]{c}$. We know A_n leaves F_1' fixed. Let ρ be a 3-cycle and apply ρ to both sides: $\rho(\gamma) = \zeta_q \gamma$. Apply ρ twice more to the equation yields $\gamma = \rho^3(\gamma) = \zeta_q^3 \gamma$. Thus, either $\rho(\gamma) = \gamma$ for all 3-cycles, or $\rho(\gamma) \neq \gamma$ for some 3-cycle and $q = 3$. Supposing the former, γ is fixed by A_n and is in F_1' contradicts our assumption about γ, so we conclude $q = 3$. But we could have applied ρ four times more to achieve $\gamma = \rho^5(\gamma) = \zeta_q^5 \gamma$, giving us a contradiction.

□

5. Explicit Version

In 1828, Abel constructed the following family of polynomials of degree 5 to show how not every polynomial is solvable in radicals. The polynomial is of the form

$$f(x) = x^5 - x + a = 0,$$

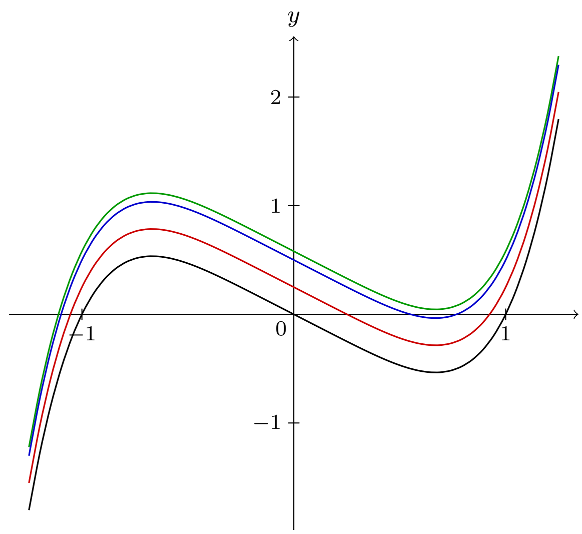
where $a \in \mathbb{C}$ chosen so that there are no multiple roots (so that all 5 roots in $\mathbb{C}$ are distinct). An equivalent condition to $f(x)$ having multiple root $x = \alpha$ is if and only if $f'(\alpha) = 0$. We have $f'(x) = 5x^4 - 1$, which implies $\alpha = e^{k\pi/2}$ for $k = 0, 1, 2, 3$ results in multiple roots, unless

$$a \neq \pm\frac{4}{5\sqrt[4]{5}}, \pm\frac{4i}{5\sqrt[4]{5}}.$$

We allow $a \in \mathbb{C} \setminus \left\{\pm\frac{4}{5\sqrt[4]{5}}, \pm\frac{4i}{5\sqrt[4]{5}}\right\}$, a punctured plane. Now we may perform an analysis on how the roots of $f(x)$ swap as a varies. Specifically, we can try to perform a one-parameter loop that begins at $a = 0$, approaches one of the forbidden values of $a = \frac{4}{5\sqrt[4]{5}}$, performs a loop about a, and then returns to $a = 0$. We will show that the roots of $f_0(x) = x^5 - x$: $\{0, \pm 1, \pm i\}$ change in this way:

$$\begin{array}{ccccc} 0 & 1 & i & -1 & -i \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 0 & i & -1 & -i \end{array}$$

We may visualize the graph of $f(x)$ as as we vary a as described.



The action merges the roots $x = 0$ and $x = 1$, and then supposedly swaps their places when returning to $a = 0$ (shown in black). Call $b_0 = \frac{1}{\sqrt[4]{5}}, a_0 = \frac{4}{5\sqrt[4]{5}}$. Then we let $x = b_0 + \epsilon$ for $\epsilon \in \mathbb{C}, |\epsilon| \approx 0$. Going back to our original formula, when $a \approx a_0$, we have an approximation

$$\begin{aligned} a = x - x^5 &= b_0 + \epsilon - (b_0 - \epsilon)^5 \\ &= (b_0 - b_0^5) + \epsilon(1 - 5b_0^4) - \epsilon^2(10b_0^3) + ... \end{aligned}$$

But we also have that b_0 is a multiple root, so $a_0 = b_0 - b_0^5$, and $b_0 = \frac{1}{\sqrt[4]{5}}$ implies $1 - 5b_0^4 = 0$. Thus, $a = a_0 - \epsilon^2(10b_0^3)$. We interpret this as a small change in x corresponding to a doubly fast change in a, explaining how the two roots swap. Similarly, we have all of the transpositions containing 0 and $u \cdot a_0$ by approaching $u \in \mathbb{C}$, where $u \in \{\pm 1, \pm i\}$ for this example. S_5 is generated by these four transpositions.

We would like to show a contradiction to solving $f(x)$ in radicals. Assume there exists

$$\begin{aligned} x_1^{k_1} &= p_1(s_1, ..., s_n), \\ x_2^{k_1} &= p_2(s_1, ..., s_n; x_1), \\ &\vdots \end{aligned}$$

such that we can describe all roots of $f(x) = x^5 - x + a$ sequentially.

Lemma 5.1. *Given 2 loops: ℓ_1, ℓ_2 in a-plane, consider their commutator $\ell = [\ell_1, \ell_2]$. Then ℓ fixes x_1.*

Proof. Let $\zeta = \zeta_{k_1}$, the k_1-th root of unity. Notice that $\ell_1 : x_1 \mapsto x_1\zeta^p$, $\ell_2 : x_1 \mapsto x_1\zeta^q$, so $\ell = [\ell_1, \ell_2] = \ell_1\ell_2\ell_1^{-1}\ell_2^{-1}$ maps

$$[\ell_1, \ell_2] : x_1 \mapsto x_1\zeta^p\zeta^q\zeta^{-p}\zeta^{-q} = x_1$$

by the abelian property of the group of roots of unity. □

Now the commutator of commutators: $[[\ell_1, \ell_2], [\ell_3, \ell_4]]$ fixes x_2, and so on. Thus, we can construct automorphisms that fix all roots of f, since $A_5 = [A_5, A_5]$ (a perfect group, known because it is simple and non-abelian). However, we said that the roots should permute, since every (even) permutation from A_5 is realized by some loop. Thus, we have reached a contradiction, showing this polynomial is not solvable in radicals.

References

[1] Jenia Tevelev. 2016. *Graduate Algebra: Numbers, Equations, Symmetries.*
[2] Clay Shonkwiler. *Algebra HW 11.*
[3] Michael I. Rosen. 1995. *Niels Hendrik Abel and Equations of the Fifth Degree.*
[4] Harpreet Bedi. 2015. *Fields to Galois Theory.*