INTRODUCTION TO GALOIS THEORY

JASON PRESZLER

1. Introduction and History

• The life of Évariste Galois and the historical development of polynomial solvability is one of the most interesting and dramatic tales in the history of mathematics.

2. Background

Definition 1 (Field Extension)**.** A field E is an *extension field* of a field F if $F \leq E$ (F a subfield of E). A field extension is denoted $E : F$.

Theorem 1 (Kronecker's Theorem)**.** *Let F be a field and let $f(x)$ be a non-constant polynomial in $F[X]$. Then $\exists$ an extension field E of F and an $\alpha \in E$ such that $f(\alpha) = 0$.*

Definition 2. If ϕ is an automorphism of a field E, then $a \in E$ is *left fixed by* ϕ if $\phi(a) = a$. The set $E_\phi = \{a \in E : \phi(a) = a\}$ is the *fixed field of* ϕ. Similarly for any collection of automorphism that fix the same elements in E.

Theorem 2 (Important but Uneventful Facts)**.** *It can easily be shown that E_ϕ is a subfield of E and that the set of all automorphisms of a field forms a group under function composition.*

Theorem 3. *If $E : F$ is a field extension, the operations*

$$(1) \qquad (a, b) \to ab \qquad (a \in F, b \in E)$$

$$(b, c) \to b + c \qquad (b, c \in E)$$

define on E the structure of a vector space over F.

Definition 3 (Degree of E over F)**.** The *degree* [E:F] of a field extension $E : F$ is the dimension of E considered as a vector space over F.

Example $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ has degree 2.

Definition 4 (Splitting Field)**.** Let E be an extension field of F and let $f(x) \in F[x]$. We say $f(x)$ *splits* in E, or E is the splitting field of $f(x)$ over F, if $f(x)$ can be factored into a product of linear factors in $E[x]$, but no proper subfield of E contains all the roots of $f(x)$.

Example Recall the Fundamental Theorem of Algebra, which can now be phrased as every non-constant polynomial with complex coefficients splits in $\mathbb{C}[x]$.

Definition 5 (Group of E over F, Galois Group)**.** The group of all automorphisms of E leaving F fixed, or the **group of** E **over** F, shall be denoted $G(E/F)$, specifically $G(E/F)$ is the Galois Group of E over F.

Theorem 4. *Let E be a field and $F \leq E$. Then $G(E/F)$ is a subgroup of the set of automorphisms of E. Furthermore, $F \leq E_{G(E/F)}$.*

Definition 6 (Intermediate Field)**.** $E_{G(E/F)}$ above is an *intermediate field* of $E : F$.

Definition 7 (Normal Extension)**.** K is a *normal extension* of F if K is a finite extension of F such that F is the fixed field of $G(K/F)$.

Theorem 5 (Herstein 5.t)**.** *Let K be a normal extension of F and let H be a subgroup of $G(K/F)$; let K_H be the fixed field of H. Then:*

1. $[K : K_H] = |H|$.
2. $H = G(K/K_H)$.

Corollary 1 (Special Case)**.** *When $H = G(K/F)$ then $[K : F] = |G(K/F)|$.*

Theorem 6 (Herstein 5.u)**.** *K is a normal extension of F iff K is the splitting field of some polynomial over F.*

3. Main Theorem of Galois Theory

The following theorem states that there is a one-to-one correspondence between subgroups of the Galois group and the intermediate fields, among other things.

Main Theorem (Fundamental Theorem of Galois Theory)**.** *Let K be a finite normal extension of the field F, that is either finite or has characteristic 0, and with Galois group $G(K/F)$. For any field E, such that $F \leq E \leq K$, let $\psi(E)$ be the subgroup of $G(K/F)$ leaving E fixed. Then ψ is a one-to-one map of the set of all such intermediate fields onto the set of all subgroups of $G(K/F)$ with the following properties:*

1. $\psi(E) = G(K/E)$. *($\psi : K \to G(K/F)$)*
2. $E = K_{G(K/E)} = K_{\psi(E)}$.
3. *For $H \leq G(K/F)$, $\psi(E_H) = H$.*
4. $[K : E] = |\psi(E)|$ *and* $[E : F] = [G(K/F) : \psi(E)]$, *the index for groups.*
5. *E is a normal extension of F iff $\psi(E)$ is a normal subgroup of $G(K/F)$. When $\psi(E) \trianglelefteq G(K/F)$, then $G(E/F) \simeq G(K/F)/G(K/E)$.*
6. *The lattice of subgroups of $G(K/F)$ is the inverted lattice of intermediate fields of K over F.*

Proof. Property 1 follows directly from the definition of ψ in the statement. Since K is the splitting field of $f(x) \in F$, by Herstein 5.u K is a normal extension of E and by the definition of normality E is the fixed field of $G(K/E)$, or $E = K_{G(K/E)}$; proving property 2.

Property 3 follows from directly from Herstein 5.t. Furthermore any subgroup of $G(K/F)$ is of the form $H = G(K/K_H)$, so ψ maps the set of all subfields of K containing F *onto* the set of all subgroups of $G(K/F)$. ψ is also one-to-one because, if $G(K/E_1) = G(K/E_2)$ then by property 2, $E_1 = K_{G(K/E_1)} = K_{G(K/E_2)} = E_2$.

Since K s a normal extension of E, using Herstein 5.t, $[K : E] = |G(K/E)|$, but then $|G(K/F)| = [K : F] = [K : E][E : F] = |G(K/E)|[E : F]$ and finally:

$$[E : F] = \frac{|G(K/F)|}{|G(K/E)|} = [G(K/F) : G(K/E)] \ (index \ for \ groups).$$

This concludes property 4.

Property 5 shows that the two uses of the word normal correspond and the first statement is proven by pushing through the two definitions of normal (one for groups and the other for field extensions) and employing a few other facts. The isomorphism results from the automorphisms of $G(E/F)$ inducing automorphisms of $G(K/F)$ and then showing the kernel of a map $\lambda : G(K/F) \to G(E/F)$ is $G(K/E)$. Combining these facts λ is onto and with the fundamental isomorphism theorem $G(E/F) \simeq G(K/F)/G(K/E)$. (more details will be provided if desired)

Property 6 is follows from the correspondence, ψ, that relates the subgroups of the Galois group to the intermediate fields. Easily one can see that the lattice structures must be symmetric, but the inversion is not immediately clear. Consider subgroups of the Galois group, as the order of the subgroups increase there are going to be fewer elements of K fixed by all of the automorphisms in the subgroup, thus the relation is inversely proportional. By definition the identity map in $G(K/F)$ fixes the entire field K, but it's also the smallest subgroup of $G(K/F)$. On the other extreme, F is the smallest subfield of K that contains F and by definition of the Galois group $G(K/F)$ is the group of automorphisms of K that fix F. Naturally everything in between will fall into place. □

Notes on the Fundamental Theorem

• Often it is much easier to determine the lattice of subgroups that the lattice of intermediate fields.

• The importance of the fundamental theorem is its power as a tool, allowing the application of group theory to more complex realms.

Example of Galois Theory and Polynomials[7]

• Consider the polynomial $f(x) = x^4 - 4x^2 - 5 = 0$.

• The factors are (x^2+1) and (x^2-5), therefore its roots are $\pm i$ and $\pm\sqrt{5}$.

• Now create the field extension $L:\mathbb{Q}$ such that $L=\mathbb{Q}(i,\sqrt{5})$.

• There are only 4 automorphisms of L that fix $\mathbb{Q}$, let us call them I,R,S,T. We now there are 4 because a basis for the extension is $\{1,i,\sqrt{5},i\sqrt{5}\}$, thus $[L:\mathbb{Q}]=4$ which is equal to the order of the Galois group by the fundamental theorem.

• The automorphism I is the identity map, R sends i to $-i$, S sends $\sqrt{5}$ to $-\sqrt{5}$, and T is the composite of R and S. Clearly this is a group and furthermore each element is its own inverse.

• The subgroups of $G(L/\mathbb{Q})$ are $I,\{I,R\},\{I,S\},\{I,T\}$, and $\{I,R,S,T\}$.

• By the fundamental theorem, the corresponding subfields of L are: $L,\mathbb{Q}(\sqrt{5}),\mathbb{Q}(i),\mathbb{Q}(i\sqrt{5})$, and $\mathbb{Q}$.

4. Insolvability of the Quintic

Definition 8 (Solvable Group)**.** A group G is *solvable* iff G has a series of subgroups

$$\{e\}=H_0\subset H_1\subset\cdots\subset H_k=G$$

where, for each $0\leq i<k$, $H_i\trianglelefteq H_{i+1}$ and H_{i+1}/H_i is abelian.

Theorem 7 (Facts about Solvable groups)**.** *Let G be a group, H a subgroup of G and N a normal subgroup of G.*

1. *If G is solvable then H is solvable.*
2. *If G is solvable then G/N is solvable.*
3. *If N and G/N are solvable then G is solvable.*

Theorem 8 ($A_n<S_n$)**.** *The alternating group, A_n, is a subgroup of the symmetric group, S_n.*

Theorem 9 (S_n is not solvable)**.** *The symmetric group S_n is not a solvable group $\forall\ n>4$.*

Proof. • Note that the alternating group has order $n!/2$, and for all $n>4$, A_n is simple.

• A simple group is solvable iff it is a cyclic group of prime order (Stewart, thrm 13.3)

• Clearly $n!/2$ is not prime if $n > 4$.

• Therefore A_n is insolvable and by the first fact of solvable groups, S_n can't be solvable. □

Theorem 10 (Solvable By Radicals Implies A Solvable Group)**.** *Let F be a field of characteristic zero and let $f(x) \in F[x]$. Suppose that $f(x)$ splits in $F(a_1, \ldots, a_t)$ where $a_1^{n_1} \in F$ and $a_i^{n_i} \in F(a_1, \ldots, a_t)$ for $2 \leq i \leq t$. Let E be the splitting field for $f(x)$ over F in $F(a_1, \ldots, a_t)$. Then $G(E/F)$ is solvable.*

Proof. Page 565 of Gallian □

Theorem 11 (Lemma for the quintic)**.** *Let p be a prime and f an irreducible polynomial of degree p over $\mathbb{Q}$. Suppose that f has precisely 2 non-real zeros in $\mathbb{C}$, then the Galois group of f over $\mathbb{Q}$ is S_p.*

Proof. • By the fundamental theorem of algebra, $\mathbb{C}$ contains the splitting field for f.

• The Galois group is a permutation of the zeros of f, as seen in the above example. Therefore the Galois group is a subgroup of S_p.

• When constructing the splitting field, E, of f, we first adjoin an element of degree p. Such an element exists since $f(a) = 0$ implies that a is algebraic over $\mathbb{Q}$ and since f is irreducible, f is the minimal polynomial for a over $\mathbb{Q}$.

• Note $[\mathbb{Q}(a) : \mathbb{Q}] = p$ (Gallian, ex. 2, p. 361 for more info). Therefore p divides $[E : \mathbb{Q}]$ and by property 4 of the fundamental theorem, the Galois group is divisible by p.

• By Cauchy's Theorem (Gallian, 24.3 corollary) the Galois group then contains an element of order p, which implies that $\exists$ a p-cycle in the Galois group.

• Since f has two non-real zeros and complex conjugation is a valid automorphism in the Galois group, we know that the Galois group contains a two-cycle.

• Since the Galois group contains a p-cycle and a 2-cycle, and is a subgroup of S_p it must be isomorphic to S_p since S_p is the only such subgroup with these properties. (This is a theorem in most books but Gallian leaves it as exercise 25.25) □

Corollary 2 (Special Case)**.** *The polynomial* $f(t) = t^5 - 6t + 3$ *over* $\mathbb{Q}$ *is not solvable by radicals.*

Proof. • By Eisenstein's Criterion, $f(t)$ is irreducible over $\mathbb{Q}$.

• By any number of methods it can be shown that $f(t)$ has three real zeros and 2 non-real zeros, thus $f(t)$ is not solvable by radicals and our goal has been achieved! □

Final Note

• "Of course this is not the end of the story. There are more ways of killing a quintic than choking it with radicals." –Ian Stewart ([7], p. 135)

5. Conclusions and Other Uses of Galois Theory

• There are other methods for finding the roots of a polynomial. The only practical one is numerical analysis, which is easier than Galois Theory and solving by radicals when possible, but by no means as elegant.

• Galois theory was originally phrased in terms of polynomial solvability, which is way the quintic is its classical example. However, the relationship between groups and fields that it provides a tool for is of the greatest importance in modern algebra.

• Galois theory can be used to solve many other problems such as (this is not an exhaustive list):

1. Geometric constructions (squaring the circle, trisecting the angle, etc.)
2. Proving numbers are transcendental (π, e).
3. Cyclotomic extensions

• Galois theory has also developed into several branches, including differential Galois Theory, constructive Galois theory, categorical Galois theory, probabilistic Galois theory, and inverse Galois theory. (This list is also not exhaustive)

• It is not uncommon for large mathematics programs to have an entire semester long class on Galois theory for undergrads and most graduate schools have one or two semesters of Galois theory.

References

1. Emil Artin, *Galois theory*, Dover, New York, 1998, Unaltered republication of the 1944 2nd edition by University of Notre Dame Press, based on Artin's 1926 lecture.
2. John Durbin, *Modern algebra an introduction*, 3rd ed., John Wiley & Sons, New York, 1992.
3. Harold Edwards, *Galois theory*, Springer-Verlag, New York, 1984.
4. John Fraleigh, *A first course in abstract algebra*, 6th ed., Addison-Wesley, New York, 1999.
5. Joseph Gallian, *Contemporary abstract algebra*, 4th ed., Houghton Mifflin Company, New York, 1998.
6. I. N. Herstein, *Topics in algebra*, Blaisdell, London, 1964.
7. Ian Stewart, *Galois theory*, 2nd ed., Chapman & Hall/CRC, New York, 1989.
8. B.L. van der Waerden, *Modern algebra*, 2nd ed., vol. 1, Frederick Ungar, New York, 1943.

E-mail address: jpreszler@ups.edu