Galois Theory and Noether's Problem

Meredith Blue
Eckerd College

Abstract

Galois theory was developed in the early 1800's as an approach to understand polynomials and their roots. The beauty of theory has developed in its own right, with the Inverse Galois Problem as one of the most famous unsolved problems in algebra. Noether's Problem arose during Emmy Noether's approach to solving the Inverse Galois Problem. This paper reviews Galois extensions, defines Noether's Problem and comments on it's relation to the Inverse Galois Problem and to parameterization of Galois Extensions.

Galois theory expresses a correspondence between algebraic field extensions and group theory. We are particularly interested in finite algebraic extensions obtained by adding roots of irreducible polynomials to the field of rational numbers. Galois groups give information about such field extensions and thus, information about the roots of the polynomials.

We begin with the definition of a group:

Definition 1 *A* **group,** *G is a set of elements with a binary operation $* : (G \times G) \rightarrow G$ satisfying the following:*

1. *Closure: $\forall a,\ b \in G$, $a * b \in G$.*
2. *Associativity: $(a * b) * c = a * (b * c)$*
3. *Identity: $\exists e \in G \ni a * e = e * a = a$*
4. *Inverses: $\forall a \in G$, $\exists a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$*

EXAMPLES:

1. The integers $\mathbb{Z}$ with addition as the binary operation.
2. $\mathbb{Q} - \{0\}$ with multiplication as the binary operation.

3. **Symmetric Group:** Let X be a set with n objects $X = \{x_1, \dots, x_n\}$. Let G be the set of all one-to-one onto maps $\sigma : X \to X$. G is a group with binary operation, $\circ$, composition of functions. This group is called the **Symmetric Group on n letters** denoted S_n.

4. $C = \{f : \mathbb{R} \to \mathbb{R} \mid f$ is increasing and continuous$\}$ with binary operation composition of functions.

If G is a finite group, we let $|G|$ represent the number of elements of G. Next, we define fields:

Definition 2 *A* **field** F *is a set of elements and 2 binary operations:* $+$ *and* $\times$ *such that* F *is a group under* $+$ *with identity* 0*, and* $F - \{0\}$ *is a group under multiplication. Moreover:*
$\forall x,\ y \in\ F, x + y = y + x$ *and* $x \times y = y \times x$

For simplicity we write $x \times y$ as xy.

EXAMPLES:

1. $\mathbb{Q}$

2. $\mathbb{R}$

3. $\mathbb{C}$

4. $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ with addition and multiplication modulo 7.

Definition 3 *A field* F *is a* subfield *of a field* K *if* $F \subset K$*.*

Definition 4 *If* $f \subset K$ *are fields, then we say* K *is an* extension *field of* F*. This is denoted* K/F*.*

Let $\alpha \in \mathbb{C}$. Let $\mathbb{Q}(\alpha)$ be the smallest field containing $\mathbb{Q}$ and α; in particular any field K that contains $\mathbb{Q}$ and α contains $\mathbb{Q}(\alpha)$. The field $\mathbb{Q}(\alpha)$ can either be an *algebraic* or a *transcendental* extension. We give an example of each and express some important properties of each type of extension.

We first consider $\mathbb{Q}(\pi)$. π is transcendental over $\mathbb{Q}$: i.e. there is no polynomial with rational coefficients that has π as a root. $\mathbb{Q}(\pi)$ is isomorphic to the field of rational functions in x over $\mathbb{Q}$. In addition, we may add another transcendental element e. $\mathbb{Q}(\pi, e) \cong \mathbb{Q}(x, y)$ the field of rational functions in 2 variables over $\mathbb{Q}$. These are *infinite* extensions because $\mathbb{Q}(x)$ is infinite dimensional as a vector space over $\mathbb{Q}$. For example, $\{x^i \mid i \in \mathbb{Z}\}$ is an infinite linearly independent set in $\mathbb{Q}(x)$ when viewed as a vector space over $\mathbb{Q}$.

We next consider $\mathbb{Q}(\sqrt{2})$. $\sqrt{2}$ is a root of the polynomial x^2-2. Thus, we say $\sqrt{2}$ is *algebraic* over $\mathbb{Q}$, and $\mathbb{Q}(\sqrt{2})$ is an *algebraic extension* field of $\mathbb{Q}$. An easy exercise shows that any element in $\mathbb{Q}(\sqrt{2})$ can be written as $a+b\sqrt{2}$ with a and b rational numbers. Thus, $\mathbb{Q}(\sqrt{2})$ is a vector space of dimension 2 over $\mathbb{Q}$. This is a *finite* extension.

If an extension field $L \supset \mathbb{Q}$ can be obtained by adding finitely many roots of polynomials, we say L is a *finite algebraic extension of* $\mathbb{Q}$. The next theorem states that any finite algebraic extension can be obtained by adding a single element to $\mathbb{Q}$.

Theorem 5 *(Primitive Element Theorem) Any finite algebraic extension, L, of $\mathbb{Q}$, has the form:*

$$L = \mathbb{Q}(\alpha) \textit{ for some } \alpha \in \mathbb{C}$$

Let us return to our original interpretation in terms of polynomials.

Definition 6 *Let α be algebraic over $\mathbb{Q}$. $f(x)$ is the* **minimal polynomial** *for α (denoted $\min_{\mathbb{Q}}(\alpha)$) if:*

1. *$f(x)$ has leading coefficient 1.*
2. *$f(\alpha) = 0$ and*
3. *If $g(x)$ is any polynomial with rational coefficients such that $g(\alpha) = 0$ then the degree of $g(x) <$ the degree of $f(x)$.*

A polynomial $p(x)$ is *irreducible* if whenever $p(x) = h(x)k(x)$ with $h(x)$ and $k(x)$ polynomials, then either $h(x)$ or $k(x)$ is a constant (i.e. rational number.)

Theorem 7 *$\min_{\mathbb{Q}}(\alpha)$ is irreducible.*

Proof: Let $f(x) = \min_{\mathbb{Q}}(\alpha)$. Suppose $f(x) = p(x)q(x)$. Since α is a root of $f(x) \in \mathbb{C}$, $f(\alpha) = 0 = p(\alpha)q(\alpha)$. $p(\alpha)$ and $q(\alpha)$ are just complex numbers whose product is 0. Thus, either $p(\alpha) = 0$ or $q(\alpha) = 0$. Without loss of generality, assume $p(\alpha) = 0$. Since $f(x)$ is the polynomial with minimum degree with α as a root, the degree of $p(x) =$ degree $f(x)$. Thus, the degree of $q(x)$ is 0. This shows $f(x)$ is irreducible.

q.e.d.

Theorem 8 *Let $f(x) = \min_{\mathbb{Q}}(\alpha)$ for some $\alpha \in \mathbb{C}$. Suppose $g(x)$ is a polynomial with rational coefficients such that $g(\alpha) = 0$. Then, $g(x) = f(x)k(x)$ for some polynomial $k(x)$.*

Proof: By the definition of $\min_{\mathbb{Q}}(\alpha)$, $deg(g(x)) \geq deg(f(x))$. Using the Euclidean algorithm for polynomials, we can write

$$g(x) = q(x)f(x) + r(x)$$

where $r(x) = 0$ or $deg(r(x)) < deg(f(x))$. Plugging in α for x we have

$$g(\alpha) = q(\alpha)f(\alpha) + r(\alpha)$$

$g(\alpha) = f(\alpha) = 0$, so $r(\alpha) = 0$. Since $deg(f(x))$ is minimal with respect to having α as a root, $r(x) = 0$. Thus, $g(x) = q(x)f(x)$.

q.e.d.

Galois is famous for his result that polynomials of degree 5 are not solvable by radicals, that is there can be no formula for solving all degree 5 polynomials. In light of this we are interested in fields $K \supset \mathbb{Q}$ where K is the smallest field containing all roots of a given polynomial with rational coefficients. These fields are called *splitting fields*:

Definition 9 *A field $K \supset \mathbb{Q}$ is a* **splitting field** *for the polynomial $f(x)$ if*

1. *K contains all roots of $f(x)$.*
2. *If L is another field containing all roots of $f(x)$, then $L \subseteq K$.*

Galois studied these extension fields using *automorphisms*:

Definition 10 *A* **field automorphism** *is a mapping $\phi : F \to F$ where F is a field satisfying:*

$$\phi(xy) = \phi(x)\phi(y)$$

and

$$\phi(x + y) = \phi(x) + \phi(y)$$

Let $L/\mathbb{Q}$ be a field extension. Let G be the set of automorphisms on L that leave $\mathbb{Q}$ fixed, that is:

$\sigma \in G$ if and only if $\sigma : L \to L$ is a field automorphism and $\sigma(q) = q$ for all $q \in \mathbb{Q}$.

Theorem 11 *If $L/\mathbb{Q}$ is a field extension, then the set, $G(G, \mathbb{Q})$ of automorphisms on L leaving $\mathbb{Q}$ fixed is a group with binary operation composition of mappings.*

Let's look at this another way. Suppose G is a group of automorphsims on a field F. We are interested in the subset $F^G \subset F$ that is fixed under all automorphisms $\sigma \in G$. An easy exercise shows that this F^G is in fact a field.

Definition 12 *Let G be the set of automorphisms on a field L. The set of elements $x \in L$ such that $\sigma(x) = x$ for all $x \in L$ and all $\sigma \in G$ is called the* **fixed field** *of G. We denote this L^G.*

Again, we look at some examples to observe that $G(L, \mathbb{Q})$ may be different from $G(K, \mathbb{Q})$ if L and K are different extension fields of $\mathbb{Q}$.

Example: Consider $\mathbb{Q}(\sqrt{2})$. Let $G + G(\mathbb{Q}(\sqrt{2}, \mathbb{Q})$ be the set of automorphisms of $\mathbb{Q}(\sqrt{2})$ that leave $\mathbb{Q}$ fixed.

There are 2 automorphisms of $\mathbb{Q}(\sqrt{2})$ that leave $\mathbb{Q}$ fixed, the identity and:

$$\sigma(\sqrt{2}) = -\sqrt{2} \quad \sigma(q) = q \;\forall\; q \in \mathbb{Q}$$

Hence, the fixed field of G, $\mathbb{Q}(\sqrt{2})^G = \mathbb{Q}$.

Example: Now consider $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$. Let H be the set of automorphisms of $\mathbb{Q}(\sqrt[3]{2})$ that leave $\mathbb{Q}$ fixed.

Notice that $(\sqrt[3]{2})$ is a root of $x^3 - 2$. Suppose τ is an automorphism of $\mathbb{Q}(\sqrt[3]{2})$. Consider $\tau(\sqrt[3]{2}^3 - 2)$.

$$\tau(0) = \tau(\sqrt[3]{2}^3 - 2) = (\tau(\sqrt[3]{2}))^3 - 2$$

Thus, any automorphism of $\mathbb{Q}(\sqrt[3]{2})$ leaving $\mathbb{Q}$ fixed will take $\sqrt[3]{2}$ to another root of $x^3 - 2$. Since there are no other real roots, all automorphisms in H must fix $\sqrt[3]{2}$ also.

Thus the fixed field of G is $\mathbb{Q}(\sqrt[3]{2})$.

Definition 13 *A field extension $L/\mathbb{Q}$ is* **Galois with group** *G if and only if G is the group of automorphisms of L leaving $\mathbb{Q}$ fixed and $L^G = \mathbb{Q}$.*

Let us now restate the Galois extension condition for the simple algebraic extension $L = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathbb{C}$. Let $f(x) = \min_{\mathbb{Q}}(\alpha)$. In this case, $L/\mathbb{Q}$ is Galois if and only if L contains all roots of $f(x)$. This is easily seen in the two examples above. $\mathbb{Q}(\sqrt[3]{2})$ only contains one root of $f(x) = x^3 - 2$, whereas $\mathbb{Q}(\sqrt{2})$ contains both roots of $f(x) = x^2 - 2$. This is easily described in terms of splitting fields:

Theorem 14 *A field extension L/F is Galois if and only if L is the splitting field for some irreducible polynomial $f(x) \in F[x]$.*

Galois theory relates the theory of field extensions to group theory. In particular it exhibits a one-to-one correspondence between subgroups of the Galois group and subfields of the Galois field extension. Using this correspondence and the theory of solvable groups, Galois showed that there can be no formula to solve all 5th degree polynomials with rational coefficients.

The most famous open question involving Galois theory is the

Inverse Galois Problem: Does every finite group G appear as a Galois group over $\mathbb{Q}$?

In 1918, Emmy Noether had the following approach to solving the Inverse Galois Problem:

Let G be a finite group. Consider the set of $|G|$ indeterminates indexed by the elements of G:

$$X = \{x_g \mid g \in G\}$$

In particular $|X| = |G|$. The X is just a set, we want to incorporate the binary operation of G as well. To do this we consider a *group action* on X.

Definition 15 *A group G* **acts** *on a set S if there are $|G|$ mappings:*

$$g : S \to S$$

satisfying

1. *$e(s) = s$ for all $s \in S$ where e is the identity element of G.*
2. *$g(h(s)) = gh(s)$, where the left side is composition of functions and the right side is the mapping given by the element $gh \in G$.*

In the case of Noether's approach we let:

$$g(x_h) = x_{gh}$$

Now, form the purely transcendental field

$$\mathbb{Q}(X) = \mathbb{Q}(x_e, x_g, \dots, x_h)$$

We can now think of G as automorphsims of $\mathbb{Q}(X)$ by letting $g(q) = q$ for all $q \in \mathbb{Q}$ and all $g \in G$. We are of course interested in the fixed field of $\mathbb{Q}(X)$ under G: $(\mathbb{Q}(X))^G$. By construction $\mathbb{Q}(X)/(\mathbb{Q}(X))^G$ is Galois with group G.

Theorem 16 *(Emmy Noether)*
If G is finite and $\mathbb{Q}(X)^G/\mathbb{Q}$ is rational (purely transcendental), then there is a Galois field extension $K/\mathbb{Q}$ with group G.

This follows from Hilbert's Irreducibility Theorem:

Theorem 17 (Hilbert's Irreducbility Theorem) *If $f(x)$ is an irreducible polynomial with coefficients in $\mathbb{Q}(t)$, then there are infinitely many points $t_0 \in \mathbb{Q}$ such that $f_{t_0}(x)$ is irreducible (over $\mathbb{Q}$).*

A proof of Hilbert's Irreducibilty Theorem can be found in [Se].

Proof of Theorem 16: If $\mathbb{Q}(X)^G/\mathbb{Q}$ is rational, then $\mathbb{Q}(X)^G \cong \mathbb{Q}(w_1, w_2, \ldots, w_n)$ where the w_i's are indeterminates. Since $\mathbb{Q}(X)/\mathbb{Q}(X)^G$ Galois with group G, there is an irreducible polynomial $f(y) \in \mathbb{Q}(w_1, w_2, \ldots w_n)$ such that $\mathbb{Q}(X)$ is the splitting field for $f(y)$. By the Primitive Element Theorem there is an $\alpha \in \mathbb{Q}(X)$ such that $f(\alpha) = 0$, and $\mathbb{Q}(X) = \mathbb{Q}(X)^G(\alpha)$.

Let t_0 be a point in $\mathbb{Q}^n$. Let $f_{t_0}(y)$ be the polynomial in $\mathbb{Q}[y]$ obtained by substituting $t_0 = (a_1, a_2, \ldots, a_n)$ in for $(w_1, w_2, \ldots, w_n)$ in $f(y) \in \mathbb{Q}(w_1, w_2, \ldots, w_n)[y]$. Successive applications of Hilbert's Irreducibility Theorem result in infinitely many $t_0 \in \mathbb{Q}^n$ such that $f_{t_0}(y) \in \mathbb{Q}[y]$ is irreducible (over $\mathbb{Q}$).

Let $L \supset \mathbb{Q}$ be the splitting field of $f_{t_0}(y)$ for some t_0 where $f_{t_0}(y)$ is irreducible. Then L is Galois over $\mathbb{Q}$ with group G.

q.e.d.

We conclude with a simple example to illustrate:

Example: Let G be the group with 2 elements: that is $G = \{0, 1\}$ with binary operation addition mod 2.

In Noether's approach, we let $X = \{x_0, x_1\}$. Of course we must think of G as automorphisms: G contains two elements, the identity map, i and a map σ. These maps satisfy the following:

$$i(x_0) = x_0,\ i(x_1) = x_1,\ \text{and}\ \sigma(x_0) = x_1,\ \sigma(x_1) = x_0$$

To find $\mathbb{Q}(X)^G$, we must find combinations involving sums and products of x_1 and x_0.

In this case, $\mathbb{Q}(X)^G = \mathbb{Q}(x_0 + x_1, x_0x_1)$ Explicitly,

$$\sigma(x_0 + x_1) = \sigma(x_0) + \sigma(x_1) = x_1 + x_0 = x_0 + x_1$$

and

$$\sigma(x_0x_1) = \sigma(x_0)\sigma(x_1) = x_1x_0 = x_0x_1$$

It is easy to see that $x_0 + x_1$ and x_0x_1 are transcendental over $\mathbb{Q}$ so there exists a Galois extension with group G over $\mathbb{Q}$. Of course, we saw a concrete example earlier: $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.

Of course, $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ is also a Galois extension over $\mathbb{Q}$ with group G. Both $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ can be realized as "specializations" of $\mathbb{Q}(x_0, x_1)/\mathbb{Q}(x_0+x_1, x_0x_1)$ by using the following map.

$$\phi : \mathbb{Q}(x_0, x_1) \to \mathbb{Q}(\sqrt{a})$$

is a field isomorphism (i.e. $\phi(xy) = \phi(x)\phi(y)$ and $\phi(x + y) = \phi(x) + \phi(y)$) satisfying:

$$\phi(q) = q\ \forall q \in \mathbb{Q} \text{ and } \phi(x_0) = \sqrt{a} \text{ and } \phi(x_1) = -\sqrt{a}.$$

In particular $\phi(x_0x_1) = \phi(x_0)\phi(x_1) = -a \in \mathbb{Q}$, and $\phi(x_0 + x_1) = \phi(x_0) + \phi(x_1) = 0 \in \mathbb{Q}$, so $\mathbb{Q}(x_0 + x_1, x_0x_1) \tilde{=} \mathbb{Q}$. In this specialization a can be any rational number which is not a square. The parameterization can be expressed by the following sentence: "Any extension of $\mathbb{Q}$ with a 2-element Galois group is obtained by adding a root of the polynomial $x^2 - a$ where a is any rational number such that $\sqrt{a}$ is not rational."

References

[H] Herstein, I. N. *Topics in Algebra.* Xerox Corporation. 1975

[I] Issacs, I. Martin. *Abstract Algebra.* Brooks/Cole Publishing Company. 1994.

[N] Noether, E. "Gleichungen mit Vorgeschribener Gruppe." Math Ann., **78** 221-229. (1918)

[S6] Saltman, David J. "Groups acting on fields, Noether's Problem." Contemporary Mathematics. **Vol. 43** 267-277. (1985)

[Se] Serre, Jean-Peirre. *Topics in Galois Theory.* Jones and Bartlett Publishers, Inc. 1992.

[Sw2] Swan, Richard G. “Noether’s Problem in Galois Theory.” in Emmy Noether in Bryn Mawr. Srinivasan, B. and Sally, J. eds. Springer-Verlag, New York. 21-40. (1983)