An Introduction to Galois Groups

Vincent Zimmern

University of Virginia

April 22, 2008

Definition of Extension

Definition

1. *If E is a field and F is a subset which, under the operations of E is itself a field then F is called a subfield of E.*

Definition of Extension

Definition

1. *If E is a field and F is a subset which, under the operations of E is itself a field then F is called a subfield of E.*
2. *E is then called an* **extension** *of F.*

Definition of Extension

Definition

1. *If E is a field and F is a subset which, under the operations of E is itself a field then F is called a subfield of E.*
2. *E is then called an* **extension** *of F.*
3. *We denote this extension by E/F.*

Definition of Normal Extension

Given an extension of E/F, we can define a subgroup G_F of the group of field automorphisms of E by

$$G_F = \{\sigma : E \longrightarrow E \mid \sigma(z) = z \, \forall z \in F\}$$

Definition of Normal Extension

Given an extension of E/F, we can define a subgroup G_F of the group of field automorphisms of E by

$$G_F = \{\sigma : E \longrightarrow E \mid \sigma(z) = z \, \forall z \in F\}$$

The fixed field of G_F will be a field containing F (i.e. $F \subseteq E^{G_F}$).

Definition of Normal Extension

Given an extension of E/F, we can define a subgroup G_F of the group of field automorphisms of E by

$$G_F = \{\sigma : E \longrightarrow E \mid \sigma(z) = z \,\forall z \in F\}$$

The fixed field of G_F will be a field containing F (i.e. $F \subseteq E^{G_F}$).

Definition

We say that E/F is a **normal extension** *if $[E : F]$ is finite and $F = E^{G_F}$. A normal extension is also called a Galois extension*

Definition of Galois Group

Definition

Let E/F be a normal extension of fields. Let $G(E/F) = \{\sigma : E \longrightarrow E \mid (\sigma|F) = 1\}$. This is called the **Galois group of** *E/F.*

Definition of Splitting Field

Definition

Let E/F be an extension and let

$$a_0x^n + a_1x^{n-1} + \cdots + a_n = p(x) \in F[x]$$

be a polynomial.

Definition of Splitting Field

Definition

Let E/F be an extension and let

$$a_0x^n + a_1x^{n-1} + \cdots + a_n = p(x) \in F[x]$$

be a polynomial.
We call E a **splitting field for p(x)** *if there exist $\alpha_1, \cdots, \alpha_n$ such that $p(x)$ factors in $E[x]$ in the following way:*

$$p(x) = a_0(x - \alpha_1)\cdots(x - \alpha_n) \in E[x]$$

Definition of Splitting Field

Definition

Let E/F be an extension and let

$$a_0x^n + a_1x^{n-1} + \cdots + a_n = p(x) \in F[x]$$

be a polynomial.
We call E a **splitting field for p(x)** *if there exist $\alpha_1, \cdots, \alpha_n$ such that $p(x)$ factors in $E[x]$ in the following way:*

$$p(x) = a_0(x - \alpha_1) \cdots (x - \alpha_n) \in E[x]$$

and there exists no intermediate field, $F \subseteq K \subseteq E$, with K different from E, such that $p(x)$ factors into linear factors in $K[x]$.

Definition of Characteristic Zero

Definition

The **characteristic** *of F, written char(F), is the (positive) generator of*

$$n \in Z \mid 0 = n \bullet x = x + \cdots + x \, (n \, times) \forall x \in F$$

Definition of Characteristic Zero

Definition

The **characteristic** *of F, written* $char(F)$, *is the (positive) generator of*

$$n \in Z \mid 0 = n \bullet x = x + \cdots + x\,(n\,times) \forall x \in F$$

If K is a field, it is a nice result that $char(F)$ is a prime p or zero.

Definition of Radical Extension

This is the last round of definitions – I promise! Just hold on!

Definition

A field extension, L/K , is called a radical extension if there exists a chain of intermediate fields,

$$K = K_0 < K_1 < K_2 < \ldots < K_r = L$$

with some $K_{i+1} = K_i(\alpha_i)$ and $\alpha_i^{n_i} \in K_i$ for some integer n_i.

Definition of Solvable

OK... sorry... there's one more definition but I swear it's the last one!

Definition

A polynomial, $f(x) \in K[x]$, is said to be solvable by radicals if its splitting field is contained in a radical extension of K.

Definition of Solvable

OK... sorry... there's one more definition but I swear it's the last one!

Definition

A polynomial, $f(x) \in K[x]$, is said to be solvable by radicals if its splitting field is contained in a radical extension of K.

Definition

A finite group, G, is **solvable** *if there exists a sequence of subgroups*

$$1 = G_n \triangleleft G_{n-1} \triangleleft G_{n-2} \triangleleft \ldots \triangleleft G_1 \triangleleft G_0 = G$$

such that each G_i/G_{i+1} is abelian.

When is a polynomial solvable by radicals?

Let K be a field of characteristic zero.
The polynomial, $f(x) \in K[x]$, is solvable by radicals if and only if its Galois group is solvable.

History of Polynomials Solvable by Radicals

Solving the Quintic by Radicals: Part I

It is not too terribly difficult to show that S_n is not solvable for $n \geq 5$. This realization, combined with Galois' discovery, sounded the death knoll for all those "solvers by radical".

Solving the Quintic by Radicals: Part I

It is not too terribly difficult to show that S_n is not solvable for $n \geq 5$. This realization, combined with Galois' discovery, sounded the death knoll for all those "solvers by radical".

Let's look at the following polynomial which has S_5 as its Galois group: $f(x) = 2x^5 - 10x + 5 \in Z[x] \subset Q[x]$.
So this Galois group has to be isomorphic to a subgroup of S_5.

Solving the Quintic by Radicals: Part I

It is not too terribly difficult to show that S_n is not solvable for $n \geq 5$. This realization, combined with Galois' discovery, sounded the death knoll for all those "solvers by radical".

Let's look at the following polynomial which has S_5 as its Galois group: $f(x) = 2x^5 - 10x + 5 \in Z[x] \subset Q[x]$.
So this Galois group has to be isomorphic to a subgroup of S_5.

We now need to show that the Galois group in fact **is** S_5 in its entirety.

Solving the Quintic by Radicals: Part II

Let α be any root of $f(x)$. Then $[Q(\alpha) : Q] = 5$ by the fact that the index of F in $F(\alpha)$ is just the degree of $f(x)$.
If L/Q is the splitting field extension of $f(x)$ then $[L : Q] = [L : Q(\alpha)][Q(\alpha) : Q]$. Consequently, the Galois group is isomorphic to a subgroup of S_5 that has a 5-cycle.
We need to find some element of the Galois group that switches the two roots and fixes the rest. So, if we can show that $f(x)$ has three real roots, then we have met that criterion.

Solving the Quintic by Radicals: Part II

Let α be any root of $f(x)$. Then $[Q(\alpha) : Q] = 5$ by the fact that the index of F in $F(\alpha)$ is just the degree of $f(x)$.

If L/Q is the splitting field extension of $f(x)$ then $[L : Q] = [L : Q(\alpha)][Q(\alpha) : Q]$. Consequently, the Galois group is isomorphic to a subgroup of S_5 that has a 5-cycle.

We need to find some element of the Galois group that switches the two roots and fixes the rest. So, if we can show that $f(x)$ has three real roots, then we have met that criterion.

Using the derivative of the polynomial and our basic calculus skills at finding roots, we isolate the three real roots. Since the sign of the function changes three times (between -1 and -2, between 0 and 1, and between 1 and 2), we can rest assured that there are indeed three real roots.