Introduction to Galois Theory

Yunsheng Lu

University of Virginia

January 7, 2022

polynomial ring: Let R be a ring, and we write $R[x]$ to be the set of all polynomials with coefficients from R. $R[x]$ is also a ring and R is a subring of $R[x]$.

irreducible: Let F be a field and $f(x) \in F[x]$. Then $f(x)$ is irreducible over F. if $f(x)$ cannot be expressed as $f(x) = p(x)g(x)$, where both $p(x), g(x) \in F[x]$ are nonconstant polynomials.

maximal ideal: A nontrivial proper ideal $I \subseteq$ ring R is maximal ideal if the only ideals J in R s.t. $I \subseteq J \subseteq R$ are $J = I$ and $J = R$.

Theorem

Let F be a field. A nontrivial ideal $I = < p(x) >$, then **TFAE**:

- *I a maximal ideal in $F[x]$*
- *$p(x)$ is irreducible over F*
- *$F[x]$ is a field*

Motivating Question

1. Give a field both contains $\mathbb{Q}$ and $\sqrt{2}$ Answer: $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$
2. What's the smallest field containing both $\mathbb{Q}$ and $\sqrt{2}$

Theorem

Let F, E be field and $E \subseteq F$, and $\alpha \in E$, then

1. $F[\alpha] = \{f(\alpha) \mid f(x) \in F[x]\}$ *is the smallest subring containing both F and α*
2. $F(\alpha) = \{f(\alpha)/g(\alpha) \mid f(x), g(x) \in F[x], g(\alpha) \neq 0\}$ *is the smallest field containing both F and α*

notice: if $F[\alpha]$ is already a field, then $F[\alpha] = F(\alpha)$

Answer: $\mathbb{Q}(\sqrt{2})$

Definition (extension)

Let F, E be fields. If F is a subfield of E, then E is an **extension field** of F. In the previous example, E is said to be obtained by adjoining α to F. If E is an extension of F, then we denote the field extension to be E/F.

Definition (algebraic extension & transcendental extension)

$\alpha \in E$ is **algebraic** over F if $\exists$ nonzero $f(x) \in F[x]$, s.t. $f(\alpha) = 0$.
A field extension E/F is called **algebraic** if every element in E is algebraic over F. Otherwise, it's called **transendental extension**.

Example

algebraic extension: $\mathbb{Q}(\sqrt{3})$ transcendental extension: $\mathbb{Q}(\pi)$

Theorem

(Papantonopoulou, p312) Let F be a subfield of E, and $\alpha \in E$ be algebraic over F,then exist unique monic polynomial $p(x) \in F[x]$, s.t.

- $p(\alpha) = 0$
- $p(x)$ *irreducible over* F
- *if* $f(x) \in F[x]$ *s.t.* $f(\alpha) = 0$, *then* $p(x)$ *divides* $f(x)$

Such $p(x)$ *is called the* **minimal polynomial** *of* α

Let α be a zero of an irreducible polynomial $p(x)$ over field F. Define $\phi : F[x] \mapsto \mathbb{C} : \phi(f(x)) = f(\alpha)$.
$Im(\phi) = \{f(\alpha) \, | f(x) \in F[x]\} = F[\alpha] = F(\alpha) \qquad Ker(\phi) =< p(x) >$
By FT of Ring Homomorphism, $Im(\phi) \cong F[x]/Ker(\phi)$, we have:

$$F(\alpha) \cong F[x]/ < p(x) >$$

Definition (degree of α and degree of E/F)

The of α over F, denoted as $deg\ F(\alpha)$ is $deg\ p(x)$, where $p(x)$ is the minimal polynomial of α over F. The degree of the field extension E/F is defined to the dimension of E over F, denoted as $[E : K]$

Theorem

Let $F \subseteq E$ be fields, $\alpha \in E$ be algebraic over F with $deg\ F(\alpha) = n$, then:

- $F(\alpha) \cong F[x]/ < p(x) >$
- $\{\alpha, \alpha^2, ..., \alpha^{n-1}\}$ *is a basis for vector space $F(\alpha)$ over F*
- $dim_F\ F(\alpha) = deg\ F(\alpha) = deg\ p(x)$

Definition (split)

Let F be a field, $f(x) \in F[x]$ a non-constant polynomial, and E an extension field of F. Then $f(x)$ **splits** over E if $f(x)$ can be factorized as:
$f(x) = u(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$, $u \in F$
(note: repeat roots allowed)

Definition (splitting field)

The extension field K is a **splitting field** for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors in $K[x]$ and K is the "smallest" such field.

Example

- $f(x) = x^2 - 2$: the splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$

Definition (Primitive)

A generator of the cyclic group of all the n^{th} roots of the unity. Let $\zeta_n = e^{2\pi i/n}$, then every other primitives should be ζ_n^k, where $\gcd(k, n) = 1$

Definition (Cyclotomic Field)

The splitting field of the polynomial $x^n - 1$ over $\mathbb{Q}$, denoted as $\mathbb{Q}(\zeta_n)$

Example (n=6, let $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$)

$\zeta_6 = e^{2\pi i/6} = \frac{1}{2} + \frac{\sqrt{3}}{2}i = -\omega^2$
$\zeta_6^2 = \omega \quad \zeta_6^3 = -1 \quad \zeta_6^4 = \omega^2 \quad \zeta_6^5 = -\omega \quad \zeta_6^6 = 1$
$\mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{3})$
$deg_{\mathbb{Q}}(\mathbb{Q}(\zeta_6)) = [E : K] = 2$

Definition (F-automorphism)

Let E be an extension field of F, then an automorphism $\phi : E \mapsto E$ is called F-**automorphism** if $\phi(a) = a$ for all $a \in F$

Notice:

- $Aut(E)$, the set of all automorphisms over E forms a group
- the set of all automorphisms that fix F forms a group
- the set of all F-automorphism is a subgroup of $Aut(E)$

Definition (Aut(E/F))

The set of all F-automorphism over E is denoted as $Aut(E/F)$

Definition (fixed field)

If H is a subgroup of $Aut(E)$, then the elements fixed by H forms a subfield of E, and is called **fixed field**, dentoted as E^H.

Property of F-automorphism

- for any $\phi \in Aut(E/F)$, $f(x) \in F[x]$, $\alpha \in E$, α is a zero of $f(x)$ if and only if $\phi(\alpha)$ is a zero of $f(x)$
  $\phi(f(\alpha)) = \phi(a_n\alpha^n + \cdots + a_1\alpha + a_0) = a_n(\phi(\alpha))^n + \ldots a_1\phi(\alpha) + a_0$

Theorem (for simple extension)

Let $E = F(\alpha)$, then for any $\phi \in Aut(E/F)$, ϕ is completely determined by $\phi(\alpha)$.

Theorem (for iterated extension)

Let $E = F(\alpha_1, \alpha_2, \ldots \alpha_s)$, then for any $\phi \in Aut(E/F)$, ϕ is completely determined by $\phi(\alpha_i)$, for $1 \leq i \leq s$.

Example ($\mathbb{Q}(\sqrt{2})$)

let $\delta(\sqrt{2}) = -\sqrt{2}$, $\iota(\sqrt{2}) = \sqrt{2}$, then
$|Aut(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

Question: $Aut|K/F| = [K : F]$? counterexample: $\mathbb{Q}(2^{1/3})$

Definition (separable)

Let $f(x) \in F[x]$ a polynomial over F. Then $f(x)$ is **separable** if all its zeros have multiplicity 1 in its splitting field. An element $\alpha \in F$ is **separable** if its *minimal polynomial* is separable.

useful technique: for irreducible $f(x) \in F[x]$, $f(x)$ is separable iff $f'(x)$ is not zero polynomial. If char F=0, then irreducible $f(x)$ is separable over F

Theorem

E is the splitting field of separable $f(x)$ over F $\implies |Aut(E/F)| = [E : F]$

Definition (**Galois extension** & **Galois group**)

Let E be a field extension of F, E is **Galois** if $|\mathrm{Aut}(E/F)| = [E : F]$. If E is a Galois extension of F, then $Aut(E/F)$ is called Galois group, and denoted as $Gal(E/F)$

Properties of Galois extension E/F (Dummit and Foote, p574)

- K is the splitting field of a separable polynomial over F
- fields where F is the set of elements precisely fixed by $Aut(E/F)$
- finite, normal, separable extension

Theorem (Fundamental Theorem of Galois Theory)

Let E be a Galois extension of a field F then there exists a bijection between the normal subgroup of the Galois group H and the intermediate extension K/F.

1. *For any subgroup H of Gal(E/F), the corresponding fixed field, denoted E^H, is the set of those elements of E which are fixed by every automorphism in H.*
2. *For any intermediate field K of E/F, the corresponding subgroup is Aut(E/K), that is, the set of those automorphisms in Gal(E/F) which fix every element of K.*

Example ($\mathbb{Q}(\sqrt{2}, \sqrt{3})$)

$$f = \begin{cases} f(\sqrt{2}) = -\sqrt{2} \\ \mathrm{f}(\sqrt{3}) = \sqrt{3} \end{cases} \qquad g = \begin{cases} g(\sqrt{2}) = \sqrt{2} \\ \mathrm{g}(\sqrt{3}) = -\sqrt{3} \end{cases}$$

Then $Aut(\mathbb{Q}(\sqrt{2}, \sqrt{3})) = \{1, f, g, fg\}$, and

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{3}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash] & \mathbb{Q}(\sqrt{2}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
& \{1\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\{1, f\} \arrow[dr, dash] & \{1, fg\} \arrow[d, dash] & \{1, g\} \arrow[dl, dash] \\
& \{1, f, g, fg\} &
\end{tikzcd}$$

Theorem

(Dummit and Foote, p596)
The Galois group of the cyclotomic field $\mathbb{Q}(\zeta_n)$ of n^{th} roots of unity is isomorphic to the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$. The isomorphism is explicitly given by the map: $\phi : (\mathbb{Z}/n\mathbb{Z})^\times \mapsto Gal(\mathbb{Q}[\zeta_n]/\mathbb{Q})$, where $\phi(a) = \sigma_a$, and $\sigma_a(\zeta_n) = (\zeta_n)^a$ (note: ζ_n is primitive n^{th} root and $\gcd(a, n) = 1$*)*

Proof.

1. ϕ is well-defined, since ζ_n is a primitive n^{th} root, σ_a is indeed an automorphism on cyclotomic field.
2. ϕ is homomorphism: $(\sigma_a\sigma_b)(\zeta_n) = \sigma_a(\zeta_n^b) = (\zeta_n^b)^a = (\zeta_n)^{ab} = \sigma_{ab}(\zeta_n)$
3. ϕ is bijection

$\square$

Definition (Legendre symbol)

Let p be an odd prime, for any interger a, define:

$$(\frac{a}{p}) = \begin{cases} 1 & \text{if } p \nmid \text{ and } x^2 \equiv a \mod p \text{ is solvable} \\ \text{-1} & \text{if } p \nmid \text{ and } x^2 \equiv a \mod p \text{ is not solvable} \\ 0 & \text{if } p \mid a \end{cases}$$

Theorem (Quadratic Reciprocity Law)

Let $p \neq q$ also be odd prime. **Quadratic Reciprocity Law** *states that:*

$$(\frac{q}{p})(\frac{p}{q}) = \begin{cases} -1 & \textit{if both } p, q \equiv 3 \mod 4 \\ 1 & \textit{if either } p \equiv 1 \mod 4 \textit{ or } q \equiv 1 \mod 4 \end{cases}$$

Example

Let $p = 3, q = 7$,

then by definition: $(\frac{7}{3})$=1, because $4^2 = 7 + 3 * 3$

then by Q.R.: because both $4, 7 \equiv 4 \mod 3$, then $(\frac{3}{7})(\frac{7}{3}) = -1$

so $(\frac{3}{7}) = -1$, so 7x+3 cannot be a square for any $x \in \mathbb{Z}$

Lemma

Let Z be a cyclic group of even order, Z has a unique element of order 2, denoted as "-1". If $a \in Z$, then $x^2 \equiv a$ has two solutions if $a^n = 1$ and no solution if $a^n = -1$

by lemma, q be odd prime, $Z = F_q^\times$, then we'll have: $(\frac{a}{q}) \equiv a^{\frac{q-1}{2}} \mod q$
by $(\frac{ab}{q}) = (\frac{a}{q})(\frac{b}{q})$: we have $(\frac{-1}{q}) = (-1)^{\frac{q-1}{2}}$

recall the isomorphism: $\phi : (\mathbb{Z}/n\mathbb{Z})^\times \mapsto \text{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$, where $\phi(a) = \sigma_a$, and $\sigma_a(\zeta_n) = (\zeta_n)^a$, let R=$\mathbb{Z}[\zeta]$. By applying the theorem, for $u \in R$, we can have $u^q - \delta_1(u)$ is a multiple of q in R

Define: $G = \sum_{a \mod p} (\frac{a}{p})\zeta^a$, also denote $p^* = \begin{cases} \text{p} & \text{if } p \equiv 1 \mod 4 \\ \text{-p} & \text{if } p \equiv 3 \mod 4 \end{cases}$, *then* $G^2 = p^*$ and we can deduce that $\sqrt{p^*} \subseteq \mathbb{Q}[\zeta_p]$.

We can also prove that $\delta_q(G) = (\frac{q}{p})G \implies \delta_q(G) = (\frac{q}{p})\sqrt{p^*}$. Thus we can prove the quadratic reciprocity law.