Galois Theory workshop

zc231

Contents

1 Before the workshop

We will assume basic theorems of rings, modules and some linear algebra. This includes

1. Polynomial ring. If K is a field then $K[X]$ is a Euclidean domain (and so a principal ideal domain). Let $f(X) \in K[X]$ be an irreducible polynomial, then the ideal $\langle f(X) \rangle$ is maximal.

2. Division Algorithm of polynomials. Let K be a field, and $f(X) \in K[X]$ be a polynomial of degree n. Then for any polynomial $g(X) \in K[X]$, there exist $q(X), r(X) \in K[X]$ such that

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

   where either $r(X) = 0$ or $\deg r(X) < \deg f(X)$.

3. Gauss's lemma: For each primitive polynomial $f(X) \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$, $f(X)$ is irreducible in $\mathbb{Z}[X]$ if and only if $f(X)$ is irreducible in $\mathbb{Q}[X]$.

4. Eisenstein criterion: Let

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0, a_i \in \mathbb{Z}$$

be a primitive polynomial with integer coefficients. If there exists a prime number p such that

(i) p does not divide a_n,

(ii) p divides a_i for each $i \neq n$,

(iii) p^2 does not divide a_0,

then $f(X)$ is irreducible.

5. Any non-trivial field homomorphism is injective.

6. Application of rank-nullity theorem

(i) If K be a finite integral domain, then K is a field.

(ii) Let L_1, L_2 be vector spaces over K such that $\dim_K(L_1) = \dim_K(L_2)$. If $\sigma : L_1 \to L_2$ is an injective K-linear map, then σ is an isomorphism.

2 Things we are going to cover (summary)

We will cover the following topics with examples in this workshop. Field extensions, Tower law, Algebraic extensions, Separability and primitive element theorem, Automorphism of fields, Galois extension, Fundamental theorem of Galois, Finite fields, Cyclotomic Extensions and Kummer Theory.

3 Field extensions

Definition 3.1 (**Simple Extension**). *Let K be a field and so $K[X]$ is a principal ideal domain. Let $f(X) \in K[X]$ be an irreducible polynomial so $\langle f(X)\rangle$ is a maximal ideal. Let α be a root of $f(X)$ and n be the degree of f. Then*

$$L = K(\alpha) := \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in K\}$$

is a field extension of K. Note that L is a K-vector space with basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

We have an isomorphism

$$K[X]/\langle f(X)\rangle \cong K(\alpha), \quad g(X) + \langle f(X)\rangle \mapsto g(\alpha).$$

We will mainly focus on the case $K = \mathbb{Q}$.

Example 3.2. *The ring $\mathbb{Q}[X]$ is a principal ideal domain and $X^2 + 1$ is an irreducible polynomial. So $\langle X^2 + 1\rangle$ is a maximal ideal and $\mathbb{Q}[X]/\langle X^2 + 1\rangle$ is a field. We have an isomorphism*

$$\mathbb{Q}[X]/\langle X^2 + 1\rangle \cong \mathbb{Q}(i) := \{a + bi : a, b \in \mathbb{Q}\}, a + bX \mapsto a + bi.$$

For example, by division algorithm

$$X^2 + 2X + 1 = (X^2 + 1) + 2X$$

and so $2X$ is a representative of $X^2 + 2X + 1$ for $\mathbb{Q}[X]/\langle X^2 + 1\rangle$. So

$$X^2 + 2X + 1 = (X^2 + 1) + 2X \mapsto 2i.$$

Remark 3.3. *We should NOT distinguish between i and $-i$. They should only be considered as roots of $X^2 + 1$ and the i in the above example is just a fixed choice of a root of $X^2 + 1$.*

More generally,

Definition 3.4. *Let L be a field. If a subring K of L is a field, we call K a subfield of L and L is a field extension of K. We refer to the pair as an extension L/K (L over K).*

4 Tower law

Definition 4.1. *Let $L = K(\alpha)$ be a simple extension of K such that there exists a monic irreducible polynomial $f(X) \in K[X]$ with $f(\alpha) = 0$ ($f(X)$ is called the minimal polynomial of α). Then the* **degree** *of the extension L/K, written $[L : K]$, is defined as the degree of $f(X)$. Equivalently, $[L : K]$ is the dimension of L as K-vector space.*

Example 4.2. *Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ and the degree $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}]$.*

More generally,

Definition 4.3. *Let L/K be a field extension. We say L/K is a finite extension if L is a finite K-vector space; otherwise L/K is infinite. In the case when L/K is finite, the* **degree** *of L/K, written $[L : K]$, is the dimension of L as K-vector space.*

Lemma 4.4 (**Tower Law**). *Let $F/L/K$ be field extensions. Then*

$$[F : K] = [F : L][L : K].$$

Exercise 4.5. *Let $K(\alpha)/K$ be a finite extension of odd degree. Then $K(\alpha) = K(\alpha^2)$.*

5 Algebraic extensions

Definition 5.1. *Let K be a field. We say α is algebraic over K if there exists a polynomial $f(X) \in K[X]$ such that $f(\alpha) = 0$.*

We say L/K is an algebraic extension if α is algebraic over K for all $\alpha \in L$.

Example 5.2. *$\sqrt[3]{2}$ is algebraic over $\mathbb{Q}$ because it is a root of $X^3 - 2$.*

Lemma 5.3. *α, β are algebraic over K if and only if $\alpha + \beta, \alpha\beta$ are both algebraic over K.*

This shows that the set of algebraic numbers over $\mathbb{Q}$ is a field.

Example 5.4. *We have seen that $\sqrt{2} + \sqrt{3}$ is a root of $x^4 - 10x^2 + 1 = 0$. In fact we can see that this is algebraic before we did the computation because $\sqrt{2}, \sqrt{3}$ are both algebraic.*

Proposition 5.5. *If L/K is a finite extension, then it is an algebraic extension.*

Remark 5.6. *The converse is not true. For example,*

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \ldots)$$

is an infinite algebraic extension.

6 Separability and primitive element theorem

Definition 6.1. *Let K be a field. We say $f(X) \in K[X]$ is separable if $f(X)$ has no repeated root in any field extension L/K. Let α be algebraic over K. We say α is separable over K if the minimal polynomial of α is separable. Finally, L/K is a a separable extension if every element of L is separable over K.*

Lemma 6.2. *Let K be a field of characteristic zero and L/K a field extension of K. Then L/K is a separable extension.*

Since we mainly focus on the case $K = \mathbb{Q}$, so every finite extension of $\mathbb{Q}$ is separable. A finite extension of $\mathbb{Q}$ is called a **number field**.

Theorem 6.3 (Primitive element theorem). *Let L/K be a finite separable extension. Then $L = K(\alpha)$ for some α.*

Remark 6.4. *α is not unique. For example, $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{3} - \sqrt{2})$.*

Example 6.5. *Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Find α such that $L = \mathbb{Q}(\alpha)$.*

Exercise 6.6. *Let p and q be distinct primes. Find α such that*

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{p}, \sqrt{q}).$$

7 Automorphisms of fields

Definition 7.1. *Let $L/K, L'/K$ be field extensions over K. We say $\sigma : L \to L'$ is a K-homomorphism if σ is a ring homomorphism such that $\sigma(x) = x$ for all $x \in K$. The set of (non-zero) K-homomorphisms from L to L' is denoted by $Hom_K(L, L')$. In the case when $L' = L$ and σ is a ring isomorphism, we say that σ is a K-automorphism of L. The set of K-automorphism of L is denoted by $Aut_K(L)$.*

Remark 7.2. *By using rank-nullity and the fact that any K-homomorphism is injective, we conclude that $Hom_K(L, L) = Aut_K(L)$.*

Example 7.3. *Let $\sqrt{2}$ be a root of $X^2 - 2 = 0$ and $L = \mathbb{Q}(\sqrt{2})$, considered as a subfield of $\mathbb{C}$. Then*

$$Hom_{\mathbb{Q}}(L, \mathbb{C}) = \{\sigma = id, \quad \tau : \sqrt{2} \mapsto -\sqrt{2}\}.$$

Example 7.4. *Can you find a non-trivial K-automorphism of L where $L = \mathbb{Q}(\sqrt[3]{2})$ where $\sqrt[3]{2}$ is a fixed choice of a root of $X^3 - 2 = 0$.*

Lemma 7.5. *Let $L = K(\alpha)$ be a field extension of K. If σ is a K-automorphism of L, then we must have $\sigma(\alpha) = \beta$ where β is a root of $f(X)$ in L and $f(X)$ is the minimal polynomial of α over K.*

Proof. Since σ is a K-automorphism, we have

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$$

and so $\sigma(\alpha)$ must be a root of $f(X)$ in L. □

In the case when $K = \mathbb{Q}$, the map $\sigma : \alpha \mapsto \beta$ extends to a K-homomorphism from L to $\mathbb{C}$. The above lemma shows that

Lemma 7.6. *Let $L/K, L'/K$ be field extensions of K. Let $K \subset F \subset L$ and $\alpha \in L$ be algebraic over F with minimal polynomial $f(X) \in F[X]$.*

Then for every $\tau \in Hom_K(F, L')$ we have a bijection:

$$\{\rho \in Hom_K(F(\alpha), L') : \rho\big|_F = \tau\} \ni \rho \mapsto \rho(\alpha) \in Root_{(\tau f)}(L').$$

Example 7.7. *Let $K = F = \mathbb{Q}(\sqrt{2})$ and $\alpha = \sqrt[4]{2}$. Then $L = \mathbb{Q}(\sqrt[4]{2})$ and $f(X) = X^2 - \sqrt{2}$. Let $L' = \mathbb{Q}(i\sqrt[4]{2})$. Let τ be the natural injection $F \hookrightarrow L'$. Suppose ρ is a F-homomorphism from L to L', then ρ must be an isomorphism (Rank Nullity). Then the above lemma tells us that ρ must correspond to a root of $f(X) = X^2 - \sqrt{2}$ in L'. However, L' does not contain any root of $f(X)$ because otherwise $L' \supset L$ and so $L' = L$ by using tower law $[L' : \mathbb{Q}] = [L' : L][L : \mathbb{Q}]$, which is impossible because L is real but L' is not. Therefore we conclude that L is not F-isomorphic to L'. Nonetheless, L and L' are $\mathbb{Q}$-isomorphic because they are both isomorphic to $\mathbb{Q}[X]/\langle X^4 - 2\rangle$.*

Proposition 7.8. *Let L/K be a finite extension. Then*

$$Hom_K(L, L') \leq [L : K]$$

for any extension L'/K. Moreover, if L/K is a separable extension, then equality holds for some extension L'/K.

Proof. We sketch the proof for the case L/K is a finite separable extension. By primitive element theorem we can write $L = K(\alpha)$ for some $\alpha \in L$. Let $f(X)$ be the minimal polynomial of α. Take $F = K$ and τ as the natural injection $K \hookrightarrow L'$, then we have a bijection between $\mathrm{Hom}_K(L, L')$ and the set of roots of $f(X)$ in L'. So the number of $\mathrm{Hom}_K(L, L')$ is at most the degree of $f(X)$, which is $[L : K]$. In particular, equality holds if we take L' to be the field which contains every root of $f(X)$. □

Example 7.9. *Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Describe $Aut_K(L)$.*

8 Galois extensions

We will mainly focus on finite Galois extension.

Definition 8.1. *Let L/K be a finite separable extension so by primitive element theorem we write $L = K(\alpha)$ for some α. Let $f(X)$ be the minimal polynomial of α. We say L/K is* **Galois** *if every root of $f(X)$ lies in L. Equivalently,*

$$|Aut_K(L)| = [L : K].$$

Moreover, one can show that L/K is Galois if and only if $L = K(\alpha_1, \ldots, \alpha_n)$ and every root of $f_i(X)$ is contained in L, where $f_i(X)$ is the minimal polynomial of α_i.

Example 8.2. *Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$. Then L/K is Galois. Indeed,*

$$\zeta_3, \zeta_3^2, \sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2} \in L.$$

Remark 8.3. *A tower of Galois extensions is not necessarily Galois. For example, $L = \mathbb{Q}(\sqrt[4]{2}), F = \mathbb{Q}(\sqrt{2})$ and $K = \mathbb{Q}$. Then L/F and F/K are both Galois but L/K is not.*

Definition 8.4. *Let L/K be a finite Galois extension. The* **Galois group** *of L/K, written $\mathrm{Gal}(L/K)$, is the group of K-automorphisms $Aut_K(L)$.*

Example 8.5. *Find the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q})$.*

Definition 8.6. *Let K be a field. Then splitting field of a polynomial $f(X) \in K[X]$ is the smallest field which contains every root of $f(X)$. In other words, if $\alpha_1, \ldots, \alpha_n$ are roots of $f(X)$, then the splitting field of $f(X)$ is $K(\alpha_1, \ldots, \alpha_n)$.*

Example 8.7. *The splitting field of $X^3 - 2 \in \mathbb{Q}[X]$ is $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$.*

Exercise 8.8. *Find the Galois group $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ where α is a root of $X^4 - 2X^2 + 25 = 0$.*

9 Fundamental theorem of Galois

Definition 9.1. *Let L/K be a finite Galois extension and $G = \mathrm{Gal}(L/K)$. Let H be a subgroup of $\mathrm{Gal}(L/K)$. We write L^H to be the fixed subfield of H, i.e.*

$$L^H = \{x \in L : \sigma(x) = x \text{ for all } \sigma \in H\}.$$

Theorem 9.2 (**Fundamental theorem of Galois**). *Let L/K be a finite Galois extension.*

1. *We have a one-to-one correspondence between the subgroup of $\mathrm{Gal}(L/K)$ and the intermediate extension F (i.e. $K \subset F \subset L$). More explicitly, each subgroup H of $\mathrm{Gal}(L/K)$ corresponds to the fixed field L^H.*
2. *L/L^H is Galois with Galois group H and $[L : L^H] = |H|$.*
3. *L^H/K is Galois if and only if H is a normal subgroup of $\mathrm{Gal}(L/K)$.*

Example 9.3. *Illustrate the Galois correspondence of $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}$.*

Exercise 9.4. *Illustrate the Galois correspondence of $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}$.*

10 Finite Fields

Example 10.1. *Let p be a prime. Then $\mathbb{Z}/p\mathbb{Z}$ is a field of p elements. In fact, every field of p elements is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ and we write this field as $\mathbb{F}_p$.*

Lemma 10.2. *If K is a field of q elements, then $q = p^d$ for some $d \geq 1$ where p a prime and is the characteristic of K.*

Lemma 10.3.
1. *There exists a field with q elements, unique up to $\mathbb{F}_p$-isomorphism. We denote this field by $\mathbb{F}_q$. Explicitly, we can take the set of all roots $\{x \in K : x^q = x\}$, which is a field of q elements.*
2. *Let $d, d' \geq 1$ and $q = p^d, q' = p^{d'}$. Then $\mathbb{F}_{q'}$ contains $\mathbb{F}_q$ if and only if q' is a power of q, i.e. $d|d'$. If $q' = q^n$, then $[\mathbb{F}_{q'} : \mathbb{F}_q] = n$.*
3. *The field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is Galois with cyclic Galois group $\mathbb{Z}/n\mathbb{Z}$, generated by the Frobenius automorphism*
$$Fr_q : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, \quad x \mapsto x^q.$$

Example 10.4. *$\mathbb{F}_2(\zeta_3) = \mathbb{F}_{2^2}$ because ζ_3 is a root of $X^2 + X + 1 = 0$ and $X^2 + X + 1$ is irreducible over $\mathbb{F}_2$. So $\mathbb{F}_2(\zeta_3)$ is a degree 2 extension of $\mathbb{F}_2$, which is $\mathbb{F}_4$ (up to isomorphism).*

Exercise 10.5. *Let $K = \mathbb{F}_2[X]$ and $f(X) = X^5 + X^4 + 1 \in K[X]$. Find the splitting field of $f(X)$.*

11 Cyclotomic Extension

By cyclotomic extension we mean a field extension of the form $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

Theorem 11.1. *Let $L = \mathbb{Q}(\zeta_n)$. Then $L/\mathbb{Q}$ is Galois with Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$. Explicitly, we have an isomorphism*
$$\mathrm{Gal}(L/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times, (\zeta_n \mapsto \zeta_n^j) \mapsto j.$$

Example 11.2. *Let $L = \mathbb{Q}(\zeta_5)$. Then $L/\mathbb{Q}$ is Galois with Galois group $(\mathbb{Z}/5\mathbb{Z})^\times$, generated by $\zeta_5 \mapsto \zeta_5^2$. We have a subgroup of order 2, $H = \{4, 1\}$ and we shall find the subfield corresponding to H. Can we find an element not in $\mathbb{Q}$, but fixed by elements in H?*

Exercise 11.3. *Illustrate Galois correspondence for $\mathbb{Q}(\zeta_{12})/\mathbb{Q}$. (Beware: $\zeta_{12} + \zeta_{12}^7 = 0$)*

12 Kummer theory

Theorem 12.1 (Kummer theory). *Let $\mu_n \subset K$ with $(charK, n) = 1$. If F/K is cyclic (that is, a Galois extension with cyclic Galois group) of degree n, then $F = K(\sqrt[n]{a})$ for some $a \in K$.*

Example 12.2. *Let $K = \mathbb{Q}(\zeta_3)$ and $L = K(\alpha)$ where α is a root of $f(X) = X^3 + X + 1$. Let α be a root of $f(X)$. Then $\alpha^2 - 2$ and $-\alpha^2 - \alpha + 2$ are also roots and so $L = K(\alpha)$ is Galois over K. By Kummer theory we search for an element $a \in K$ such that $L = K(\sqrt[3]{a})$. Let σ be a generator of $\mathrm{Gal}(L/K)$ such that*
$$\sigma : \alpha \mapsto \alpha^2 - 2.$$
Let
$$x = \alpha + \zeta_3\sigma(\alpha) + \zeta_3^2\sigma^2(\alpha).$$
Then $\sigma(x) = \zeta_3^2 x$ and so $\sigma(x^3) = x^3$. This shows that x^3 is fixed by σ and hence fixed by $\mathrm{Gal}(L/K)$. So $x^3 \in K$ by fundamental theorem of Galois. A direct computation shows that $x^3 = 27\zeta_3$ and so we can write $L = K(\sqrt[3]{\zeta_3})$.