

M3P11 Galois Theory

Lectured by Prof Alessio Corti

Typeset by David Kurniadi Angdinata

Spring 2019

Contents

0	What is Galois theory?	3
1	Elementary facts	9
2	Axiomatics	11
3	Galois correspondence	14

0 What is Galois theory?

Lecture 1
Thursday
10/01/19

The following are references.

- E Artin, Galois theory, 1994
- A Grothendieck and M Raynaud, Revêtements étales et groupe fondamental, 2002
- I N Herstein, Topics in algebra, 1975
- M Reid, Galois theory, 2014

Notation. If K is a field, or a ring, I denote

$$K[x] = \{a_0 + \cdots + a_n x^n \mid a_i \in K\},$$

the ring of polynomials with coefficients in K .

Example.

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- Quadratic fields

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} = \frac{\mathbb{Q}[x]}{\langle x^2 - 2 \rangle}.$$

It is also a field, since

$$\frac{1}{(a + b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}.$$

- If p is prime, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a finite field. If $f(x) \in K[x]$ is irreducible, $K[x]/\langle f(x) \rangle$ is a field. For example, $x^2 - 2$. Both \mathbb{Z} and $K[x]$ have a division algorithm. For example, let $[a] \in \mathbb{Z}/p\mathbb{Z}$ and $[a] \neq 0$, that is $p \nmid a$. Since p is prime, $\gcd(p, a) = 1$, so there exist $x, y \in \mathbb{Z}$ such that $ax + py = 1$. Thus $[a] \cdot [x] = 1$ in $\mathbb{Z}/p\mathbb{Z}$.
- For K a field, either for all $m \in \mathbb{Z}$, $m \neq 0$ in K , so K has characteristic $\text{ch}(K) = 0$, or there exists p prime such that $m = 0$ if and only if $p \mid m$, so K has characteristic $\text{ch}(K) = p$.
- For K a field,

$$K(x) = \text{Frac}(K[x]) = \left\{ \phi(x) = \frac{f(x)}{g(x)} \mid f, g \in K[x], g \neq 0 \right\}.$$

is also a field, the field of rational functions with coefficients in K . For example, $\mathbb{F}_p(x, Y) = \mathbb{F}_p(x)(Y)$.

Example. Consider algebraic equations in a field K .

- Let $ax^2 + bx + c = 0$ for $a, b, c \in K$ be a quadratic. There is a formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

- For a cubic $y^3 + 3py + 2q = 0$,

$$y = \sqrt[3]{-q + \sqrt{q^2 + p^3}} + \sqrt[3]{-q - \sqrt{q^2 + p^3}}.$$

- There is a formula for quartic equations.
- It is a theorem that there can be no such formula for equations of degree at least five.

Galois theory deals with these easily.

Lecture 2
Friday
11/01/19

Definition 0.1. A **field homomorphism** is a function $\phi : K_1 \rightarrow K_2$ that preserves the field operations, for all $a, b \in K_1$,

$$\begin{aligned}\phi(a + b) &= \phi(a) + \phi(b), \\ \phi(ab) &= \phi(a)\phi(b),\end{aligned}$$

and $\phi(0_{K_1}) = 0_{K_2}$ and $\phi(1_{K_1}) = 1_{K_2}$.

Remark. All field homomorphisms are injective. If $a \in K_1 \setminus \{0\}$, then there exists $b \in K_1$ such that $ab = 1$, then $\phi(a)\phi(b) = 1$, so $\phi(a) \neq 0$. This easily implies ϕ is injective. If $a_1 \neq a_2$, then $a_1 - a_2 \neq 0$, so $0 \neq \phi(a_1 - a_2) = \phi(a_1) - \phi(a_2)$. Then $\phi(a_1) \neq \phi(a_2)$.

We concern ourselves with field extensions $k \subset K$, and every homomorphism is an extension. Consider a field extension $k \subset K$ and $\alpha \in K$. Then $k(\alpha) \subset K$ denotes the smallest subfield of K that contains k, α . Not to be confused with $k(x)$.

Example. There are two very different cases exemplified in $\mathbb{Q} \subset \mathbb{C}$.

- $\alpha = \sqrt{2}, \mathbb{Q}(\sqrt{2})$.
- $\alpha = \pi, \mathbb{Q}(\pi)$.

Definition 0.2.

- α is **algebraic** over k if $f(\alpha) = 0$ for some $0 \neq f \in k[x]$. Otherwise we say that α is **transcendental** over k .
- The extension $k \subset K$ is **algebraic** if for all $\alpha \in K$, α is algebraic over k .

Definition 0.3. Consider a field k and $f \in k[x]$. We say that $k \subset K$ is a **splitting field** for f if

- $f(x) = a \prod_{i=1}^n (x - \lambda_i) \in K[x]$ for $a \in k \setminus \{0\}$, and
- $K = k(\lambda_1, \dots, \lambda_n)$.

Example.

- If $f(x) = x^2 - 2 \in \mathbb{Q}[x]$, then $K = \mathbb{Q}(\sqrt{2})$ is a splitting field for f . Indeed

$$x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2}) \in \mathbb{Q}(\sqrt{2})[x].$$

- If $f(x) = x^2 + 2$, then $K = \mathbb{Q}(\sqrt{-2})$.
- If $f(x) = x^3 - 2$, then

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$$

is not a splitting field. $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$, where $\omega = \frac{-1+\sqrt{3}}{2}$, is a splitting field.

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2}).$$

Theorem 0.4 (Fundamental theorem of Galois theory). Assume characteristic zero. Let $k \subset K$ be the splitting field of $f(x) \in k[x]$. Let

$$G = \{\sigma : K \rightarrow K \mid \sigma \text{ field automorphism, } \sigma|_k = id_k\}.$$

We call this group the **Galois group**. There is a one-to-one correspondence

$$\begin{aligned} \{k \subset K_1 \subset K \mid K_1 \text{ subfield}\} &\leftrightarrow \{H \leq G \mid H \text{ subgroup}\} \\ K_1 &\mapsto \{\sigma \in G \mid \forall \lambda \in K_1, \sigma(\lambda) = \lambda\} \\ \{\lambda \in K \mid \forall \sigma \in H, \sigma(\lambda) = \lambda\} &\leftarrow H \leq G \end{aligned}$$

Why is this cool? Fields are hard, groups are easy. We will see that there is a good formula for the roots of $f(x)$ if and only if G is a soluble group.

Example. Let $\deg(f) = 2$ and $f(x) = x^2 + 2Ax + B \in K[x]$. If K already contains the roots then $L = K$ and $G = \{id\}$. Suppose K does not contain the roots. We still have quadratic formula

$$\lambda_{1,2} = -A \pm \sqrt{A^2 - B}.$$

If $\Delta = A^2 - B$ then $\sqrt{\Delta}$ does not exist in K . We must have

$$L = K(\sqrt{\Delta}) = \{a + b\sqrt{\Delta} \mid a, b \in K\}.$$

Then $K \subset L$ and

$$G = \{\sigma : L \rightarrow L \mid \sigma|_K = id_K\} = C_2$$

is generated by

$$\sigma : a + b\sqrt{\Delta} \mapsto a - b\sqrt{\Delta}.$$

Further specialisation is the following.

- Let $K = \mathbb{R}$ and $\Delta = -1$. Then

$$L = \mathbb{C} = \{a + b\sqrt{-1} \mid a, b \in \mathbb{R}\},$$

and $G = C_2$ is generated by

$$\sigma : a + b\sqrt{-1} \mapsto a - b\sqrt{-1},$$

complex conjugation.

- Let $K = \mathbb{Q}$ and $\Delta = 2$. Then

$$L = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\},$$

and $G = C_2$ is generated by

$$\sigma : a + b\sqrt{2} \mapsto a - b\sqrt{2}.$$

The fundamental theorem implies there does not exist

$$K \subsetneq K_1 \subsetneq K(\sqrt{\Delta}) = L.$$

Is this obvious? Consider $x \in L \setminus K$, so $x = a + b\sqrt{\Delta}$, and $b \neq 0$, and then

$$\sqrt{\Delta} = \frac{x - a}{b},$$

so $K(x) = L$.

Example. Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ and $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$, where $\omega = \frac{-1+i\sqrt{3}}{2}$ is a solution of $x^2 + x + 1 = 0$. Then

$$\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3}), \quad \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}.$$

Lecture 3
Tuesday
15/01/19

Remark. For any splitting field of f , there is always a natural inclusion group homomorphism

$$\rho : G \hookrightarrow S(\lambda_1, \dots, \lambda_n),$$

where $S(\lambda_1, \dots, \lambda_n)$ is the group of permutations of the roots of $f = x^n + a_1 x^{n-1} + \dots + a_n$.

- If $\sigma \in G$, $f(\lambda) = 0$, so $\lambda^n + a_1 \lambda^{n-1} + \dots + a_n = 0$.

$$0 = \sigma(0) = \sigma(\lambda^n + a_1 \lambda^{n-1} + \dots + a_n) = \sigma(\lambda)^n + a_1 \sigma(\lambda)^{n-1} + \dots + a_n.$$

- ρ is injective. If for all i , $\sigma(\lambda_i) = \lambda_i$, then $\sigma = id$ on $K(\lambda_1, \dots, \lambda_n) = L$.

The fundamental theorem and remark gives $G = \mathfrak{S}_3$.

Definition 0.5. $K \subset L$ is **finite** if L is finite-dimensional as a vector space over K . The **degree** of L over K is $[L : K] = \dim_K(L)$.

Lecture 4
Thursday
17/01/19

Two things about this.

Theorem 0.6 (Tower law). Let $K \subset L \subset F$. Then $[F : K] = [F : L][L : K]$.

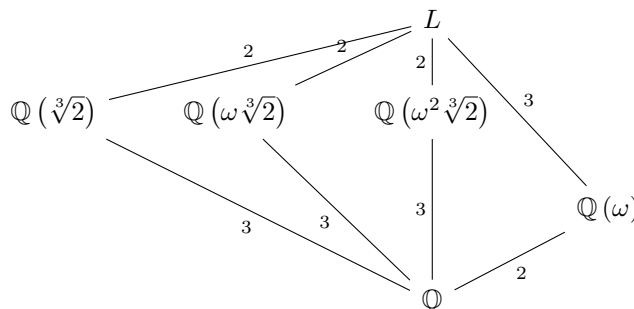
Theorem 0.7. Suppose $f(x) \in K[x]$ is irreducible of degree $d = \deg(f)$ and $L = K(\lambda)$ where $f(\lambda) = 0$, then $[K(\lambda) : K] = d$.

Example.

$$K = \mathbb{Q}(\sqrt[3]{2}) = \left\{ a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q} \right\}$$

is a field, and $[K : \mathbb{Q}] = 3$.

Example. Let $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ be the splitting field of $x^3 - 2$ over \mathbb{Q} . The lattice of subfields is



Then

$$\mathbb{Q}(\sqrt[3]{2} + \omega) = L, \quad \mathbb{Q}(\omega^2 \sqrt[3]{2}) \cap \mathbb{Q}(\omega \sqrt[3]{2}) = \mathbb{Q}, \quad \mathbb{Q}(\sqrt[3]{2}, \omega \sqrt[3]{2}) = L.$$

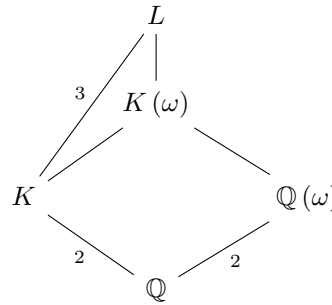
(Exercise) What is $[L : \mathbb{Q}(\sqrt[3]{2})]$? Note that $L = \mathbb{Q}(\sqrt[3]{2})(\sqrt{-3})$. Could $\sqrt{-3} \in \mathbb{Q}(\sqrt[3]{2})$? Consider $x^2 + 3 \in \mathbb{Q}(\sqrt[3]{2})[x]$. By the tower law,

$$\begin{cases} [L : \mathbb{Q}] = [L : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}] = 2[L : \mathbb{Q}(\omega)] & \implies 2 \mid [L : \mathbb{Q}] \\ [L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3[L : \mathbb{Q}(\sqrt[3]{2})] & \implies 3 \mid [L : \mathbb{Q}] \end{cases} \implies 6 \mid [L : \mathbb{Q}].$$

- Either $x^2 + 3$ is irreducible over $\mathbb{Q}(\sqrt[3]{2})$, so by Theorem 0.7 $[L : \mathbb{Q}(\sqrt[3]{2})] = 2$ and $[L : \mathbb{Q}] = 6$.
- Or $x^2 + 3$ is not irreducible, so $\mathbb{Q}(\sqrt[3]{2}) = L$ and $[L : \mathbb{Q}] = 3$, a contradiction.

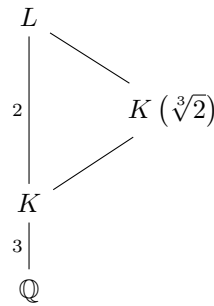
Are there any other fields? Claim that there are no other fields. Suppose $\mathbb{Q} \subsetneq K \subsetneq L$ is such a field. By the tower law $[K : \mathbb{Q}] = 2$ or $[K : \mathbb{Q}] = 3$.

- Suppose $[K : \mathbb{Q}] = 2$.



- Either $\omega \in K$, that is $\mathbb{Q}(\omega) \subset K$, so by the tower law $\mathbb{Q}(\omega) = K$.
- Or $\omega \notin K$ gives $[K(\omega) : K] = 2$, so $[K(\omega) : \mathbb{Q}] = 4$ contradicts the tower law for $\mathbb{Q} \subset K(\omega) \subset L$.

- Suppose $[K : \mathbb{Q}] = 3$.



Claim that $x^3 - 2 \in K[x]$ splits. Suppose that it were irreducible, then $[K(\sqrt[3]{2}) : K] = 3$, which contradicts the tower law for $K \subset K(\sqrt[3]{2}) \subset L$. So it has a root in K . Either $\sqrt[3]{2} \in K$, $\omega\sqrt[3]{2} \in K$, or $\omega^2\sqrt[3]{2} \in K$. Thus $\mathbb{Q}(\sqrt[3]{2}) = K$, $\mathbb{Q}(\omega\sqrt[3]{2}) = K$, or $\mathbb{Q}(\omega^2\sqrt[3]{2}) = K$.

I want to prove that

$$G = \text{Aut}_{\mathbb{Q}}(L) = \{\sigma : L \rightarrow L \mid \sigma|_{\mathbb{Q}} = \text{id}_{\mathbb{Q}}\} = \mathfrak{S}_3.$$

Proof of Theorem 0.6. Suppose $y_1, \dots, y_m \in F$ is a basis of F as a vector space over L . Suppose $x_1, \dots, x_n \in L$ is a basis of L as a vector space over K . Claim that $\{x_i y_j\}$ is a basis of F over K .

- $\{x_i y_j\}$ generates F . Let $z \in F$. There exist $\mu_1, \dots, \mu_n \in L$ such that

$$z = \mu_1 y_1 + \dots + \mu_n y_n. \quad (1)$$

$\mu_j \in L$ so for all j there exists $\lambda_{ij} \in K$ such that

$$\mu_j = x_1 \lambda_{1j} + \dots + x_m \lambda_{mj}. \quad (2)$$

Plug in (2) into (1),

$$z = \sum_{i,j} \lambda_{ij} x_i y_j.$$

- $\{x_i y_j\}$ are linearly independent over K . Suppose there exists $\lambda_{ij} \in K$ such that

$$0 = \sum_{i,j} \lambda_{ij} x_i y_j = \sum_j \left(\sum_i \lambda_{ij} x_i \right) y_j,$$

so for all j , $\sum_i \lambda_{ij} x_i = 0$, so for all j and all i , $\lambda_{ij} = 0$.

□

Lecture 5
Friday
18/01/19

Example. To show $G = \mathfrak{S}_3$. Let $\sigma = (1 \ 2)$. A basis of L/\mathbb{Q} is

$$1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \omega\sqrt[3]{2}, \omega\sqrt[3]{4}.$$

- $\sigma(1) = 1$.
- $\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}$.
- $\sigma(\omega\sqrt[3]{2}) = \sqrt[3]{2}$.
- $\sigma(\sqrt[3]{4}) = \sigma(\sqrt[3]{2} \cdot \sqrt[3]{2}) = \omega\sqrt[3]{2} \cdot \omega\sqrt[3]{2} = \omega^2\sqrt[3]{4} = (-\omega - 1)\sqrt[3]{4} = -\omega\sqrt[3]{4} - \sqrt[3]{4}$.
- $\sigma(\omega) = \sigma(\omega\sqrt[3]{2}/\sqrt[3]{2}) = \sigma(\omega\sqrt[3]{2})/\sigma(\sqrt[3]{2}) = \sqrt[3]{2}/\omega\sqrt[3]{2} = 1/\omega = -1 - \omega$.
- $\sigma(\omega\sqrt[3]{4}) = \sigma(\omega\sqrt[3]{2} \cdot \sqrt[3]{2}) = \sigma(\omega\sqrt[3]{2}) \cdot \sigma(\sqrt[3]{2}) = \sqrt[3]{2} \cdot \omega\sqrt[3]{2} = \omega\sqrt[3]{4}$.

Thus

$$\sigma = \begin{pmatrix} 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 \end{pmatrix}.$$

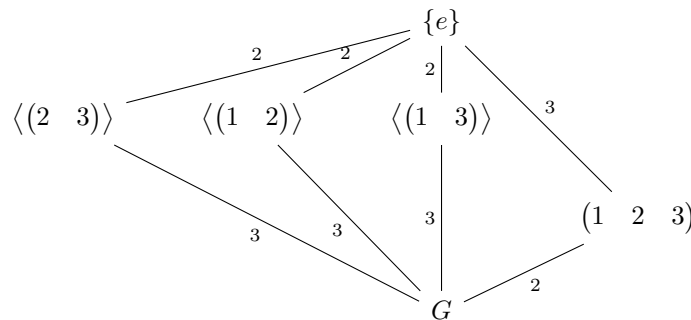
A question is if there were $\sigma \in G$ such that $\rho(\sigma) = (1 \ 2)$ then we have written the matrix of σ as a \mathbb{Q} -linear map of L in a basis. But how to check that this \mathbb{Q} -linear map is a field homomorphism? We know the Galois correspondence for extensions of degree two.

$$\text{Gal}_{\mathbb{Q}(\sqrt[3]{2})}(L), \text{Gal}_{\mathbb{Q}(\omega^2\sqrt[3]{2})}(L), \text{Gal}_{\mathbb{Q}(\omega\sqrt[3]{2})}(L) \subset G$$

contain an element of order two, and

$$\begin{aligned} \rho : \quad \text{Gal}_{\mathbb{Q}(\sqrt[3]{2})}(L) &\mapsto (2 \ 3) \\ \text{Gal}_{\mathbb{Q}(\omega^2\sqrt[3]{2})}(L) &\mapsto (1 \ 2) \\ \text{Gal}_{\mathbb{Q}(\omega\sqrt[3]{2})}(L) &\mapsto (1 \ 3). \end{aligned}$$

The lattice of subgroups is



$\mathbb{Q}(\omega)/\mathbb{Q}$ is the splitting field of $x^2 + x + 1$ and of $x^2 + 3$.

We can learn the following. Let $k \subset L$ be a splitting field. Consider $k \subset K \subset L$. Then $K \subset L$ is also a splitting field. The corresponding $H \leq G$ is the Galois group $\text{Gal}_K(L)$. On the other hand $k \subset K$ is not always a splitting field. It is a splitting field if and only if the corresponding $H \leq G$ is a normal subgroup and in that case $\text{Gal}_k(K) = G/H$.

1 Elementary facts

Let $K \subset L$ and $a \in L$. The **evaluation homomorphism**

$$\begin{aligned} e_a : K[x] &\rightarrow K[a] \subset L \\ f(x) &\mapsto f(a) \end{aligned}$$

is a surjective ring homomorphism, where $K[a]$ is the smallest subring of L containing K and a .

Definition 1.1. $f(x) = a_0x^n + \cdots + a_n \in K[x]$ is **monic** if $a_0 = 1$.

Lemma 1.2.

- If a is transcendental, e_a is injective and it extends to $\tilde{e}_a : K(x) \rightarrow K(a)$, by

$$\begin{array}{ccc} K(x) & & \\ \cup & \searrow \tilde{e}_a & \\ K[x] & \xrightarrow{e_a} & L \end{array} .$$

- If a is algebraic, then $\text{Ker}(e_a) = \langle f_a \rangle$, where $f_a \in K[x]$ is irreducible, or prime, and unique if monic, then called the minimal polynomial of $a \in L/K$. In this case

$$\begin{array}{ccc} K[x] & \xrightarrow{e_a} & K[a] \cong K(a) \subset L \\ \cup & \nearrow \sim & \\ \frac{K[x]}{\langle f_a \rangle} & \xrightarrow{[e_a]} & \end{array} .$$

Proof. There is nothing to prove. □

Remark. Let $g(x) \in K[x]$ and $g(a) \neq 0$. Claim that $1/g(a) \in K[a]$. Indeed $\gcd(f, g) = 1$ in $K[x]$ and $f \nmid g$. There exists $\phi, \psi \in K[x]$ such that $f\phi + g\psi = 1$ and $g(a)\psi(a) = 1$. All of this is saying

- $K[a] \cong K(a)$, and
- $K[x] / \langle f_a \rangle \cong K(a)$.

Let

$$\text{Emb}_K(K(a), F) = \{\sigma : K(a) \rightarrow F \mid \sigma \text{ field homomorphism, } \sigma_K = \text{id}_K\},$$

where

$$\begin{array}{ccc} & & K(a) \\ & \subset & \vdots \\ k & & \sigma \\ & \subset & \vdots \\ & & F \end{array} .$$

Corollary 1.3. For $K \subset L$ and $a \in L$ algebraic over K ,

- $[K(a) : K] = \deg(f_a)$, and
- If $K \subset F$ is an extension,

$$\text{Emb}_K(K(a), F) = \{b \in F \mid f_a(b) = 0\}.$$

Lecture 6
Tuesday
22/01/19

Proof. Since $K(a) = K[a]$, $[K(a) : K] = \dim_K(K(a)) = \dim_K(K[a])$. Suppose

$$f(x) = x^n + \mu_1 x^{n-1} + \cdots + \mu_n \in K[x]$$

is the minimal polynomial of a over K . Claim that $1, \dots, a^{n-1}$ is a basis of $K[a]$ over K .

- The set generates $K[a]$. Let $c \in K[a]$. There exists $g \in K[x]$ such that $g(a) = c$. Long division gives

$$g(x) = f(x)q(x) + r(x), \quad m = \deg(r(x)) < n.$$

Then $r(x) = \lambda_0 + \cdots + \lambda_m x^m$ and $g(a) = r(a) = \lambda_0 + \cdots + \lambda_m a^m$.

- The set is linearly independent, otherwise there exists

$$g(x) = \lambda_0 + \cdots + \lambda_{n-1} x^{n-1} \in K[x], g(a) = 0,$$

and f was not the minimal polynomial.

$\sigma(a)$ is a root of f , since applying σ to $f(a) = 0$ gives

$$0 = \sigma(a^n + \mu_1 a^{n-1} + \cdots + \mu_n) = \sigma(a)^n + \mu_1^{n-1} \sigma(a)^{n-1} + \cdots + \mu_n = f(\sigma(a)).$$

Vice versa, if $b \in F$ is a root of f ,

$$K(b) \xleftarrow[\sim]{[e_b]} \frac{K[x]}{\langle f \rangle} \xrightarrow[\sim]{[e_a]} K(a),$$

then $\sigma = [e_b][e_a]^{-1}$. Thus there is a one-to-one correspondence

$$\begin{array}{ccc} \text{Emb}_K(K(a), F) & \leftrightarrow & \{b \in F \mid f(b) = 0\} \\ \sigma & \mapsto & \sigma(a) \\ [e_b][e_a]^{-1} & \leftarrow & b \end{array}.$$

□

Corollary 1.4. Let K be a field and $f \in K[x]$. Then there exists $K \subset L$ such that f has a root in L .

Proof. Take g a prime factor of f . Take $L = K[x] / \langle g \rangle$. In here $a = [x]$ is a root of g hence a root of f . □

From now on in this course, we study field extensions $K \subset L$, always assumed to be finite, so $[L : K] = \dim_K(L) < \infty$.

Remark. $K \subset L$ is finite if and only if

- it is algebraic, that is for all $a \in L$, a is algebraic over K , and
- it is finitely generated, that is there exist $a_1, \dots, a_m \in L$ such that $L = K(a_1, \dots, a_m)$.

An important point of view is that we study all possible field homomorphisms

$$\text{Emb}(K, L) = \{\sigma : K \rightarrow L \mid \sigma \text{ field homomorphism}\}.$$

Often there is a field $k \subset K, L$ in the background which we want to stay fixed, so

$$\text{Emb}_k(K, L) = \{\sigma : K \rightarrow L \mid \sigma \text{ field homomorphism, } \sigma|_k = \text{id}_k\}.$$

Example. Let $K = \mathbb{Q}(\sqrt[3]{2})$. The minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$. Let $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ be the splitting field of $x^3 - 2$. Then

$$\text{Emb}_{\mathbb{Q}}(K, L) = \text{Emb}(K, L) = \{\text{roots of } x^3 - 2 \text{ in } L\} = \{\sqrt[3]{2}, \omega \sqrt[3]{2}, \omega^2 \sqrt[3]{2}\}.$$

Remark. Suppose $k \subset K$. $\text{Emb}_k(K, K) = G = \text{Gal}_k(K)$. Indeed every k -homomorphism $\sigma : K \rightarrow K$ is automatically invertible. We know σ is injective. σ is also surjective because σ is a k -linear endomorphism of a finite-dimensional k -vector space.

Lecture 7
Thursday
24/01/19

2 Axiomatics

Proposition 2.1. Fix $k \subset K$ and $k \subset L$. Then $\#Emb_k(K, L) \leq [K : k]$.

Proof.

Special case. If $K = k(a)$, let $f(x) \in k[x]$ be the minimal polynomial of a . Then $Emb_k(k(a), L)$ is the roots of $f(x)$ in L , so

$$\#Emb_k(K, L) = \#\{\text{roots}\} \leq \deg(f) = [k(a) : k],$$

as proved last time.

General case. If $k = K$, nothing to do. Otherwise choose $a \in K \setminus k$.

$$\begin{array}{ccccc} & & & & L \\ & & & \nearrow & \uparrow \\ & & y & & \\ k & \subset & k(a) & \subset & K \end{array}$$

Consider the restriction map

$$\rho : Emb_k(K, L) \rightarrow Emb_k(k(a), L).$$

Fix $y \in Emb_k(k(a), L)$. Then

$$\rho^{-1}(y) = \{x : K \rightarrow L \mid x|_{k(a)} = id_{k(a)}\}.$$

Since $[k(a) : k] > 1$, by the tower law $[K : k(a)] < [K : k]$. By induction we may assume $\#\rho^{-1}(y) \leq [K : k(a)]$. So

$$\#Emb_k(K, L) \leq \sum_{y \in Emb_k(k(a), L)} \#\rho^{-1}(y) \leq [k(a) : k][K : k(a)] = [K : k],$$

by the tower law.

□

Proposition 2.2. Suppose given two field extensions $k \subset K$ and $k \subset L$. Then there is a non-unique bigger common field

$$\begin{array}{ccc} & K & \\ \sigma \searrow & & \cap \nearrow \\ k & & \Omega \\ \cap \searrow & & \cap \nearrow \\ & L & \end{array}$$

that contains both.

Remark.

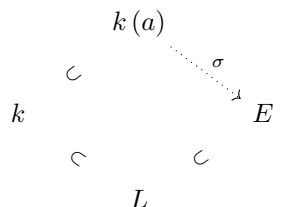
- More formally, suppose given $\sigma_1 \in Emb(k, K)$ and $\sigma_2 \in Emb(k, L)$, then there exists Ω , $\phi_1 \in Emb(K, \Omega)$, and $\phi_2 \in Emb(L, \Omega)$ such that $\phi_1 \circ \sigma_1 = \phi_2 \circ \sigma_2$.
- I never said that Ω is unique. For example, let $K = \mathbb{Q}(\sqrt[3]{2})$ and $L = \mathbb{Q}(\sqrt[3]{2})$. One choice is $\Omega = k$. Another choice is $\Omega = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$, where

$$\begin{array}{ccc} & \mathbb{Q}(\sqrt[3]{2}) & \\ \sigma \searrow & & \nearrow \phi_1 : \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \mathbb{Q} & & \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) \\ \cap \searrow & & \nearrow \phi_2 : \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ & \mathbb{Q}(\sqrt[3]{2}) & \end{array}$$

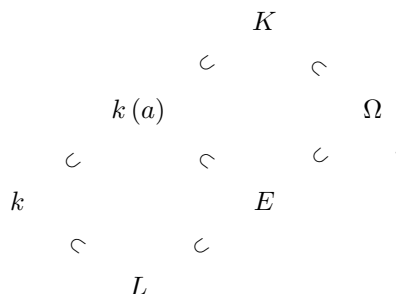
Another more precise way to state this is there exists $k \subset \Omega$ such that $Emb_k(K, \Omega)$ and $Emb_k(L, \Omega)$ are both non-empty.

Proof.

Special case. If $K = k(a)$, let $f(x) \in k[x]$ be the minimal polynomial of a over k . Let $L \subset E$ be such that $f(x) \in L[x]$ has a root $\alpha \in E$. Then there exists $\sigma \in Emb_k(k(a), E)$ such that $\sigma(a) = \alpha$.



General case. By induction on $[K : k]$. If $[K : k] = 1$, take $\Omega = L$. If $[K : k] > 1$, take $a \in K \setminus k$.



By special case there exists E as in the diagram. By tower law $[K : k(a)] < [K : k]$ hence by induction find Ω as in the diagram. Ω solves the original problem.

□

Proposition 2.3. Let L be any field and G be a finite group acting on L as automorphisms. Let

$$K = G^* = \text{Fix}(G) = L^G = \{\lambda \in L \mid \forall \sigma \in G, \sigma(\lambda) = \lambda\}.$$

Consider $\text{Aut}_K(L) = K^\dagger$. Then the obvious inclusion $G \subset K^\dagger = (G^*)^\dagger$ is an equality, so G is all of K^\dagger .

Remark. Contextualising, this thing is half of the Galois correspondence.

$$\begin{aligned} \{F \mid k \subset F \subset \Omega\} &\leftrightarrow \{G \mid G \leq \text{Aut}_k(\Omega)\} \\ F &\mapsto \text{Aut}_F(\Omega) = F^\dagger \\ \text{Fix}(G) = G^* &\leftarrow G \end{aligned}$$

Then to prove the Galois correspondence, we need for all G , $G = (G^*)^\dagger$. We also need for all F , $F = (F^\dagger)^*$.

Proposition 2.3 follows from the following lemma.

Lemma 2.4. $K \subset L$ is a finite extension of degree $[L : K] \leq |G|$.

Proof of Proposition 2.3. From Proposition 2.1, $\text{Aut}_K(L) = \text{Emb}_K(L, L)$ because $K \subset L$ is finite, and $\#\text{Emb}_K(L, L) \leq [L : K]$. By Lemma 2.4,

$$[L : K] \leq \#\text{Emb}_K(L, L) \leq [L : K],$$

so $|G| = \#\text{Emb}_K(L, L)$. By what we said, $G \subset \text{Emb}_K(L, L)$, so $G = \text{Emb}_K(L, L)$.

□

Lecture 9 is a problem class.

Lecture 8
Friday
25/01/19

Lecture 9
Tuesday
29/01/19
Lecture 10
Thursday
31/01/19

Proof of Lemma 2.4. Write $G = \{\sigma_1, \dots, \sigma_n\}$ for $n = |G|$. Want that all $(n+1)$ -tuples $a_1, \dots, a_{n+1} \in L$ are linearly dependent over K . Let $a_1, \dots, a_{n+1} \in L$. Consider the $n+1$ vectors in L^n . Let

$$\overline{a_1} = \begin{pmatrix} \sigma_1(a_1) \\ \vdots \\ \sigma_n(a_1) \end{pmatrix}, \dots, \overline{a_{n+1}} = \begin{pmatrix} \sigma_1(a_{n+1}) \\ \vdots \\ \sigma_n(a_{n+1}) \end{pmatrix} \in L^n.$$

These are linearly dependent over L . There exist $x_1, \dots, x_{n+1} \in L$ not all zero such that

$$x_1 \overline{a_1} + \dots + x_{n+1} \overline{a_{n+1}} = \overline{0}.$$

By reordering the $\overline{a_i}$, may assume

$$x_1 \overline{a_1} + \dots + x_k \overline{a_k} = \overline{0}, \tag{3}$$

for some $1 \leq k \leq n+1$ with

- for all $i \in \{1, \dots, k\}$, $x_i \neq 0$,
- such k is the smallest, and
- $x_1 = 1$.

Claim that all these $x_i \in K$. This does it, by reading j -th row where $\sigma_j = id_G$. We need to show for all i $x_i \in L^G$. Take $\sigma \in G$.

$$\sigma(x_1) \begin{pmatrix} \sigma(\sigma_1(a_1)) \\ \vdots \\ \sigma(\sigma_n(a_1)) \end{pmatrix} + \dots + \sigma(x_k) \begin{pmatrix} \sigma(\sigma_1(a_k)) \\ \vdots \\ \sigma(\sigma_n(a_k)) \end{pmatrix} = \overline{0} \in L^n.$$

Note that

$$\begin{array}{ccc} G & \rightarrow & G \\ \tau & \mapsto & \sigma \circ \tau \end{array}$$

is a bijective function and $\{\sigma \circ \sigma_1, \dots, \sigma \circ \sigma_n\} = G$. Multiplying by σ reshuffles the rows. So in fact,

$$\sigma(x_1) \overline{a_1} + \dots + \sigma(x_k) \overline{a_k} = \overline{0}. \tag{4}$$

Claim that for all i $\sigma(x_i) = x_i$. Otherwise (3) – (4),

$$(x_2 - \sigma(x_2)) \overline{a_2} + \dots + (x_k - \sigma(x_k)) \overline{a_k} = \overline{0}$$

is a shorter solution, contradicting k minimal. □

3 Galois correspondence

Definition 3.1. $k \subset K$ is **normal** if

$$\forall k \subset \Omega, \forall \sigma_1, \sigma_2 \in \text{Emb}_k(K, \Omega), \exists \sigma \in \text{Emb}_k(K, K), \sigma_2 = \sigma_1 \circ \sigma. \quad (5)$$

Equivalently,

$$\forall k \subset \Omega, \forall \sigma_1, \sigma_2 \in \text{Emb}_k(K, \Omega), \sigma_2(K) \subset \sigma_1(K). \quad (6)$$

Example. $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ is not normal. Take $\Omega = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$.

(5) \implies (6) Indeed for all $\lambda \in K$, $\sigma_2(\lambda) = \sigma_1(\sigma(\lambda)) \in \sigma_1(K)$, so $\sigma_2(K) \subset \sigma_1(K)$.

(6) \implies (5) Work inside Ω .

$$k \subset \sigma_2(K) \subset \sigma_1(K) \subset \Omega.$$

Tower law gives

$$[K : k] = [\sigma_1(K) : k] = [\sigma_1(K) : \sigma_2(K)] [\sigma_2(K) : k] = [\sigma_1(K) : \sigma_2(K)] [K : k].$$

So $[\sigma_1(K) : \sigma_2(K)] = 1$, so $\sigma_1(K) = \sigma_2(K)$. Take $\sigma = \sigma_1^{-1} \circ \sigma_2$. σ is clearly bijective and it is more or less obvious that $\sigma \in \text{Emb}_k(K, K)$.