4-11-25 (WEEK 8) Shun/翔海(@shun4midx)

GALOIS THEORY

MOTIVATION

- $ax^2+bx+c=0 \Rightarrow x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$
- $x^3+px+q=0$ ($x^3+ax^2+bx+c=0$, take $x=x'-\frac{a}{3}$)
  Let $x=u+v$, we get $u^3+v^3+(3uv+p)(u+v)+q=0$
  Let $\begin{cases} 3uv+p=0 \\ u^3+v^3+q=0 \end{cases}$, then we can solve it! Then, $x=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$
- $x^4+ax^3+bx^2+cx+d=0 \Rightarrow (x^4+ax^3+bx^2+cx+d)+(px+q)^2=(px+q)^2 \Rightarrow (x^2+\frac{a}{2}x+k)^2=(px+q)^2$
  $\Rightarrow 2k+\frac{a^2}{4}=b+p^2,\ ak=c+2pq,\ k^2=d+q^2 \Rightarrow p^2=2k+\frac{a^2}{4}-b,\ 2pq=ak-c,\ q^2=k^2-d \Rightarrow 4(k^2-d)(2k+\frac{a^2}{4}-b)=(ak-c)^2$
  $\Rightarrow x^2+\frac{a}{2}x+k-px-q=0$ or $x^2+\frac{a}{2}x+k+px+q=0$ ✓
- Abel (1824): $\exists\ x^5+a_1x^4+\dots+a_5=0$ with no root-formula!
- Galois (1811–1832): $f(x)=x^n+a_1x^{n-1}+\dots+a_{n-1}x+a_n=0$ with roots $\alpha_1,\dots,\alpha_n$.
  Let $K=\mathbb{Q}(a_1,\dots,a_n)$, $L=K(\alpha_1,\dots,\alpha_n)$
  $\therefore f(x)$ has root-formula $\Leftrightarrow \mathrm{Aut}_K(L)$ is solvable

SIMPLE EXTENSION

DEFINITION

- L/K is called an extension of fields if L is a field and K is a subfield of L. (subset)
- Given L/K and $A\subseteq L$, $K(A):=$ the smallest subfield of L containing A and K

REMARK

- $A=\{\alpha\} \Rightarrow K(A)=K(\alpha)=\left\{\frac{P(\alpha)}{Q(\alpha)} \middle| P(x), Q(x)\in K[x], Q(\alpha)\neq 0\right\}$
- In general, $K(A)=\left\{\frac{P(\alpha_1,\dots,\alpha_k)}{Q(\alpha_1,\dots,\alpha_k)} \middle| k\in\mathbb{N},\ \alpha_1,\dots,\alpha_k\in A,\ P(x_1,\dots,x_k), Q(x_1,\dots,x_k)\in K[x_1,\dots,x_k] \text{ with } Q(\alpha_1,\dots,\alpha_k)\neq 0\right\}$
- Given L/K, $A,B\subseteq L$, $K(A\cup B)=K(A)(B)$
- Given L/K, L can be regarded as a vector space over K.

DEFINITION

- The degree of L/K is $[L:K]=\dim_K L$
- L/K is a finite extension if $[L:K]<\infty$

EXAMPLE

- $\mathbb{R}/\mathbb{Q}$ is not a finite extension since $\mathbb{R}$ is uncountable
- $\mathbb{C}/\mathbb{R}$ is of degree 2

PROPOSITION 1

Given M/L and L/K, then $[M:K]=[M:L][L:K]$

Proof

- Assume that $[M:L]=m<\infty$, $[L:K]=n<\infty$.
  Let $\{x_1,\dots,x_m\}$ be a basis of M over L, $\{y_1,\dots,y_n\}$ is a basis of L over K
  Claim: $\{y_jx_i\}_{i=1,\dots,m,\ j=1,\dots,k}$ forms a basis for M over K
  Proof
  - Lin indep: $\sum_{i,j} c_{ij}y_jx_i=0$ with $c_{ij}\in K \Rightarrow \sum_{i=1}^m(\underbrace{\sum_{j=1}^n c_{ij}y_j}_{\in L})x_i \Rightarrow \sum c_{ij}y_j=0\ \forall j \Rightarrow c_{ij}=0\ \forall i,j$
  - Generating: $z\in M \Rightarrow z=\sum_{i=1}^m a_ix_i,\ a_i\in L,\ a_i=\sum_{j=1}^n b_{ij}y_j,\ b_{ij}\in K \Rightarrow z=\sum_{i,j} b_{ij}y_jx_i$ □

$\therefore [M:K]=[M:L][L:K]$ □

- Assume $[M:K]=\ell<\infty$ and $\{z_1,\dots,z_\ell\}$ be a basis for M over K Shun/翔海 (@shun4midx)

$\because L/K \subseteq M/K \therefore [L:K]<\infty$

Also, $M=Kz_1+\dots+Kz_\ell \subseteq Lz_1+\dots+Lz_\ell \subseteq M \Rightarrow M=Lz_1+\dots+Lz_\ell \Rightarrow [M:L]<\infty$ □

$\therefore$ This implies that if $[M:L]=\infty$ or $[L:K]=\infty$, then $[M:K]=\infty$ □

DEFINITION

Given L/K and $\alpha\in L$, consider the evaluation map $ev_\alpha: K[x] \longrightarrow K[\alpha] \subseteq L$

$f(x) \longmapsto f(\alpha)$

Then,
- α is **algebraic** over K if $\ker ev_\alpha \neq \{0\}$ (intuition: This means $\exists$ nontrivial polynomial s.t. α is a root)
- α is **transcendental** over K if $\ker ev_\alpha = \{0\}$

PROPOSITION 2

Given L/K and $\alpha\in L$, if α is algebraic over K, then $\exists!$ monic min poly $m_{\alpha,K}(x)\in K[x]$ of minimal degree, s.t. $m_{\alpha,K}(\alpha)=0$ and $\forall f(x)\in K[x]$ with $f(\alpha)=0 \Rightarrow m_{\alpha,K}(x) \mid f(x)$

Proof

Consider $ev_\alpha: \underbrace{K[x]}_{PID} \longrightarrow K[\alpha]$, so $\ker ev_\alpha = \langle f(x)\rangle$

How about "irreducible"? If not, $\exists$ g,h, s.t. $\deg g<\deg f$, $\deg h<\deg f$, s.t. $f(x)=g(x)h(x)$, i.e. $f(\alpha)=g(\alpha)h(\alpha)$

$\therefore h(\alpha)=0$ or $g(\alpha)=0$ $\divideontimes$

REMARK

Every root of $m_{\alpha,K}(x)$ in L has the same minimal poly $m_{\alpha,K}(x)$

PROPOSITION 3

TFAE:

(1) α is algebraic over K

(2) $K[\alpha]=K(\alpha)$

(3) $[K(\alpha):K]<\infty$

Proof

(1)⇒(2): By first isom thm, $\overset{PID}{K[x]}/\langle \underset{\max}{m_{\alpha,K}(x)}\rangle \cong F[\alpha]$, which is a field

Also, by def, $\underset{\text{smallest}}{K(\alpha)} \subseteq K[\alpha] \Rightarrow K(\alpha)=K[\alpha]$

(2)⇒(1): $\because \alpha^{-1}\in K(\alpha)=K[\alpha]$

$\therefore \alpha^{-1}=p(\alpha)=a_0+a_1\alpha+\dots+a_n\alpha^n \Rightarrow 1=a_0\alpha+a_1\alpha^2+\dots+a_n\alpha^{n+1} \Rightarrow \alpha$ is algebraic

(1)⇒(3): Assume $\deg m_{\alpha,K}=n$

Claim: $\{1,\alpha,\dots,\alpha^{n-1}\}$ forms a basis for $K(\alpha)$ over K

Proof
- If $a_0+a_1\alpha+\dots+a_{n-1}\alpha^{n-1}=0$, then $a_0+a_1x+\dots+a_{n-1}x^{n-1}\in\ker ev_\alpha \Rightarrow a_1=\dots=a_{n-1}=0$
- $\forall f(\alpha)\in K(\alpha)=K[\alpha]$ with $f(x)\in K[x]$, let $q(x), r(x)\in K[x]$, s.t. $f=m_{\alpha,K}q+r$ with $\deg r<\deg m_{\alpha,K}=n$ $\therefore f(\alpha)=r(\alpha)\in\langle 1,\dots,\alpha^{n-1}\rangle_K$

(3)⇒(1): Let $[K(\alpha):K]=n<\infty$

Consider $1,\alpha,\dots,\alpha^n$

Case 1: $\exists \alpha^s=\alpha^t$, s.t. $0\le s<t\le n$, then $x^t-x^s\in\ker ev_\alpha \Rightarrow \alpha$ is algebraic

Case 2: $1,\dots,\alpha^n$ are distinct $\because [K(\alpha):K]=n$ $\therefore \exists a_0,\dots,a_n$ not all in K s.t. $a_0+a_1\alpha+\dots+a_n\alpha^n=0$ $\therefore \alpha$ is algebraic □

DEFINITION

For L/K, define $L_\alpha := \{\alpha\in L \mid \alpha \text{ is algebraic over } K\} \underset{\text{subfield}}{\subseteq} L$

Notice: $\forall \alpha,\beta\in L_\alpha$, $\alpha+\beta, \alpha\beta, \frac{\alpha}{\beta} \overset{?}{\in} L_\alpha$

Claim: $[K(\alpha,\beta):K]<\infty$ $\underset{\text{algebraic}}{\Rightarrow}$ $<\infty$

Proof: $[K(\alpha,\beta):K]=[\underline{K(\alpha)(\beta):K(\alpha)}][K(\alpha):K]<\infty$ □

$\therefore \alpha\pm\beta, \alpha\beta, \frac{\alpha}{\beta}\in K(\alpha,\beta) \Rightarrow \alpha\pm\beta, \alpha\beta, \frac{\alpha}{\beta}\in L_\alpha$

EXAMPLE

$\overline{\mathbb{Q}}=\{\alpha\in\mathbb{R} \mid \alpha \text{ is alg over } \mathbb{Q}\}$: the field of alg numbers

- $[\overline{\mathbb{Q}}:\mathbb{Q}]=\infty$: $[\mathbb{Q}(\sqrt[n]{2}):\mathbb{Q}]=n\ \forall n$ (x^n-2 irred by Eisenstein)
- $\overline{\mathbb{Q}}$ is countable ($\therefore \overline{\mathbb{Q}}\neq\mathbb{R}$)

  $\mathbb{Q}$ is countable $\Rightarrow \{x^n+a_1x^{n-1}+\dots+a_n \mid a_i\in\mathbb{Q}\}$ is countable

  $\Rightarrow V_n=\{\alpha\in\mathbb{R} \mid \alpha^n+a_1\alpha^{n-1}+\dots+a_n=0,\ a_i\in\mathbb{Q}\}$ is countable

  $\Rightarrow \overline{\mathbb{Q}}=\bigcup_{n=1}^{\infty}V_n$ is countable

EXAMPLE

Let $m_{\alpha,\mathbb{Q}}(x)=x^3-x^2+x+2$ and $\beta=1+2\alpha-\alpha^2$. Find $m_{\beta,\mathbb{Q}}$, β^{-1}

Consider $T:\mathbb{Q}(\alpha)\longrightarrow\mathbb{Q}(\alpha)$, $f\longmapsto\beta f$ which is a $\mathbb{Q}$-linear transformation, $\mathbb{Q}(\alpha)$ has basis $\{1,\alpha,\alpha^2\}$.

$T(1)=1+2\alpha-\alpha^2$

$T(\alpha)=\alpha+2\alpha^2-\alpha^3=\alpha+2\alpha^2-(\alpha^2-\alpha-2)=2+2\alpha+\alpha^2$

$T(\alpha^2)=2\alpha+2\alpha^2+(\alpha^2-\alpha-2)=-2+\alpha+3\alpha^2$

$\therefore [T]_{\{1,\alpha,\alpha^2\}}=\begin{bmatrix}1&2&-2\\2&2&1\\-1&1&3\end{bmatrix}=A$, char poly of A is $x^3-6x^2+4x+17$

By Cayley-Hamilton thm, $T^3-6T^2+4T+17=0$. $\because T(1)=\beta$ $\therefore \beta^3-6\beta^2+4\beta+17=0$ (min cuz can either deg 1 or 3 by divisibility, but very fucking clearly not deg 1)

Now, $\beta(\beta^2-6\beta+4)=17 \Rightarrow \beta^{-1}=-\frac{1}{17}(\beta^2-6\beta+4)$

REMARK

If $[L:K]=p$ prime, then L/K is a simple extension

Proof

Pick $\alpha\in L\setminus K\Rightarrow [K(\alpha):K]>1$ and $\underbrace{[K(\alpha):K]}_{=p}\mid[L:K]=p$ $\square$