Algebra II — Galois Theory

Shun/翔海 (@shun4midx)

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 $K=\mathbb{Q}(a_1,\dots,a_n)$, $L=K(\alpha_1,\dots,\alpha_n)$
  ∴ $f(x)$ has root-formula $\Leftrightarrow$ $\mathrm{Aut}_K(L)$ is solvable

SIMPLE EXTENSION

DEFINITION

- L/K is called an extension of fields (subset) if L is a field and K is a subfield of L.
- 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: $\{y_jx_i\}_{i=1,\dots,m,\ j=1,\dots,n}$ 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: $z\in M \Rightarrow z=\sum_{i=1}^{m}a_ix_i$, $a_i=\sum_{j=1}^{n}b_{ij}y_j$, $b_{ij}\in K \Rightarrow z=\sum_{i,j}b_{ij}y_jx_i$ □

  ∴ $[M:K]=[M:L][L:K]$ □

Shun/郑顺海 (@shun4midx)

- Assume $[M:K]=\ell<\infty$ and $\{z_1,\dots,z_\ell\}$ be a basis for M over K
  $\because L/K \subseteq M/K \therefore [L:K]<\infty$
  Also, $M=Kz_1+\dots+Kz_\ell \subseteq Lz_1+\dots+Lz_\ell \subseteq M \Rightarrow M=Lz_1+\dots+Lz_\ell \Rightarrow [M:L]<\infty$ □
  ∴ 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 $ev_\alpha: K[x] \longrightarrow K(\alpha)$ (P10), so $\ker ev_\alpha=(f(x))$

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. $f(\alpha)=g(\alpha)h(\alpha)$

∴ $h(\alpha)=0$ or $g(\alpha)=0$ ↯

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, $K[x]/\langle m_{\alpha,K}(x)\rangle \cong F[\alpha]$ (P10, max), which is a field
Also, by def, $K(\alpha)\subseteq K[\alpha] \Rightarrow K(\alpha)=K[\alpha]$ (smallest)

(2)⇒(1): $\because \alpha^{-1}\in K(\alpha)=K[\alpha]$
∴ $\alpha^{-1}=p(\alpha)=a_0+a_1\alpha+\dots+a_n\alpha^n \Rightarrow 1=a_0\alpha+a_1\alpha^2+\dots+a_n\alpha^{n+1} \Rightarrow \alpha$ 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 $\deg r<\deg m_{\alpha,K}=n$ ∴ $f(\alpha)=r(\alpha)\in\langle 1,\dots,\alpha^{n-1}\rangle_K$

(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 $\because [K(\alpha):K]=n$ ∴ $\exists\, a_0,\dots,a_n$ not all in K s.t. $a_0+a_1\alpha+\dots+a_n\alpha^n=0$ ∴ α is algebraic □

DEFINITION

For L/K, define $L_a:=\{\alpha\in L \mid \alpha \text{ is algebraic over } K\} \subsetneq L$ (strict)

Notice: $\forall \alpha,\beta\in L_a$, $\alpha\pm\beta, \alpha\beta, \frac{\alpha}{\beta}\in L_a$
Claim: $[K(\alpha,\beta):K]<\infty$ (algebraic ⇒ $<\infty$)
Proof: $[K(\alpha,\beta):K]=[K(\alpha)(\beta):K(\alpha)][K(\alpha):K]<\infty$ □
∴ $\alpha\pm\beta, \alpha\beta, \frac{\alpha}{\beta}\in K(\alpha,\beta) \Rightarrow \alpha\pm\beta, \alpha\beta, \frac{\alpha}{\beta}\in L_a$

Shun / 翔海 (@shun4midx)

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 $\Rightarrow \{x^n + a_1 x^{n-1} + \dots + a_n \mid a_i \in \mathbb{Q}\}$ 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 $T: \mathbb{Q}(\alpha) \longrightarrow \mathbb{Q}(\alpha)$ which is a $\mathbb{Q}$-linear transformation, $\mathbb{Q}(\alpha)$ has basis $\{1, \alpha, \alpha^2\}$.

$f \longmapsto \beta f$

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

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

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

$\therefore [T]_{\{1,\alpha,\alpha^2\}} = \begin{bmatrix} 1 & 2 & -2 \\ 2 & 2 & 1 \\ -1 & 1 & 3 \end{bmatrix} = A$, 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 $[K(\alpha) : K] \overset{\neq p}{|} [L : K] = p$ $\square$

4-16-25 (WEEK 9)

Shun/翔海 (@shun4midx)

ALGEBRAIC EXTENSION

DEFINITION

L/K is said to be algebraic if $\forall \alpha \in L$, α is alg over K.

PROPOSITION 1

(When we wanna prove "alg", we always try to prove finiteness for $[K(\alpha):K]$.)

$[L:K] < \infty \Leftrightarrow L = K(\alpha_1, \dots, \alpha_n)$, where α_i is alg over K $\forall i$ (In this case, L/K is algebraic)

Proof

"$\Rightarrow$": Let $[L:K]=n$ and $\{\alpha_1, \dots, \alpha_n\}$ be a basis for L over K

$\because L = K\alpha_1 + \dots + K\alpha_n = K(\alpha_1, \dots, \alpha_n) \subseteq L$

$\therefore L = K(\alpha_1, \dots, \alpha_n)$

Now, $\forall i$, $[K(\alpha_i):K] \le [L:K] < \infty$ $\therefore \alpha_i$ is alg over K

"$\Leftarrow$": $[L:K] = [K(\alpha_1, \dots, \alpha_n) : K(\alpha_1, \dots, \alpha_{n-1})] \cdots [K(\alpha_1):K] < \infty$ ("algebraic" over") □

Moreover, $\alpha \in K(\alpha_1, \dots, \alpha_n) \Rightarrow [K(\alpha):K] \le [L:K] < \infty \Rightarrow \alpha$ is alg over K

COROLLARY

Given L/K and S as a subset of L, if $\forall \alpha \in S$, α is alg over K, then $K(S)/K$ is alg

Proof

(When we pinpoint an element, etc there is finiteness)

$\forall \alpha \in K(S)$, $\exists \alpha_1, \dots, \alpha_n \in S$, s.t. $\alpha \in K(\alpha_1, \dots, \alpha_n)$ $\therefore \alpha$ is alg over K. □

PROPOSITION 2

If M/L and L/K are alg, then M/K is alg

Proof

$\forall \alpha \in M$, we know α is alg over L, say $\alpha^n + a_1\alpha^{n-1} + \dots + a_n = 0$, $a_i \in L$. This means that α is alg over $K(a_1, \dots, a_n)$

Now, notice $[K(a_1, \dots, a_n, \alpha) : K] = [K(a_1, \dots, a_n, \alpha) : K(a_1, \dots, a_n)][K(a_1, \dots, a_n) : K] < \infty$ (α: ∞, a_i: ∞)

DEFINITION

- L is algebraically closed if each nonconstant $f(x) \in L[x]$ has a root in L (not just "a root in L")
- $\bar{K}$ is an algebraic closure of K if $\bar{K}/K$ is alg and $\forall f(x) \in K(x)$, it splits completely over L

FACT 1

K is algebraically closed $\Leftrightarrow K = \bar{K}$

Proof

"$\Rightarrow$": Claim: $\forall f(x) \in K(x)$, $f(x)$ splits over K

Proof (intuition: recursively divide, we still have a root in K)

By induction on $n = \deg f$,

- $n=1$: $f(x) = ax+b = a(x+\frac{b}{a})$
- $n>1$: Let $\alpha \in K$ be a root of $f(x)$. We have $f(x) = (x-\alpha)f_1(x)$ where $f_1(x) \in K(\alpha)[x] = K[x]$ and $\deg f_1 < n$

$\therefore f_1(x) = \lambda(x-\alpha_1)\cdots(x-\alpha_{n-1})$, $\alpha_i \in K$ ✓

"$\Leftarrow$": $\forall f \in K[x]$, $f(x)$ splits over $\bar{K} = K$, i.e. $f(x) = \lambda(x-\alpha_1)\cdots(x-\alpha_n)$ for $\alpha_i \in K$ $\therefore f(\alpha_i) = 0$

FACT 2

If $\bar{K}$ is an alg closure of K, then $\bar{K}$ is alg closed

Proof

Let $f(x) \in \bar{K}[x]$ and α be a root of $f(x)$. Then, $\bar{K}(\alpha)/\bar{K}$ is alg

By def, $\bar{K}/K$ is alg, so $\bar{K}(\alpha)/K$ is alg $\therefore \alpha$ is alg over K, i.e. $\alpha \in \bar{K}$ □

Shun/翔海 (@shun4midx)

FACT 3

Given L/K, if L is algebraically closed, then $L_\alpha = \{\alpha \in L \mid \alpha \text{ is alg over } K\} = \bar{K}$

Proof

$\forall f(x) \in K(x) \subseteq L[x]$, $f(x) = \lambda(x-\alpha_1)\dots(x-\alpha_n)$ for some $\alpha_i \in L$. Hence, $\alpha_i \in L_\alpha \ \forall i$, i.e. $f(x)$ splits over L_α

THEOREM

If K is a field, then $\bar{K}$ exists.

Proof (variable, not element)

Let $S = \{x_f \mid f \in K[x], \deg f \geq 1\}$

Consider the poly ring $K[S]$ and $I = \langle f(x_f) : \deg f \geq 1 \rangle \subset K[S]$

Claim: $I \neq K[S]$ ($\Rightarrow \exists M \in \mathrm{Max}\, K[S]$, s.t. $M \supseteq I$. Let $F_1 = K[S]/M$ which is a field and $K \hookrightarrow F_1$, then $f(\bar{x}_f) = 0$) (element, no longer variable)

Proof

Assume not, i.e. $I = K[S]$, say $1 = g_1 f_1(x_{f_1}) + \dots + g_n f_n(x_{f_n})$, $g_i \in K[S]$

Write $x_i := x_{f_i}$ and assume $g_i \in K(x_1, \dots, x_m]$, $m \geq n$

Also, $\exists \alpha_i \in \Omega \supseteq K$ (just any root for f_i), s.t. $f_i(\alpha_i) = 0$, $\alpha_j = 0 \ \forall j > n$. Then, $1 = g(\alpha_1, \dots, \alpha_m) f_1(\alpha_1) + \dots + g(\alpha_1, \dots, \alpha_n) f_n(\alpha_n) = 0$ ↯

By induction, $\exists F_1 \subseteq F_2 \subseteq F_3 \subseteq \dots$ s.t. $\forall f \in F_n[x]$, $\exists$ a root in F_{n+1}

Now, let $F = \bigcup_{i \geq 1} F_i$ which is a field and is alg closed by construction.

Finally, we take $\bar{K} = \{\alpha \in F \mid \alpha \text{ alg over } K\}$ □

GEOMETRIC CONSTRUCTION

DEFINITION ($z_1 = 0, z_2 = 1$)

Given $\{z_1, \dots, z_n\} \in \mathbb{C}$, $C(z_1, \dots, z_n) = \{z \in \mathbb{C} \mid z \text{ is constructable by rule and compass from } z_1, \dots, z_n\}$

($S_1 = \{z_1, \dots, z_n\} \rightsquigarrow S_2 \rightsquigarrow S_3 \cdots$, $C(z_1, \dots, z_n) = \bigcup_{i \geq 1} S_i$)

Notice, S_{i-1} lines: Any straight line between any two points in S_{i-1}

S_{i-1} circles: Any circle with a center in S_{i-1} and another point in S_{i-1} as its radius away

Now, we construct S_i with the following within S_{i-1}

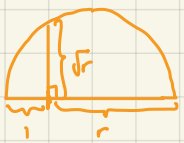
↪ I: Any intersection between two lines

↪ II: Any intersection between a line and a circle

↪ III: Any intersection between two circles

FACT 4

$C(S_1, \dots, S_n)$ is a subfield of $\mathbb{C}$ (Proof idea: $z = re^{i\theta}$, multiplication done with similar triangles)



FACT 5

$z \in C(S_1, \dots, S_n) \Rightarrow \bar{z}, z^{\frac{1}{2}} \in C(S_1, \dots, S_n)$ (Proof idea for $\sqrt{z}$: $\sqrt{z} = \sqrt{r}e^{i\frac{\theta}{2}}$. Angle bisection $\Rightarrow \frac{\theta}{2}$ is OK. $\sqrt{r}$ can be done with semicircle)

PROPOSITION 3

$C(z_1, \dots, z_n)$ is the smallest subfield of $\mathbb{C}$ containing $z_1, \dots, z_n$ and closed under conjugation and square roots

Proof

Let C' be any subfield of $\mathbb{C}$. Hope "$C' \supseteq C(z_1, \dots, z_n)$"

Observe: • $-1 \in C' \Rightarrow \sqrt{-1} = i \in C'$

• $x+iy \in C'$, $x, y \in \mathbb{R} \Rightarrow x, y \in C'$, since $x+iy \in C'$, $\overline{x+iy} = x-iy \in C'$

Shun/翔海 (@shun4midx)

Also, any line through distinct points in C' has $ax+by+c=0$, $a,b,c\in C'$
any circle constructed from C' has $x^2+y^2+dx+ey+f=0$, $d,e,f\in C'$ or $(x-a)^2+(y-b)^2=c$, $a,b,c\in C'$

from (I), (II), (III), we know any intersection point still lies in C'. Hence, $C'\supseteq C(z_1,\dots,z_n)$. □

THEOREM 2

Let $z_1=0$, $z_2=1$, $\dots$, $z_n\in\mathbb{C}$ and $F=\mathbb{Q}(z_1,\dots,z_n,\bar{z}_1,\dots,\bar{z}_n)$

Then, $C(z_1,\dots,z_n)=\{z\in\mathbb{C}\mid \exists u_1,\dots,u_r \text{ with } u_i^2\in F,\ u_i\in F(u_1,\dots,u_{i-1}) \text{ s.t. } z\in F(u_1,\dots,u_r)\}$ (say RHS $=:C''$)

Proof

"$\supseteq$": By fact 5, $F\subseteq C(z_1,\dots,z_n)\Rightarrow u_1\in C(z_1,\dots,z_n)\Rightarrow u_2\in C(z_1,\dots,z_n,u_1)=C(z_1,\dots,z_n)$

Continue this logic, we get $F(u_1,\dots,u_r)\subseteq C(z_1,\dots,z_r)$

"$\subseteq$":
- C'' is a subfield: $z\in F(u_1,\dots,u_r)$, $z'\in F(u_1',\dots,u_s')\in C''\Rightarrow z\pm z'$, zz', z^{-1}, $(z')^{-1}\in F(u_1,\dots,u_r,u_1',\dots,u_s')$ ✓
- For $z\in C''$, say $z\in F(u_1,\dots,u_r)$, then $\sqrt{z}\in F(u_1,\dots,u_r,\sqrt{z})$ $\therefore\sqrt{z}\in C''$
- For $\bar{z}\in C''$, say $\bar{z}\in F(u_1,\dots,u_r)$, then $\bar{z}\in\overline{F(u_1,\dots,u_r)}=F(\bar{u}_1,\dots,\bar{u}_r)$ $\therefore\bar{z}\in C''$

$\therefore$ The result follows from proposition 3. □

COROLLARY

If $z\in C(z_1,\dots,z_n)$, then $[F(z):F]=2^m$ for some $m\in\mathbb{N}$

Proof

Let $z\in F(u_1,\dots,u_r)$. Observe that if $u_i\in F(u_1,\dots,u_{i-1})$, then $[F(u_1,\dots,u_i):F(u_1,\dots,u_{i-1})]=1$

if $u_i\notin F(u_1,\dots,u_{i-1})$, then $[F(u_1,\dots,u_i):F(u_1,\dots,u_{i-1})]=2$

$\therefore$ Continuing this process, we get $[F(u_1,\dots,u_r):F]=2^s$ and $[F(z):F]\mid 2^s\Rightarrow[F(z):F]=2^m$ □

REMARK (3 big questions)

1. If a unit cube has volume 1, ∄ cube s.t. volume=2?
   ↳ $z=\sqrt[3]{2}\rightsquigarrow x^3-2$ $\therefore[\mathbb{Q}(z):\mathbb{Q}]=3$ ✗ (not power of 2)
2. ∄ square of area π?
   ↳ $z=\sqrt{\pi}\rightsquigarrow x^2-\pi$ $\therefore[\mathbb{Q}(\pi):\mathbb{Q}]=\infty$ ✗
3. $z=\cos 20^\circ$ is drawable? $\rightsquigarrow\frac{1}{2}=4\cos^3 20^\circ-3\cos 20^\circ\rightsquigarrow 8x^3-6x-1\rightsquigarrow$ deg=3 ✗

Now, about construction of p-gons, p: a prime, it is equivalent to drawing $z=\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}$, $z^p=1\Rightarrow z^{p-1}+z^{p-2}+\dots+1=0$

For this to be drawable, we need $[\mathbb{Q}(z):\mathbb{Q}]=p-1=2^m$, so we only can do so for $p=2^m+1$, $m=2^t$ (but is it for all $p=2^{2^t}+1$?)

4-18-25 (WEEK 9)

Shun / 舜海 (@shun4midx)

SPLITTING FIELDS

DEFINITION

Let $f(x)$ be a nonconstant polynomial in $K[x]$.
L is called a splitting field for f over K if L is the smallest field over which f splits

THEOREM 1 (Existence of a splitting field)

If $f(x)$ is of deg $n>0$, then $\exists$ a splitting field L for f over K with $[L:K]\leq n!$

Proof

By induction on n,

- $n=1$: $f(x)=ax+b$, $a,b\in K \Rightarrow L=K(-\frac{b}{a})=K \Rightarrow [L:K]=1$
- $n>1$: By Kronecker's Thm, $\exists\ K_1/K$ and $\alpha\in K_1$, s.t. $f(\alpha_1)=0$
  By division algorithm, $\exists f_1(x)\in K(\alpha_1)[x]$ with deg $f_1=n-1$, s.t. $f(x)=(x-\alpha_1)f_1(x)$
  By induction hypothesis, $\exists$ a splitting field L for f_1 over $K(\alpha_1)$ with $[L:K(\alpha_1)]\leq n!$
  By def, $f_1(x)=\lambda(x-\alpha_2)(x-\alpha_3)\cdots(x-\alpha_n)$, $\alpha_i\in L$
  Hence, $f(x)=\lambda(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ and $L=K(\alpha_1)(\alpha_2,\dots,\alpha_n)=K(\alpha_1,\dots,\alpha_n)$
  $\therefore [L:K]=[L:K(\alpha_1)][K(\alpha_1):K]\leq (n-1)!\,n=n!$ □

FACT

Let K, L be two fields and $\tau: K\hookrightarrow L$ be a nontrivial homo. Then, $\exists\ \bar{\tau}: K[x]\xrightarrow{\sim}\tau(K)[x]$ ($K\xrightarrow{\sim}\tau(K)$) and if $f(x)$ is irred, then

$a_nx^n+\dots+a_0 \longmapsto \tau(a_n)x^n+\dots+\tau(a_0)$

$\bar{\tau}(f)$ is also irred

Proof

- $\tau: K\xrightarrow{\sim}\tau(K)$ since $\ker\tau=\{0\}\Rightarrow \bar{\tau}: K[x]\xrightarrow{\sim}\tau(K)[x]$
- If $\bar{\tau}(f)=gh$ with deg $g>0$, deg $h>0$, then $f=\bar{\tau}^{-1}(g)\,\bar{\tau}^{-1}(h)$ □

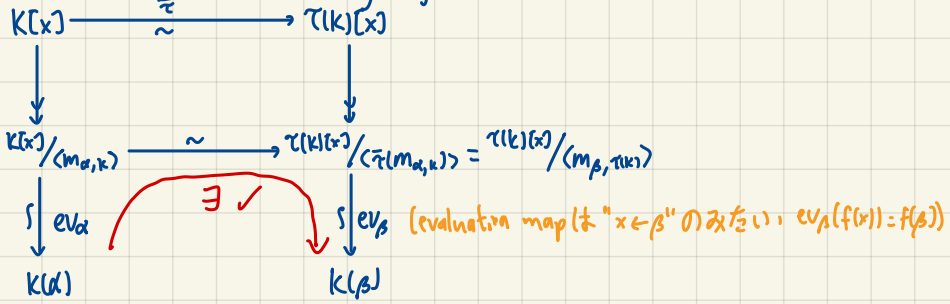
LEMMA

Given $K(\alpha)/K$ with α being algebraic over K, if $\tau: K\to L$ is nontrivial, then $\exists$ an extension σ of τ from $K(\alpha)$ to $L \Leftrightarrow \exists\ \beta\in L$, s.t. $\bar{\tau}(m_{\alpha,K})(\beta)=0$

Proof

"$\Rightarrow$": Let $\beta=\sigma(\alpha)$ and $m_{\alpha,K}=x^n+a_{n-1}x^{n-1}+\dots+a_0$
Then, $\bar{\tau}(m_{\alpha,K})(\beta)=\bar{\tau}(m_{\alpha,K})(\sigma(\alpha))=\sigma(\alpha)^n+\tau(a_{n-1})\sigma(\alpha)^{n-1}+\dots+\tau(a_0)=\sigma(\alpha^n+a_{n-1}\alpha^{n-1}+\dots+a_0)=\sigma(0)=0$ □ ($\tau(a_{n-1})=\sigma(a_{n-1})$, $\tau(a_0)=\sigma(a_0)$)

"$\Leftarrow$": First observe that $\bar{\tau}(m_{\alpha,K})=m_{\beta,\tau(K)}$ since $\bar{\tau}(m_{\alpha,K})(\beta)=0$ and it is irreducible and monic
Then, σ comes from the following diagram:



REMARK

The number of extensions $\leq$ deg $m_{\alpha,K}$. In particular, "=" holds if all roots of $m_{\alpha,K}$ are distinct ("<" because we can have repeated roots) (∵ extension ⇒ need to "grab" a root)

Shun/翔海 (@shun4midx)

THEOREM 2 (Uniqueness of a Splitting Field)

Let $\tau: K \xrightarrow{\sim} K'$ be an isomorphism of fields. Let $f(x) \in K[x]$ with a splitting field L over K. Then, τ can be extended to an isomorphism $\sigma: L \xrightarrow{\sim} L'$ and $\bar{\tau}(f(x)) \in K'[x]$ with a splitting field L' over K'.

Proof

By induction on $n = \deg f$,

- $n=1$: $L=K$ and $L'=K'$, so set $\sigma=\tau$
- $n>1$: Assume $f(\alpha)=0$. Since $m_{\alpha,K} \mid f \Rightarrow \bar{\tau}(m_{\alpha,K}) \mid \bar{\tau}(f)$, $\exists\, \beta \in L'$, s.t. $\bar{\tau}(m_{\alpha,K})(\beta)=0$ and $\bar{\tau}(m_{\alpha,K}) = m_{\beta,K'}$
  By lemma, $\exists\, \tau_1: K(\alpha) \xrightarrow{\sim} K'(\beta)$ which extends τ
  On one hand, we can write $f(x) = (x-\alpha) f_1(x)$, $f_1(x) \in K(\alpha)[x]$. Note, L is a splitting field for f_1 over $K(\alpha)$.
  On the other hand, $\bar{\tau}(f(x)) = \bar{\tau}_1(f(x)) = (x-\tau_1(\alpha))(\bar{\tau}_1(f_1(x))) = (x-\beta)\,\bar{\tau}_1(f_1(x)) \Rightarrow L$ is a splitting field for $\bar{\tau}_1(f_1)$ over $K'(\beta)$
  $\therefore$ By induction hypothesis, τ_1 is extended to an isom $\sigma: L \xrightarrow{\sim} L'$ which is also an extension of τ □

REMARK

The number of such extensions of τ is $\leq [L:K]$

of $\tau_1 \leq \deg m_{\alpha,K} = [K(\alpha):K]$
By induction hypothesis, # of σ over $\tau_1 \leq [L:K(\alpha)]$

$\therefore$ Total $\leq [L:K(\alpha)][K(\alpha):K] = [L:K]$

THEOREM 3

If L/K_1 is algebraic and $0 \neq \tau: K_1 \to K_2$ with K_2 algebraically closed, then τ can be extended to $\sigma: L \to K_2$

Proof

Set $S = \{(M, \theta) \mid M$ is a field s.t. $K_1 \subseteq M \subseteq L$, $\theta: M \to K_2$ is an extension of $\tau\}$
Since $(K_1, \tau) \in S$, thus $S \neq \emptyset$

Define partial order "$(M_1, \theta_1) \leq (M_2, \theta_2)$ iff $M_1 \subseteq M_2$ and $\theta_2|_{M_1} = \theta_1$"

Given a chain $\{(M_i, \theta_i) \mid i \in \Lambda\}$ in S, consider $N = \bigcup_{i \in \Lambda} M_i$, which is a field, and $\phi: N \to K_2$, $M_i \ni \alpha \mapsto \theta_i(\alpha)$

Then, (N, ϕ) is a least upper bound for this chain.
$\therefore$ By Zorn's Lemma, $\exists$ a max element $(M, \sigma) \in S$.

Claim: $M = L$

Proof

Suppose $M \subsetneq L$. Pick $\alpha \in L \setminus M$. Since K_2 is algebraically closed, $\exists\, \beta \in K_2$, s.t. $\bar{\sigma}(m_{\alpha,M})(\beta) = 0$
Hence, $\exists\, \sigma_1: M(\alpha) \to K_2$ with $\sigma_1|_M = \sigma$. Thus, $(M(\alpha), \sigma_1) \not\supseteq (M, \sigma)$ ↯
($\alpha \mapsto \beta$)

COROLLARY

Any two algebraic closures L_1, L_2 of K are isomorphic

Proof

Consider the inclusion homo $\tau: K \to L_2$
$\because L_1/K$ is alg and L_2 is alg closed
$\therefore \exists\, 0 \neq \sigma: L_1 \hookrightarrow L_2$, s.t. $\sigma|_K = \mathrm{id}_K$
Note that $\sigma(L_1)$ is alg closed since $L_1 \cong \sigma(L_1)$. Now, $\forall \beta \in L_2$, β is alg over $K \subseteq \sigma(L_1) \Rightarrow \beta \in \sigma(L_1)$, i.e. $L_2 = \sigma(L_1)$ □

EXAMPLE

$f(x) = x^p - 2$, p: prime (it is irred due to Eisenstein)

- $m_{\sqrt[p]{2},\mathbb{Q}} = f(x)$ since $f(x)$ is irred and monic
- Roots: $\sqrt[p]{2}, \sqrt[p]{2}\zeta_p, \sqrt[p]{2}\zeta_p^2, \ldots, \sqrt[p]{2}\zeta_p^{p-1} \Rightarrow L = \mathbb{Q}(\sqrt[p]{2}, \zeta_p) = \mathbb{Q}(\sqrt[p]{2})\mathbb{Q}(\zeta_p)$

(はい, associated poly は x^p-1 けど, $x^p-1 = (x-1)(x^{p-1}+\ldots+1)$ それは irred じゃない / それは irred)

We know that $[\mathbb{Q}(\sqrt[p]{2}):\mathbb{Q}] = p$, $[\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1$
$\therefore [L:\mathbb{Q}] = p(p-1)$ ($\because p, p-1$ coprime)

Shun / 舜海 (@shun4midx)

REMARK

Given L/L_1 and L/L_2, L_1L_2 = smallest subfield of L containing L_1 and L_2

Assume $[L_1:K]=m$ and $[L_2:K]=n$ with $\gcd(m,n)=1$. Then, $[L_1L_2:K]=mn$

Proof

$m=[L_1:K] \mid [L_1L_2:K]$, $n=[L_2:K] \mid [L_1L_2:K] \Rightarrow mn \mid [L_1L_2:K]$ ✓

Now, $L_2=K(\alpha_1,\dots,\alpha_n)$, $L_1L_2=L_1K(\alpha_1,\dots,\alpha_n)=L_1(\alpha_1,\dots,\alpha_n)$ since $m_{\alpha_i,L_1} \mid m_{\alpha_i,K}$

$\Rightarrow [L_1L_2:K]=[L_1(\alpha_1,\dots,\alpha_n):L_1][L_1:K] \le mn$

$\therefore [L_1L_2:K]=mn$ □

REMARK (IMPORTANT)

Let L/K be algebraic and $\tau: L \to L$ (with $L \supseteq Z$) be a monomorphism fixing K. Then, τ is onto

$f(x)=m_{z,K}(x)$, deg $f=n$, f has roots $z=z_1,\dots,z_n$

Then, $\tau: z_i \longmapsto z_j$, i.e. $\tau: \{z_1,\dots,z_n\} \cap L \xrightarrow{1\text{-}1} \{z_1,\dots,z_n\} \cap L$

Shun / 舜海 (@shun4midx)

SEPARABLE EXTENSIONS

RECALL

Given $f(x) \in K[x]$, L/K, L'/K: splitting fields for $f(x)$ over K, $\sigma: L \xrightarrow{\sim} L'$ which fixes K,
If $f(x) = (x-\alpha_1)^{n_1} \cdots (x-\alpha_s)^{n_s}$ with $\alpha_i \in L$, then $f(x) = (x-\sigma(\alpha_1))^{n_1} \cdots (x-\sigma(\alpha_s))^{n_s}$

If $n_i = 1$, then α_i is called a simple root in $L \Rightarrow \sigma(\alpha_i)$ is also a simple root in L'
If $n_i > 1$, then α_i is called a multiple root in $L \Rightarrow \sigma(\alpha_i)$ is also a multiple root in L'

DEFINITION

- A polynomial $f(x) \in K[x]$ is said to be **separable** over K if its factors have **no multiple root** in a splitting field L over K
- If $f(x) = a_n x^n + \dots + a_0$, then $f'(x) = n a_n x^{n-1} + \dots + a_1$

CRITERION

Let $f(x)$ be a monic poly of positive degree in $K(x)$.
Then, all roots of $f(x)$ in a splitting field are simple $\Leftrightarrow (f, f') = 1$ (↑ gcd)

Proof

"$\Rightarrow$": We can write $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$, $\alpha_1, \dots, \alpha_n$ distinct
Then, $f'(x) = \sum_{i=1}^{n} (x-\alpha_1)\cdots\widehat{(x-\alpha_i)}\cdots(x-\alpha_n) \Rightarrow (x-\alpha_i) \nmid f'(x)$ $\forall i$
$\therefore (f(x), f'(x)) = 1$ ✓

"$\Leftarrow$": Suppose $f(x)$ has a multiple root α, so $f(x) = (x-\alpha)^k g(x)$, $k > 1$
Then, $f'(x) = k(x-\alpha)^{k-1} g(x) + (x-\alpha)^k g'(x) \Rightarrow (x-\alpha) \mid f'(x) \Rightarrow (x-\alpha) \mid (f', f)$ ↯

REMARK

TFAE
(1) α is a multiple root of f
(2) α is a common root of $f(x)$ and $f'(x)$
(3) $m_{\alpha,k} \mid f(x)$ and $m_{\alpha,k} \mid f'(x)$

PROPOSITION 1

Any irr poly $f(x)$ is not separable (⇗ separable ≠ irr) over K iff $\operatorname{char} K = p > 0$ and $f(x) = g(x^p)$ for some $g \in K[x]$

Proof

"$\Rightarrow$": Let L be a splitting field for f over K and $\alpha \in L$ be a multiple root of $f(x)$. Then, $m_{\alpha,k} \mid f$, $m_{\alpha,k} \mid f'$
$\because f$ is irr $\therefore f \sim m_{\alpha,k}$, i.e. $\deg m_{\alpha,k} = \deg f$
Now, $\begin{cases} m_{\alpha,k} \mid f' \\ \deg m_{\alpha,k} > \deg f' \end{cases} \Rightarrow f' \equiv 0$

If $\operatorname{char} K = 0$, then $f = c \in K$ ↯
$\therefore$ We must have $\operatorname{char} K = p > 0$. Let $f(x) = b_0 + b_1 x + \dots + b_m x^m$
Here, $f'(x) \equiv 0 \Rightarrow i b_i = 0$ $\forall i = 1, \dots, m$, if $b_i \neq 0$, then $p \mid i$
That is, $f(x) = b_0 + b_p x^p + b_{2p} x^{2p} + \dots + b_{np} x^{np} = g(x^p)$, where $g(x) = b_0 + b_p x + b_{2p} x^2 + \dots + b_{np} x^n$ ✓

"$\Leftarrow$": $f'(x) \equiv 0 \Rightarrow$ if $m_{\alpha,k} \mid f$, then $m_{\alpha,k} \mid f' \Rightarrow \alpha$ is a multiple root of $f(x)$

REMARK

f is irr $\Rightarrow g$ is irr and not all b_i are in K^p

Proof

- If $g = g_1 g_2$, then $f(x) = g(x^p) = g_1(x^p) g_2(x^p)$ ↯
- If $\forall i$, $b_i = a_i^p$ for some $a_i \in K$, then $f(x) = a_0^p + a_p^p x^p + \dots + a_{np}^p x^{np} = (a_0 + a_p x + \dots + a_{np} x^n)^p$ ↯ $(x+y)^p = x^p + y^p$

Shun/舜海 (@shun4midx)

DEFINITION

- A field of char p is said to be **perfect** if $K=K^p$
- A field of char 0 is also said to be perfect

COROLLARY

K is perfect $\Leftrightarrow$ every polynomial in $K[x]$ is separable

Proof

"$\Rightarrow$": By prop 1, if char $K=0$, then all irr poly are separable
if char $K=p$, then $K=K^p \Rightarrow \nexists\, g$ in prop 1 $\Rightarrow$ all irr poly are separable

"$\Leftarrow$": If char $K=p>0$ and $K^p \subsetneq K$, then take $b\in K\setminus K^p \Rightarrow x^p-b$ is inseparable over K

↳ Proof x^p-b is irr: $x^p-b=g(x)h(x)$ in $K[x]$ with monic $g(x)$ and $1\le \deg g=k\le p-1$
Let L be a splitting field for x^p-b over K and $\alpha\in L$ with $\alpha^p=b$
Then, $x^p-\alpha^p=(x-\alpha)^p$ and $g(x)=(x-\alpha)^k$ in $L[x] \Rightarrow \alpha^k\in K$. As $\alpha^p\in K$, thus $\alpha\in K \Rightarrow b=\alpha^p\in K^p$ ↯

PROPOSITION 2

Let char $K=p$ and $\phi: K\longrightarrow K,\ \alpha\longmapsto\alpha^p$ be the **Frobenius monomorphism**. If $K/\mathbb{F}_p$ (= $K/\mathbb{Z}/p\mathbb{Z}$) is algebraic, then ϕ is an automorphism, i.e. $K=K^p$

In particular, any finite field is perfect

DEFINITION

- $\alpha\in L$ is said to be separable over K if $m_{\alpha,K}$ is separable
- L/K is separable if $\forall\alpha\in L$, α is separable over K

PROPOSITION 3

Let $[L:K]=d$ and $\tau: K\to L'$ be a nontrivial homo. If L/K is separable and $\forall\alpha\in L$, $\bar\tau(m_{\alpha,K})$ splits over L', then $\exists$ exactly d extensions $\sigma: L\to L'$ of τ. Otherwise, $\exists\, r<d$ such extensions.

Proof sketch

- $m_{\alpha,K}$ is separable $\Rightarrow \bar\tau(m_{\alpha,K})$ is separable
- By induction on d, $d=1\Rightarrow \sigma=\tau$.
  $d>1$: $\alpha\in L\setminus K \Rightarrow \exists$ exactly $[K(\alpha):K]$ extensions $\tau_1: K(\alpha)\to L'$
  (Otherwise, pick α s.t. it's inseparable. Then, $\exists \le [K(\alpha):K]$ extensions)
- L/K is separable $\Rightarrow L/K(\alpha)$ is separable ($\forall\beta\in L$, $m_{\beta,K(\alpha)}\mid m_{\beta,K}$)
  $\Rightarrow$ By induction hypothesis, $\exists$ exactly $[L:L(\alpha)]$ extensions σ of τ_1 (otherwise, $<$), so in total, $\exists$ exactly $[L:K(\alpha)][K(\alpha):K]$ exts of τ. ($\tau_1\to\sigma$, $\tau\to\tau_1$)

PROPOSITION 4

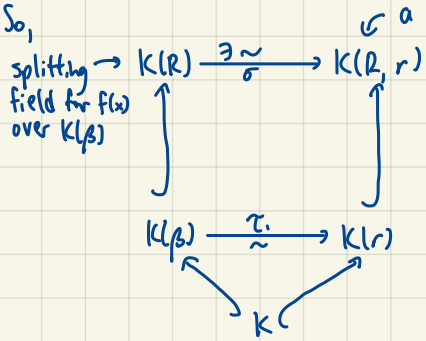
If $K(\alpha_1,\dots,\alpha_n)/K$ is alg and L is a splitting field for $f(x)=m_{\alpha_1,K}\dots m_{\alpha_n,K}$ over K, then $\forall\beta\in K(\alpha_1,\dots,\alpha_n)$, $m_{\beta,K}$ also splits over L

Proof

$\because m_{\beta,K}\in K[x]\subseteq L[x]$ $\therefore$ We can take $\Sigma\in r$, a root of $m_{\beta,K}$, as a splitting field of $m_{\beta,K}$ over L

We also write $L=K(R)$, where $R=$ the set of all roots of $f(x)$

So,



↳ a splitting field for $f(x)=\bar\tau_1(f(x))$ over $K(r)$

Now, $[K(R):K]=[K(R):K(\beta)][K(\beta):K]$
$=[K(R,r):K(r)][K(r):K]$
$=[K(R,r):K]$

$\therefore K(R)=K(R,r)$, i.e. $r\in K(R)$ □

Shun/翔海 (@shun4midx)

PROPOSITION 5

Given $K(\alpha_1,\dots,\alpha_n)/K$, if α_i is separable over $K(\alpha_1,\dots,\alpha_{i-1})=K_{i-1}$, then $K(\alpha_1,\dots,\alpha_n)/K$ is separable

Proof

Let L be a splitting field of $f(x)=m_{\alpha_1,K}\cdots m_{\alpha_n,K}$ over K. Observe that $\exists$ $[K(\alpha_1):K]$ ($=K_1$) extensions $\tau_1: K(\alpha_1)\longrightarrow L$ of $id: K\to K$ and

$\exists$ $[K(\alpha_1,\alpha_2):K(\alpha_1)]$ extensions $\tau_2: K(\alpha_1,\alpha_2)\longrightarrow L$ of $\tau_1: K_1\to L$

Continue, then $\exists$ $[K(\alpha_1,\dots,\alpha_n):K_{n-1}]$ extensions $\tau_n: K_n\to L$ of $\tau_{n-1}: K_{n-1}\to L$

$\therefore$ In total, $\exists$ $[K(\alpha_1,\dots,\alpha_n):K_{n-1}]\cdots[K_1:K]=[K_n:K]$ extensions $\sigma: K_n\to L$

By prop 4, $\forall \beta\in K(\alpha_1,\dots,\alpha_n)$, $m_{\beta,K}$ splits over L. $\therefore$ By prop 3, $K(\alpha_1,\dots,\alpha_n)/K$ is separable

COROLLARY

M/K is separable $\Leftrightarrow$ M/L, L/K are separable

Proof

"$\Rightarrow$": OK

"$\Leftarrow$": $\forall \alpha\in M$, α is separable for some $K(a_1,\dots,a_m)\le L$ (coef of $m_{\alpha,L}$)

By prop 5, $K(a_1,\dots,a_m)/K$ is separable $\square$

Shun / 舜海 (@shun4midx)

GALOIS EXTENSIONS

DEFINITION

L/K is called a normal extension if $\forall \alpha \in L$, α is alg over K, and $m_{\alpha,K}$ splits over L

PROPOSITION 1

L/K is finite and normal $\Leftrightarrow$ L is a splitting field for f over K

Proof

"$\Rightarrow$": Write $L = K(\alpha_1, \dots, \alpha_n)$ and let $f(x) = m_{\alpha_1,K} \cdots m_{\alpha_n,K}$

Claim: L is a splitting field Σ of $f(x)$, i.e. "$L = \Sigma$"

Proof

"$\subseteq$": $\forall \alpha_i$, $f(\alpha_i) = 0 \Rightarrow \alpha_i \in \Sigma \Rightarrow L \subseteq \Sigma$ ✓

"$\supseteq$": $\forall \beta$: root of $m_{\alpha,K}$, by def of normal, $\beta \in L$ ✓

"$\Leftarrow$": Let $L = K(\alpha_1, \dots, \alpha_n)$, $\{\alpha_1, \dots, \alpha_n\}$ is the set of all roots of $f(x)$

Note: $f(x)$ and $m_{\alpha_1,K} \cdots m_{\alpha_n,K}$ have the same set of roots

$\therefore$ We know $\forall \beta \in K(\alpha_1, \dots, \alpha_n)$, $m_{\beta,K}$ splits over L, i.e. L/K is normal

Moreover, $\forall \alpha_i$, α_i is alg over $K \Rightarrow L/K$ is finite. □

REMARK

If L/K is normal, then $\forall M$ with $L \supseteq M \supseteq K$, L/M is normal but M/K need not be normal

Proof

$\forall \alpha \in L$, $m_{\alpha,M} \mid m_{\alpha,K}$, so "$m_{\alpha,K}$ splits over $L \Rightarrow m_{\alpha,M}$ splits over L"

However, "M/K need not be normal":

↳ Let $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$, which is a splitting field for $x^3 - 2$ over $\mathbb{Q}$

But $M = \mathbb{Q}(\sqrt[3]{2})$ is not normal, since $m_{\sqrt[3]{2},\mathbb{Q}} = x^3 - 2$ does not split over $\mathbb{Q}(\sqrt[3]{2})$

DEFINITION

Given L/K, $(\mathrm{Aut}(L), \circ)$ is a group. Then, $\mathrm{Aut}(L/K) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma|_K : \mathrm{id}_K\} \leq \mathrm{Aut}(L)$

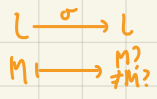
PROPOSITION 2

Let L be finite, normal, and $L \supseteq M \supseteq K$. Then, TFAE

(a) M/K is normal

(b) $\forall \sigma \in \mathrm{Aut}(L/K)$, $\sigma(M) \subseteq M$

(c) $\forall \sigma \in \mathrm{Aut}(L/K)$, $\sigma(M) = M$



Proof

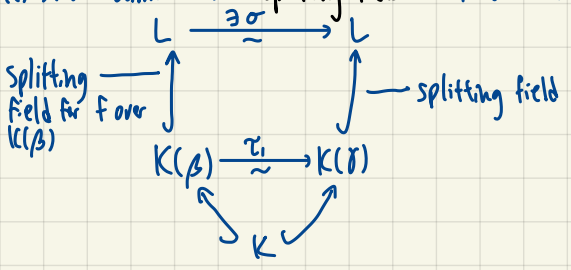
(a)$\Rightarrow$(b): $\forall \beta \in M$, $m_{\beta,K}(\sigma(\beta)) = \sigma(m_{\beta,K}(\beta)) = 0$

$\therefore \sigma(\beta)$ is a root of $m_{\beta,K}$

$\therefore \sigma(\beta) \in M$ since $m_{\beta,K}$ splits over M.

(b)$\Rightarrow$(c): $\because M/K$ is alg $\therefore \sigma|_M$ is nontrivial $\Rightarrow$ subjective

(c)$\Rightarrow$(a): Assume L is a splitting field for f over K. For $\beta \in M$, if $r \in L$ is another root of $m_{\beta,K}$, then we have



Here, σ extends τ_1, so it fixes K, i.e. $\sigma \in \mathrm{Aut}(L/K)$. By assumption, $\gamma = \tau_1(\beta) = \sigma(\beta) \in M$ □

Shun/翔海 (@shun4midx)

DEFINITION

- L/K is called a Galois extension if L/K is finite, normal, and separable, i.e. L is a splitting field for some separable poly over K
- If L/K is Galois, then define $\mathrm{Gal}(L/K) := \mathrm{Aut}(L/K)$

PROPOSITION

If L/K is Galois, then $|\mathrm{Gal}(L/K)| = [L:K]$. Otherwise, $|\mathrm{Aut}(L/K)| < [L:K]$

Proof

We know:

- normal $\Rightarrow \forall \beta \in L$, $m_{\beta,K}$ splits over L
- separable $\Rightarrow \exists$ exactly $[L:K]$ extensions $\sigma: L \to L$ of id$_K$. Also, L/K is alg $\Leftrightarrow \sigma$ is an auto
  That is, $|\mathrm{Aut}(L/K)| = [L:K]$

Otherwise, $|\mathrm{Aut}(L/K)| < [L:K]$ □

DEFINITION

Let G be a subgroup of $\mathrm{Aut}(L)$. Then, $\mathrm{Inv}\, G = \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \forall \sigma \in G\}$ (invariant) is a subfield of L

THEOREM (Artin)

If $G \leq \mathrm{Aut}(L)$ (finite), then $|G| = [L:\mathrm{Inv}\, G]$, and $G = \mathrm{Aut}(L/\mathrm{Inv}\, G)$, i.e. $L/\mathrm{Inv}\, G$ is a Galois group

Proof

Claim: $[L:\mathrm{Inv}\, G] \leq |G|$

Proof

Assume that $[L:\mathrm{Inv}\, G] > |G| =: n$. Let $G = \{\sigma_1 = \mathrm{id}, \dots, \sigma_n\}$ and $\exists$ indep $b_1, \dots, b_{n+1} \in L$ over $\mathrm{Inv}\, G$

Consider

$$(*)\begin{cases} \sigma_1(b_1)x_1 + \dots + \sigma_1(b_{n+1})x_{n+1} = 0 \\ \vdots \\ \sigma_n(b_1)x_1 + \dots + \sigma_n(b_{n+1})x_{n+1} = 0 \end{cases}$$

, which has a nontrivial solution, since #variables > #equations

Choose one $(a_1, \dots, a_{n+1})$ with the smallest number, say m, nonzero members

By reordering, we may assume it is $(a_1, \dots, a_m, 0, \dots, 0)$

If $m = 1$, then $\sigma_1(b_1)a_1 = 0 \Rightarrow a_1 = 0$ ($b_1 \neq 0$) ↯

Hence, $m > 1$, and $\sigma_1(b_1)a_1 + \dots + \sigma_1(b_m)a_m = 0$ (**) $\forall i = 1, \dots, n$

By multiplying a_m^{-1}, we may assume $a_m = 1$.

Observe, for $i = 1$, $b_1 a_1 + \dots + b_m a_m = 0$, so not all $a_i \in \mathrm{Inv}\, G$, say $a_1 \notin \mathrm{Inv}\, G$ and $\sigma_t(a_1) \neq a_1$ for some t.

By applying σ_t to (**), we get $\sigma_t\sigma_1(b_1)\sigma_t(a_1) + \dots + \sigma_t\sigma_1(b_m)\sigma_t(a_m) = 0$ $\forall i = 1, \dots, n$ (↓ $i: a_m = 1$)

As $\{\sigma_t\sigma_1, \dots, \sigma_t\sigma_n\} = \{\sigma_1, \dots, \sigma_n\}$, hence we have (***) $\sigma_1(b_1)\sigma_t(a_1) + \dots + \sigma_1(b_m)\sigma_t(a_m) = 0$ $\forall i = 1, \dots, n$

(**) − (***): $\sigma_1(b_1)(a_1 - \sigma_t(a_1)) + \dots + \sigma_1(b_{m-1})(a_{m-1} - \sigma_t(a_{m-1})) = 0$ $\forall i = 1, \dots, n$ ($\neq 0$, $i: a_1 \neq \sigma_t(a_1)$)

∴ We find that $(a_1 - \sigma_t(a_1), \dots, a_{m-1} - \sigma_t(a_{m-1}), 0, \dots, 0)$ is a nontrivial solution of (*), smaller than m nonzero terms ↯

Now, by def, $G \leq \mathrm{Aut}(L/\mathrm{Inv}\, G)$, so $|G| \leq |\mathrm{Aut}(L/\mathrm{Inv}\, G)| \leq [L:\mathrm{Inv}\, G] \leq |G| \Rightarrow |G| = |\mathrm{Aut}(L/\mathrm{Inv}\, G)| = [L:\mathrm{Inv}\, G]$

∴ $G = \mathrm{Aut}(L/\mathrm{Inv}\, G)$ and $L/\mathrm{Inv}\, G$ is Galois □

COROLLARY

L/K is Galois $\Leftrightarrow \mathrm{Inv}\, \mathrm{Aut}(L/K) = K$

Proof

"$\Rightarrow$": ∵ L/K is Galois ∴ $|\mathrm{Aut}(L/K)| = [L:K]$. By thm, $[L:K] = |\mathrm{Aut}(L/L)| = [L:\mathrm{Inv}\, \mathrm{Aut}(L/K)]$ ∴ $K = \mathrm{Inv}\, \mathrm{Aut}(L/K)$ □

"$\Leftarrow$": By thm, ok.

Shun/翔海 (@shun4midx)

DEFINITION

Let $f \in K[x]$ be separable and L be a splitting field for f over K. $Gal(L/k)$ is called the Galois group of f.

FACT

If $\deg f = n$, then the Galois group of f can be regarded as a subgroup of S_n

Proof

Let $\{\alpha_1, \dots, \alpha_n\}$ be the set of roots of f.

For $\sigma \in Gal(L/k)$, $f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = 0 \Rightarrow \sigma(\alpha_i) = \{\alpha_1, \dots, \alpha_n\} = A$

So, $\sigma: \{\alpha_1, \dots, \alpha_n\} \longrightarrow \{\alpha_1, \dots, \alpha_n\}$ is 1-1 and thus onto.

$\therefore \sigma|_A \in S_n$

EXAMPLE

To determine the Galois group of $x^4 - 2$

The roots of $x^4 - 2$ are $\pm\sqrt[4]{2}, \pm\sqrt[4]{2}i$

$\therefore$ The splitting field for $x^4 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{2}i) = \mathbb{Q}(\sqrt[4]{2}, i) =: L$

- $[L:\mathbb{Q}] = [L:\mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}] = 2(4) = 8$ ($\mathbb{Q}(\sqrt[4]{2})(i)$, $x^4 - 2$)
- $\sigma \in Gal(L/\mathbb{Q})$: $\sigma: i \longmapsto i$, $\sqrt[4]{2} \longmapsto \sqrt[4]{2}i$; $\tau: i \longmapsto -i$, $\sqrt[4]{2} \longmapsto \sqrt[4]{2}$

  Then, $\sigma^4 = \tau^2 = id$, $\tau\sigma\tau = \sigma^3$

  $\therefore \langle \sigma, \tau \mid \sigma^4 = \tau^2 = id, \tau\sigma\tau = \sigma^3 \rangle \subseteq Gal(L/\mathbb{Q})$, where $|Gal(L/\mathbb{Q})| = 8$

  $\therefore Gal(L/\mathbb{Q}) \cong D_8$
- $G = \langle \sigma \rangle \leq Gal(L/\mathbb{Q})$: $Inv\, G = ?$

  ↳ $\because |G| = 4$, $[L : Inv\, G] = 4 \Rightarrow [Inv\, G : \mathbb{Q}] = 2$. As $\mathbb{Q}(i) \subseteq Inv\, G$, thus $Inv\, G = \mathbb{Q}(i)$ ($\because [\mathbb{Q}(i):\mathbb{Q}] = 2$)
- Similarly, $G = \langle \tau \rangle \Rightarrow Inv\, G = \mathbb{Q}(\sqrt[4]{2})$

Shun / 舜海 (@shun4midx)

FUNDAMENTAL THEOREM

MAIN THEOREM (finite, separable, normal)

Let L/K be a Galois extension and $G=\mathrm{Gal}(L/K)$. Then, $\{M \mid M \text{ is a field with } K\subseteq M\subseteq L\} \longleftrightarrow \{H : H\leq G\}$

$$M \longmapsto \mathrm{Gal}(L/M)$$
$$K\subseteq \mathrm{Inv}\, H \longmapsfrom H$$

s.t. (1) $H \longmapsto \mathrm{Inv}\,H \longmapsto \mathrm{Gal}(L/\mathrm{Inv}\,H)=H$ by Artin theorem

$M \longmapsto \mathrm{Gal}(L/M) \longmapsto \mathrm{Inv}\,\mathrm{Gal}(L/M)=M$ by corollary of Artin theorem

(2) If $M_1=\mathrm{Inv}\,H_1$, $M_2=\mathrm{Inv}\,H_2$, then $M_1\subseteq M_2 \Leftrightarrow H_1\geq H_2$

(3) If $M=\mathrm{Inv}\,H$, then $H\lhd G \Leftrightarrow M/K$ is normal

Proof

Recall: M/K is normal $\Leftrightarrow \forall \sigma\in G,\ \sigma(M)=M \Leftrightarrow \forall\sigma\in G,\ \mathrm{Gal}(L/\sigma(M))=\mathrm{Gal}(L/M)$ ("$\in$": Just take Inv on both sides)

and $\tau\in\mathrm{Gal}(L/\sigma(M)) \Leftrightarrow \tau(\sigma(x))=\sigma(x)\ \forall x\in M \Leftrightarrow \sigma^{-1}\tau\sigma(x)=x\ \forall x\in M \Leftrightarrow \sigma^{-1}\tau\sigma\in\mathrm{Gal}(L/M) \Leftrightarrow \sigma\,\mathrm{Gal}(L/M)\sigma^{-1}$ $\therefore \mathrm{Gal}(L/\sigma(M))=\sigma\,\mathrm{Gal}(L/M)\sigma^{-1}$

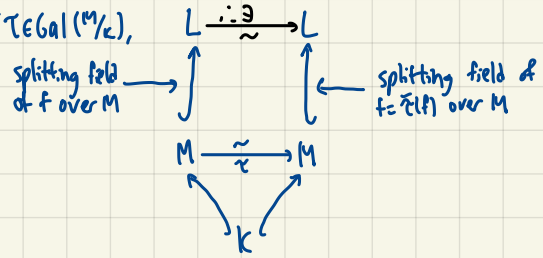
So, M/K is normal $\Leftrightarrow \mathrm{Gal}(L/M)\lhd G$ □

(4) If $H\lhd G$, then $G/H\cong \mathrm{Gal}(M/K)$

Proof

Define $\phi: G \longrightarrow \mathrm{Gal}(M/K)$, $\sigma \longmapsto \sigma|_M$

- ϕ is surjective: $\forall \tau\in\mathrm{Gal}(M/K)$,



- $\sigma\in\ker\phi \Leftrightarrow \sigma|_M=\mathrm{id}_M \Leftrightarrow \sigma\in\mathrm{Gal}(L/M)=H$

$\therefore$ By 1st Isom thm, $G/H\cong\mathrm{Gal}(M/K)$ □

(5) If $M_1=\mathrm{Inv}\,H_1$, $M_2=\mathrm{Inv}\,H_2$, then $M_1\cap M_2=\mathrm{Inv}\langle H_1,H_2\rangle$, $M_1M_2=\mathrm{Inv}\,H_1\cap H_2 \Leftrightarrow H_1\cap H_2=\mathrm{Gal}(L/M_1M_2)$

Proof

- $\alpha\in\mathrm{Inv}\langle H_1,H_2\rangle \Leftrightarrow \alpha\in\mathrm{Inv}\,H_1\cap\mathrm{Inv}\,H_2$
- $\tau\in H_1\cap H_2 \Leftrightarrow \tau$ fixes $M_1=K(\alpha_1,\dots,\alpha_s)$ and τ fixes $M_2=K(\beta_1,\dots,\beta_t) \Leftrightarrow \tau$ fixes $K(\alpha_1,\dots,\alpha_s,\beta_1,\dots,\beta_t)=M_1M_2$ □

PROPOSITION

Let L/K be Galois and N/K be arbitrary

Then, LN/N is Galois and $\phi:\mathrm{Gal}(LN/N)\cong\mathrm{Gal}(L/L\cap N)$

$\sigma \longmapsto \sigma|_L$?

Proof

- Let L be the splitting field for the separable poly f over N, say $L=K(\alpha_1,\dots,\alpha_n)$

Then, $LN=N(\alpha_1,\dots,\alpha_n)$, hence LN/N is Galois ✓

- ϕ is well-def: $\because f(\sigma(\alpha_i))=\sigma(f(\alpha_i))=0$ (as σ fixes K and $f\in K[x]$)

$\therefore \{\sigma(\alpha_1),\dots,\sigma(\alpha_n)\}=\{\alpha_1,\dots,\alpha_n\}$

- ϕ is 1-1: $\sigma\in\ker\phi \Leftrightarrow \sigma|_L=\mathrm{id}_L \Leftrightarrow \sigma(\alpha_i)=\alpha_i\ \forall i \Leftrightarrow \sigma|_M$
- ϕ is onto: let $H=\mathrm{Inv}\,\phi\leq\mathrm{Gal}(L/L\cap N)$ ($\leftrightarrow \mathrm{Inv}\,H=L\cap N$ (★))

(★): "$\supseteq$": obvious

"$\subseteq$": $\forall\sigma\in\mathrm{Gal}(LN/N)$, $\sigma|_L=x\ \forall x\in(\mathrm{Inv}\,H)N$

$\Rightarrow N\subseteq(\mathrm{Inv}\,H)N\subseteq\mathrm{Inv}\,\mathrm{Gal}(LN/N)=N \Rightarrow N=(\mathrm{Inv}\,H)N \Rightarrow \mathrm{Inv}\,H\subseteq N$ ✓

Check ϕ isom

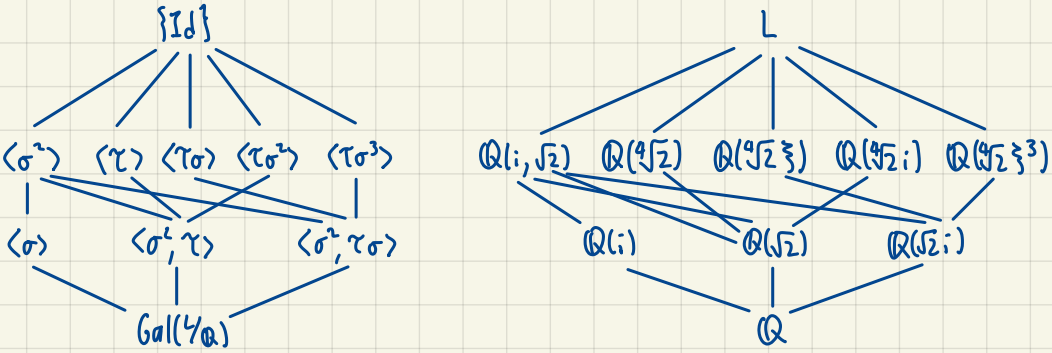
Shun/翔海 (@shun4midx)

EXAMPLE

Let $f(x)=x^4+2 \Rightarrow$ splitting field $L=\mathbb{Q}(i,\sqrt[4]{2})$

$\therefore [L:\mathbb{Q}]=8$, $Gal(L/\mathbb{Q}) \cong D_8$

$\langle \sigma, \tau \rangle$



CYCLOTOMIC EXTENSION OVER $\mathbb{Q}$

DEFINITION

- $\zeta \in \mathbb{C}$ is called an n-th root of unity if $\zeta^n=1$
- ζ is primitive if $\zeta^n=1$ but $\zeta^l \neq 1$ for $l<n$
- $\zeta_n = e^{\frac{2\pi i}{n}}$
- $\{\text{primitive } n\text{-th root of unity}\} = \{\zeta_n^k \mid 1 \le k < n, \gcd(k,n)=1\}$

DEFINITION

The nth cyclotomic poly is $\Phi_n := \prod_{1 \le k < n, \gcd(k,n)=1} (x-\zeta_n^k)$ which has degree $\phi(n)$

FACTS

- $\Phi_n \in \mathbb{Z}[x]$: By induction on n, $n=1$: $\Phi_1 = x-1$.

  $n>1$: $x^n-1 = \prod_{d \mid n} \Phi_d = \left(\prod_{d \mid n, d<n} \Phi_d\right) \Phi_n$

  $x^n-1 \in \mathbb{Z}[x]$; $\prod_{d \mid n, d<n} \Phi_d \in \mathbb{Z}[x]$ By ind hyp

  By direct comparison of coeffs on both sides, $\Phi_n \in \mathbb{Z}[x]$. □

- Φ_n is irr in $\mathbb{Z}[x]$: [Φ_n is monic, Φ_n irr in $\mathbb{Z}[x] \Leftrightarrow \Phi_n$ irr in $\mathbb{Q}[x]$, so $\Phi_n = m_{\zeta_n, \mathbb{Q}}$]

  Suppose $\Phi_n = f \cdot g$, f is irr and monic, g is monic in $\mathbb{Z}[x]$

  Let ζ be a primitive nth root of unity s.t. $f(\zeta)=0$ and p be a prime s.t. $p \nmid n$

  If $g(\zeta^p)=0$, then ζ is a root of $g(x^p) \Rightarrow f(x) \mid g(x^p)$, say $g(x^p)=f(x)h(x)$

  In $\mathbb{Z}/p\mathbb{Z}[x]$, $\bar{g}(x^p)=\bar{f}(x)\bar{h}(x) \Rightarrow (\bar{g}(x))^p = \bar{f}(x)\bar{h}(x) \Rightarrow \bar{g}(x)$ and $\bar{f}(x)$ have a common root

  $\therefore \bar{\Phi}_n = \bar{f} \cdot \bar{g}$ has a repeated root $\Rightarrow x^n-\bar{1}$ has a repeated root $\Rightarrow (x^n-\bar{1})' = \bar{n}x^{n-1} = 0 \Rightarrow p \mid n$ ↯

  $\therefore$ We conclude that $f(\zeta^p)=0$ $\forall p \nmid n$. By induction, $f(\zeta^{p^r}) = f((\zeta^{p^{r-1}})^p)=0$ $\forall r \in \mathbb{N}$ and $f(\zeta^{p_1^{r_1} \cdots p_s^{r_s}}) = f((\zeta^{p_1^{r_1} \cdots p_s^{r_s-1}})^{p_s})=0$ $\forall p_i \nmid n, r_i \in \mathbb{N}$

  $\therefore f(\zeta^k)=0$ $\forall 1 \le k < n$, $\gcd(k,n)=1$, i.e. $\Phi_n = f$ is irr □

QUESTION: IS EVERY FINITE GROUP G ISOMORPHIC TO SOME GALOIS GROUP $Gal(L/k)$?

Strategy: $S_n \not\supseteq Gal(L/k)$

CONSTRUCTION

Write $f(x)=(x-t_1)(x-t_2)\cdots(x-t_n) = x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots + (-1)^n s_n \in K[x]$, $K=F(s_1,\cdots,s_n)$

Let $L=K(t_1,\cdots,t_n)$ be a splitting field for f over K. Then, $Gal(L/k) \hookrightarrow S_n$. Notice, $L=F(t_1,\cdots,t_n)$

Now, for S_n, we can regard σ as an element in $Gal(L/k)$: $\sigma: F(t_1,\cdots,t_n) \longrightarrow F(t_1,\cdots,t_n)$

$a \in F \mapsto a \in F$

$t_i \mapsto t_{\sigma(i)}$

$f(t_1,\cdots,t_n) \mapsto f(t_{\sigma(1)},\cdots,t_{\sigma(n)})$

Key: $\sigma(s_i)=s_i\ \forall i$ since $\{\sigma(t_1),\dots,\sigma(t_n)\}=\{t_1,\dots,t_n\} \Rightarrow \sigma|_K=id_K$, i.e. $\sigma\in Gal(L/K)=S_n$

Shun/翔海 (@shun4midx)

COROLLARY

$$\text{Inv } S_n = K = F(s_1,\dots,s_n)$$
$$\text{Inv } S_n = \{f(t_1,\dots,t_n)\in K \mid f(t_{\sigma(1)},\dots,t_{\sigma(n)})=f(t_1,\dots,t_n)\ \forall \sigma\in S_n\}$$

- $P_k=\sum_{i=1}^{n} t_i^k$

  Newton's identities: $kS_k=\sum_{i=1}^{k}(-1)^{i-1}S_{k-i}P_i$, $P_k=\sum_{i=1}^{k-1}(-1)^{i+k-1}S_{k-i}P_i+(-1)^{k-1}kS_k$

REMARK

Cubic equations, $\mathrm{char}F\neq 2,3$:

For $f(x)=x^3+px+q$, $L=F(\alpha_1,\alpha_2,\alpha_3)$, $\delta=(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)$, $\delta^2=D:=$ discriminant

Then, we have: $Gal(L/F)\cong S_3 \Leftrightarrow \sqrt{D}\notin F$

$Gal(L/F)\cong A_3 \Leftrightarrow \sqrt{D}\in F$

5-2-25 (WEEK 11)

Shun / 翔海 (@shun4midx)

ABELIAN EXTENSIONS

LEMMA

If L/K is finite, then L/K is simple $\Leftrightarrow \exists$ finitely many fields M s.t. $L \supseteq M \supseteq K$

Proof

"$\Rightarrow$": Suppose $L = K(\alpha)$ and $L \supseteq M \supseteq K$

Let $m_{\alpha,M} = x^n + a_{n-1}x^{n-1} + \dots + a_0$, $a_i \in M$

We find that $M = K(a_0, \dots, a_{n-1})$

Since $[K(\alpha) : K(a_0, \dots, a_{n-1})] = \deg m_{\alpha,M} = [M(\alpha) : M] = [K(\alpha) : M]$, thus $M = K(a_0, \dots, a_{n-1})$.

And $m_{\alpha,M} \mid m_{\alpha,K} \Rightarrow$ There are finitely many monic divisors of $m_{\alpha,K} \Rightarrow \exists$ finitely many fields M s.t. $L \supseteq M \supseteq K$

"$\Leftarrow$": Case 1: $|K| < \infty$

In this case, $|L| < \infty$. We know that $(L \setminus \{0\}, \dots, \cdot)$ is a cyclic group, say $L \setminus \{0\} = \langle x \rangle$

Then, $L \setminus \{0\} = \langle x \rangle \subseteq K(\alpha) \setminus \{0\}$, so $L \setminus \{0\} = K(\alpha) \setminus \{0\} \Rightarrow L = K(\alpha)$ ✓

Case 2: $|K| = \infty$

Let $L = K(\alpha_1, \dots, \alpha_n)$ and $M = K(\alpha_1, \alpha_2)$

For $\beta \in K$, set $F_\beta = K(\alpha_1 + \beta\alpha_2)$ and thus $K \subseteq F_\beta \subseteq L$

Since $|K| = \infty$, by contradiction, $\exists \beta \neq r$ in K, s.t. $F_\beta = K(\alpha_1 + \beta\alpha_2) = K(\alpha_1 + r\alpha_2) F_\alpha$, i.e. $\alpha_1 + \beta\alpha_2 - (\alpha_1 + r\alpha_2) \in F_\beta$

By induction, $L = f(\alpha)$ and hence $M = F_\beta$ □

THEOREM (PRIMITIVE ROOT THEOREM)

If L/K is finite and separable, then L/K is simple

Proof

Let $L = K(\alpha_1, \dots, \alpha_n)$ and $f(x) = m_{\alpha_1,K}\, m_{\alpha_2,K} \cdots m_{\alpha_n,K}$ be separable over K

Take N to be a splitting field for f over K. Since $|\mathrm{Gal}(N/K)| = [N:K] < \infty$, $\exists$ finitely many subgroups of $|\mathrm{Gal}(N/K)|$

$\therefore \exists$ finitely many intermediate fields between N and K

$\therefore \exists$ finitely many intermediate fields between L and K. □

COROLLARY

If L/K is Galois, then $\exists$ irr f in $K[x]$, s.t. L is the splitting field for f over K

Proof

Finite, Separable $\Rightarrow L = K(\alpha)$, $f = m_{\alpha,K}$ ($\because L/K$ is normal) □

DEFINITION

L/K is called a **cyclic (abelian) extension** if L/K is Galois and $\mathrm{Gal}(L/K)$ is cyclic (abelian)

PROPOSITION 1

Let $\sigma_1, \dots, \sigma_n$ be distinct in $\mathrm{Aut}(K)$ and $k_1, \dots, k_n \in K^*$. Then, $\exists c \in K$, s.t. $(k_1\sigma_1 + \dots + k_n\sigma_n)(c) \neq 0$

Proof

We want to show "$\sigma_1, \dots, \sigma_n$ are lin indep over K"

Assume it is not true.

Then, $\exists$ a minimal nonempty subset $\{\sigma_{i_1}, \dots, \sigma_{i_m}\}$ which is lin indep over K, say $b_1\sigma_{i_1}(k) + \dots + b_m\sigma_{i_m}(k) = 0$ $\forall k \in K$

If $m = 1$, then $b_1 \neq 0$, $b_1\sigma_{i_1}(k) = 0$ $\forall k \in K \Rightarrow \sigma_{i_1}(k) = 0$ $\forall k \in K \Rightarrow \sigma_{i_1} = 0$ ↯

So $m > 1$, choose $0 \neq h \in K$, s.t. $\sigma_{i_1}(h) \neq \sigma_{i_m}(h) \neq 0$

$\therefore$ We have $b_1\sigma_{i_1}(hk) + \dots + b_m\sigma_{i_m}(hk) = 0$ and $b_1\sigma_{i_1}(h)\sigma_{i_1}(k) + \dots + b_m\sigma_{i_m}(h)\sigma_{i_m}(k) = 0$ $\forall k \in K$.

Subtract the two, we get $b_1(\underbrace{\sigma_{i_m}(h) - \sigma_{i_1}(h)}_{\neq 0})\sigma_{i_1}(k) + \dots + b_{m-1}(\sigma_{i_m}(h) - \sigma_{i_1}(h))\sigma_{i_{m-1}}(k) = 0$ ↯

Shun / 舜海 (@shun4midx)

PROPOSITION 2

Assume that $\mathrm{char}\, k \nmid n$. Let L be the splitting field for separable $x^n - a$ over K and ζ be a primitive n^{th} root of unity. Then, $\mathrm{Gal}(L/K(\zeta))$ is cyclic of order dividing n. Moreover, $x^n - a$ is irr over $K(\zeta) \Leftrightarrow [L:K(\zeta)] = n$, i.e. $|\mathrm{Gal}(L/K(\zeta))| = n$

↳ $m_{\alpha, K(\zeta)} = x^n - a$

Proof

Let α be a root of $x^n - a$. Then $\alpha, \alpha\zeta, \dots, \alpha\zeta^{n-1}$ are all roots of $x^n - a$. Thus, $L = K(\alpha, \zeta) = K(\zeta)(\alpha)$

Consider $\phi : \mathrm{Gal}(L/K(\zeta)) \longrightarrow \mathbb{Z}/n\mathbb{Z}$

$(\sigma : \alpha \mapsto \alpha\zeta^{j_\sigma}) \longmapsto \bar{j}_\sigma$

- ϕ is a homo: $(\tau\circ\sigma)(\alpha) = \tau(\alpha\zeta^{j_\sigma}) = \tau(\alpha)\tau(\zeta^{j_\sigma}) = \alpha\zeta^{j_\tau}\zeta^{j_\sigma} = \alpha\zeta^{j_\tau + j_\sigma} \rightsquigarrow \bar{j}_\tau + \bar{j}_\sigma$
- ϕ is 1-1: $\sigma \in \ker\phi \Leftrightarrow \bar{j}_\sigma = \bar{0} \Leftrightarrow \sigma(\alpha) = \alpha \Leftrightarrow \sigma = \mathrm{Id}$

THEOREM 1

Assume that $\mathrm{char}\, k \nmid n$

If L/K is a cyclic extension of degree n with $\zeta \in K$, then L is a splitting field for some irr poly $x^n - a$ over K

Proof

Let $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ with $\mathrm{ord}(\sigma) = n$

By prop 1, $\exists\, c \in L$, s.t. $\alpha = c + \zeta\sigma(c) + \zeta^2\sigma^2(c) + \dots + \zeta^{n-1}\sigma^{n-1}(c) \neq 0$

$\therefore \sigma(\alpha) = \sigma(c) + \zeta\sigma^2(c) + \zeta^2\sigma^3(c) + \dots + \zeta^{n-1}c = \zeta^{-1}\alpha \Rightarrow \alpha \notin K$

But $\sigma(\alpha^n) = \zeta^{-n}\alpha^n = 1(\alpha^n) = \alpha^n \in K$

$\therefore K(\alpha) = K(\zeta, \alpha) \subseteq L$ is a splitting field for $x^n - a$ over K.

Also, $\sigma : K(\alpha) \longrightarrow K(\alpha) \Rightarrow (\sigma|_{K(\alpha)}) \leq \mathrm{Gal}(K(\alpha)/K)$

$\alpha \longmapsto \zeta^{-1}\alpha$

Hence, $n = [L:K] \geq [K(\alpha):K] = |\mathrm{Gal}(K(\alpha)/K)| \geq n \Rightarrow [L:K] = [K(\alpha):K] \Rightarrow L = K(\alpha)$, $[L:K] = n \Rightarrow x^n - a$ is irr. □

DEFINITION

Say $\mathrm{char}\, k \nmid n$ and ζ is a primitive n^{th} root of unity

- L/K is a **Kummer extension** of exponent n if $\zeta \in K$ and L is a splitting field for $(x^n - a_1)(x^n - a_2)\cdots(x^n - a_k)$ over K, $a_i \in K$
- Recall: $e(G)$ is the least positive integer m, s.t. $g^m = e$ $\forall g \in G$

THEOREM 2

If L/K is Galois s.t. $\mathrm{Gal}(L/K)$ is abelian of exponent n and $\zeta \in K$, then L/K is a Kummer extension of exponent n

Proof

By induction on $[L:K]$, $[L:K] = 1$, $n = 1 \Rightarrow$ ok. Assume that $[L:K] > 1$, by FTOFAG, $\mathrm{Gal}(L/K) \cong \underbrace{\mathbb{Z}/d_1\mathbb{Z} \times \dots}_{\cong H} \times \underbrace{\mathbb{Z}/d_s\mathbb{Z}}_{N = \text{cyclic group of order } N}$ with $d_i \mid d_{i+1}$, $i = 1, \dots, s-1$

$\Rightarrow n = d_s$, $e(H) = e = d_{s-1} \mid n$

If $s = 1$, then, by thm 1, it is done. Assume $s > 1$.

Set $M = \mathrm{Inv}\, N$, $[M:K] < [L:K]$ and $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) = N \cong H$

Also, $(\zeta^{\frac{n}{e}})^e = \zeta^n = 1 \Rightarrow \zeta^{\frac{n}{e}} \in K$ is a primitive e^{th} root of unity

$\therefore$ By induction hypothesis, M is a splitting field for $(x^e - b_1)\cdots(x^e - b_{k-1})$ over K, $b_j \in K$

Note: if we set $a_i := b_i^{\frac{n}{e}} \in K$, then M is also a splitting field for $(x^n - a_1)\cdots(x^n - a_{k-1})$ over K

Let $N = \langle\sigma\rangle$, then $\mathrm{Gal}(L/K) = \{\sigma^i\tau^j \mid 0 \leq i \leq n-1,\ \tau \in H\}$

By prop 1, $\exists\, c$, s.t. $\alpha = \sum_{\tau\in H}\tau(c) + \zeta\sum_{\tau\in H}\sigma\tau(c) + \dots + \zeta^{n-1}\sum_{\tau\in H}\sigma^{n-1}\tau(c) \neq 0$

$\therefore \sigma(\alpha) = \zeta^{-1}\alpha$, $\tau(\alpha) = \alpha$ $\forall \tau \in H$, $\sigma(\alpha^n) = \alpha^n \Rightarrow \alpha \notin M$, $a_k := \alpha^n \in M$, so $M(\alpha)$ is a splitting field for $x^k - a$ over M

Also, $n = [L:M] \geq [M(\alpha):M] = |\mathrm{Gal}(M(\alpha)/M)| \geq n \Rightarrow L = M(\alpha)$ □

REMARK

$L \rightsquigarrow (x^n - a_1)\cdots(x^n - a_k)$ (a_1 ⇝ a_k) $\Rightarrow \forall \sigma \in \mathrm{Gal}(L/K)$, $\sigma(\alpha_i) = \alpha_i\zeta^{j_{\sigma,i}}$, $0 \leq j_{\sigma,i} \leq n-1 \Rightarrow \sigma^n(\alpha_i) = \alpha_i\zeta^{nj_{\sigma,i}} = \alpha_i$ $\forall i \Rightarrow \sigma^n = \mathrm{id}$

$\forall \tau \in \mathrm{Gal}(L/K)$, $\tau\sigma(\alpha_i) = \tau(\alpha_i\zeta^{j_{\sigma,i}}) = \alpha_i\zeta^{j_{\tau,i}}\zeta^{j_{\sigma,i}} = \sigma\tau(\alpha_i)$ $\forall i \Rightarrow \sigma\tau = \tau\sigma$

5-7-25 (WEEK 12)

Shun / 舜海 (@shun4midx)

SOLUTION BY RADICALS

DEFINITION

- Given L/K and $\beta \in L$, β is called a **radical** over K if $\beta^n \in K$ for some $n \in \mathbb{N}$
- L/K is called an **extension by radicals** if $\exists\, L = L_n \supseteq L_{n-1} \supseteq \dots \supseteq L_0 = K$, s.t. $\forall i = 1, \dots, n$, $L_i = L_{i-1}(\beta_i)$ with β_i a radical over L_{i-1}
- $f(x) \in K[x]$ is **solvable by radicals** if $\exists\, L/K$ is an extension by radicals and f splits over L

RECALL

Let G be a finite group, G is **solvable** if $\exists\, \{e\} = G_n \lhd G_{n-1} \lhd \dots \lhd G_0 = G$, s.t. G_{i-1}/G_i is cyclic $\forall i$

MAIN THEOREM

Under some proper assumption on $\operatorname{char} K$, a separable poly $f(x) \in K[x]$ is solvable by radicals $\Leftrightarrow$ the Galois group of $f(x)$ over K is solvable

LEMMA 1

Given $M = L(\beta)$, $\beta^n \in L$, assume that $\operatorname{char} K \nmid n$. Then $\exists\, N$

$$\begin{array}{c} M \\ | \text{ by a radical} \\ L \\ | \text{ Galois} \\ K \end{array} \qquad \begin{array}{c} N \\ | \text{ by radicals} \\ M \\ | \\ L \\ | \\ K \end{array}$$

s.t. N/K is Galois and N contains a primitive root of unity ζ_n

Proof

We know that $M(\zeta_n) = L(\zeta_n, \beta)$ is a splitting field for $x^n - a = x^n - \beta^n$ (separable) over L

If we set $f(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} (x^n - \sigma(a))$ (separable), then all coef of $f(x)$ are elementary symmetric poly w.r.t. $\{\sigma(a) \mid \sigma \in \mathrm{Gal}(L/K)\}$, which are fixed by $\mathrm{Gal}(L/K)$, so $f(x) \in K(x)$

Assume that L is a splitting field for $g(x)$ over K. Then N is chosen as a splitting field for $f(x)g(x)$ (separable) over K

$\therefore$ By def, N/K is Galois

Note that $N = K(\underbrace{\alpha_1, \dots, \alpha_s}_{\text{roots of } g(x)}, \beta, \{\beta\sigma, \sigma \in \mathrm{Gal}(L/K) \setminus \{\mathrm{id}\}\}, \zeta_n)$

L — M — $\beta\sigma = \sigma(a)$

$\therefore$ N/M is an extension by radicals $\square$

LEMMA 2

Let $L = L_m \supseteq L_{m-1} \supseteq \dots \supseteq L_0 = K$ s.t. $L_i = L_{i-1}(\beta_i)$ with $\beta_i^{n_i} = a_i \in L_{i-1}$

If $\operatorname{char} K \nmid n_1 n_2 \cdots n_m$, then $\exists\, N/L$, s.t. N/K is a Galois extension by radicals and $\zeta_{n_i} \in N$ $\forall i = 1, \dots, m$

Proof

By induction on m,

- $m = 1$: $L = K(\beta_1)$ with $\beta_1^{n_1} = a_1 \in K$. Set $N = L(\zeta_n) = K(\zeta_n, \beta_1)$ which is a splitting field for $x^{n_1} - a_1$ over K
- $m > 1$: By induction hypothesis, $\exists\, N'/L_{m-1}$, s.t. N'/K is a Galois extension by radicals and N' contains ζ_{n_i} $\forall i = 1, \dots, m-1$

Sketch:

$L = L_{m-1}(\beta_m) \supseteq L_{m-1} \supseteq \dots \supseteq K$

$N'(\beta_m) \supseteq N'$ ← ind hyp

↑ By lemma 1

By lemma 1, $\exists\, N/N'(\beta_m)$, which is an extension by radicals s.t. N/K is Galois and N contains ζ_{n_m}. $\square$

Shun/翔海 (@shun4midx)

THEOREM A

Let $L=L_m \supseteq L_{m-1} \supseteq \dots \supseteq L_0 = K$ s.t. $L_i = L_{i-1}(\beta_i)$, $\beta_i^{n_i} = a_i \in L_{i-1}$ and $\mathrm{char} K \nmid n_1 \cdots n_m$.
If a separable poly $f \in K[x]$ splits over L, then the Galois group of f over K is solvable

REMARK

$H \lhd G$, G is solvable $\Leftrightarrow$ $H, G/H$ are solvable

Proof

"$\Leftarrow$": OK

"$\Rightarrow$": Assume $G = G_0 \rhd \cdots \rhd G_n = \{e\}$.

For H, $\dfrac{G_{i-1}\cap H}{G_i \cap H} = \dfrac{G_{i-1}\cap H}{(G_{i-1}\cap H)\cap G_i} \cong \dfrac{(G_{i-1}\cap H)G_i}{G_i} \hookrightarrow G_{i-1}/G_i$

For G/H, $G/H \rhd G_1H/H \rhd \cdots \Rightarrow \dfrac{G_{i-1}H/H}{G_iH/H} \cong G_{i-1}H/G_iH \ni xnG_iH = (\underbrace{xnx^{-1}}_{\in H})(\underbrace{a_ib_i}_{\in H}) = a^s a^{-s}(xnx^{-1})a^s b_i H = a^s G_i H \Rightarrow \dfrac{G_{i-1}H}{G_iH} \le \langle aG_iH \rangle$

PROOF OF THEOREM A

By lemma 2, we can assume that L/K is Galois ($\lceil L/L_i$ is Galois)

If we set $n = \mathrm{lcm}(n_1, \dots, n_m)$, then
- "containing ζ_n" $\Leftrightarrow$ "containing ζ_{n_i} $\forall i = 1, \dots, m$"
- $\zeta_n \in L$

Consider $L = L(\zeta) \supseteq L_{m-1}(\zeta) \supseteq \cdots \supseteq L_0(\zeta)$ (Galois)
(L, L_m'; L_{m-1}'; L_0')

We have L/L_i' is Galois and let $G_i = \mathrm{Gal}(L/L_i')$. We may also find:
- $G_m = \{e\}$, $G_0 = \mathrm{Gal}(L/L_0')$
- $G_{i-1}/G_i = \dfrac{\mathrm{Gal}(L/L_{i-1}')}{\mathrm{Gal}(L/L_i')} \cong \mathrm{Gal}(L_i'/L_{i-1}')$ is cyclic.

$\therefore$ G_0 is solvable

Moreover, $L \supseteq L_0 \supseteq K$, $K(\zeta)$ is a splitting field for $x^n - 1$ over K and $\mathrm{Gal}(K(\zeta)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \Rightarrow \mathrm{Gal}(K(\zeta)/K)$ is solvable
As $\mathrm{Gal}(K(\zeta)/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/L_0)$, thus $\mathrm{Gal}(L/K)$ is solvable

Let N be a splitting field for $f(x)$ over K. Then, $L \supseteq N$ and $\mathrm{Gal}(N/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/N)$ is solvable $\square$

THEOREM B

Let f be separable in $K[x]$ and L be a splitting field for f over K. Assume $\mathrm{char} K \nmid |\mathrm{Gal}(L/K)|$
If $\mathrm{Gal}(L/K)$ is solvable, then f is solvable by radicals

Proof

Let $n = |\mathrm{Gal}(L/K)|$ and $\zeta := \zeta_n$.
Let N be a splitting field for f over $K(\zeta)$, i.e. $N = LK(\zeta)$

Since $\mathrm{Gal}(LK(\zeta)/K(\zeta)) \cong \mathrm{Gal}(L/K(\zeta)\cap L) \le \mathrm{Gal}(L/K)$, $\mathrm{Gal}(L/K)$ is solvable $\Rightarrow \mathrm{Gal}(LK(\zeta)/K(\zeta))$ is solvable
Say $\{e\} = G_n \lhd \cdots \lhd G_0 = \mathrm{Gal}(N/K(\zeta))$, G_i/G_{i-1} is cyclic

If we set $N_j := \mathrm{Inv}\, G_j \le N$, then $N = N_m \supseteq \cdots \supseteq N_0 = K(\zeta)$ and $G_j = \mathrm{Gal}(N/N_j)$
Also, $G_{i-1}/G_i = \mathrm{Gal}(N/N_{i-1})/\mathrm{Gal}(N/N_i) \cong \mathrm{Gal}(N_i/N_{i-1})$ is cyclic

Note, $n_i = [N_i : N_{i-1}] = |G_{i-1}/G_i| \mid |G_0| \mid n \Rightarrow \zeta_{n_i} \in N_{i-1}/N_i$
Also, $\mathrm{char} K \nmid n_i$, so $N_i = N_{i-1}(\beta_i)$ with $\beta_i^{n_i} \in N_{i-1}$
$\therefore$ $N/K(\zeta)$ is an extension by radicals and thus N/K is too. $\square$

Shun / 翔海 (@shun4midx)

REMARK

In thm A, $Gal(K(\zeta)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$

In fact, $\hookrightarrow$ may not be "$=$".

For example, $n=5 \Rightarrow x^5-1$, $[K(\zeta_5):K]=4=\varphi(5)$ assume $\mathrm{char}K \neq 5$

$\Updownarrow$

$x^4+x^3+x^2+x+1$ irr in $K(x)$

$K=\mathbb{Z}/11\mathbb{Z}$, $x^4+x^3+x^2+x+1$ is divisible by $x-3$, in fact, it is $(x-3)(x-5)(x-4)(x-9) \Rightarrow \not\Rightarrow$ ($\because$ deg $=1 \neq \varphi(5)$)

$K=\mathbb{Z}/19\mathbb{Z}$, $x^4+x^3+x^2+x+1=(x^2+5x+1)(x^2-4x+1) \Rightarrow \not\Rightarrow$ ($\because$ deg $=2 \neq \varphi(5)$)

5-9-25 (WEEK 12)

Shun / 翔海 (@shun4midx)

FINITE FIELDS

WARM UP

Say $|K|=p^n$, K is a field. Then, $(K^\times, \cdot)$ is cyclic

FACT

$ab=ba$, $\text{ord}(a)=\alpha$, $\text{ord}(b)=\beta \Rightarrow \exists c \in \langle a,b\rangle$, s.t. $\text{ord}(c)=\text{lcm}(\alpha,\beta)$

Proof

Write $\alpha=\prod p_i^{m_i}$, $\beta=\prod p_i^{n_i}$

For each i, $(M_i,N_i)=\begin{cases}(m_i,0), & m_i \geq n_i \\ (0,n_i), & \text{otherwise}\end{cases}$

Set $\alpha'=\prod p_i^{M_i}$, $\beta'=\prod p_i^{N_i} \Rightarrow \text{lcm}(\alpha',\beta')=\text{lcm}(\alpha,\beta)$

Also, $\alpha' \mid \alpha$ and $\beta' \mid \beta \Rightarrow c=a^{\frac{\alpha}{\alpha'}} b^{\frac{\beta}{\beta'}} \Rightarrow \text{ord}(c)=\text{lcm}(\alpha,\beta)$ □

Let $d=$ lcm of the orders of all $a \in K^\times$

$\therefore \forall a \in K^\times$, $a^d=1 \Rightarrow a^{d+1}=a \Rightarrow (x-a) \mid x^{d+1}-x \Rightarrow |K^\times|=p^n-1 \leq d$

However, $\forall a \in K^\times$, $d \mid p^n-1$, $a^{p^n}=a$

$\therefore d=p^n-1$

$\therefore$ By fact and induction, $\exists g \in K^\times$, s.t. $K^\times=\langle g\rangle$ □

THEOREM 1

$\exists$ a finite field K, s.t. $|K|=q \Leftrightarrow q=p^n$ for some prime p and $n \in \mathbb{N}$. Moreover, K is unique up to isomorphism, denoted by $\mathbb{F}_{p^n}$

Proof

"$\Rightarrow$": Let $\text{char}K=p$, $[K:\mathbb{Z}/p\mathbb{Z}]=n \Rightarrow q=p^n$

"$\Leftarrow$": Let K be a splitting field for $f(x)=x^{p^n}-x$ over $\mathbb{Z}/p\mathbb{Z}$.

Claim: The set of all roots of f forms a field

Proof

$(\alpha \pm \beta)^{p^n}=\alpha^{p^n} \pm \beta^{p^n}=\alpha \pm \beta$, $(\alpha\beta)^{p^n}=\alpha^{p^n}\beta^{p^n}=\alpha\beta$, $(\alpha^{-1})^{p^n}=(\alpha^{p^n})^{-1}=\alpha^{-1}$ with $\alpha \neq 0$ ✓

As K is the smallest field containing all roots of $f(x)$ of f, $K=$ set of all roots of f

As $f'=-1$ has no roots, there is no multiple root, i.e. $|K|=p^n$

Note: $\mathbb{Z}/p\mathbb{Z} \hookleftarrow x^p-x=0$ and $x^p-x \mid x^{p^n}-x$, so $\mathbb{Z}/p\mathbb{Z} \hookrightarrow K$

$\because K$ is a splitting field for f

$\therefore K$ is unique up to isom □

THEOREM 2

(1) If $n \in \mathbb{Z}^{>0}$ and $\mathbb{F}_q$ is a finite field, then $\exists!\ \mathbb{F}_{q^n}/\mathbb{F}_q$, s.t. $[\mathbb{F}_{q^n}:\mathbb{F}_q]=n$ and it is Galois.

Proof

By thm 1, $q=p^r$ for some prime p and $r \in \mathbb{N}$.

Then, $q^n=p^{nr} \Rightarrow \mathbb{F}_{q^n}=\mathbb{F}_{p^{nr}}$ is Galois over $\mathbb{F}_p$, so $\mathbb{F}_{q^n}$ is Galois over $\mathbb{F}_{q^n} \supseteq \mathbb{F}_q \supseteq \mathbb{F}_p$ □

(2) $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)=\langle \sigma_q \rangle$, $\sigma_q: \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ (q-Frobenius automorphism)

$\alpha \longmapsto \alpha^q$

Proof

- $\sigma_q \in \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$
  - ↳ Homo since $q=p^r$
  - ↳ Isom since σ_q is not trivial
  - ↳ Fixes $\mathbb{F}_q$ since $\forall \alpha \in \mathbb{F}_q$, $\alpha^q=\alpha$

- $\forall \alpha \in \mathbb{F}_{q^n}$, $\sigma_q^n(\alpha) = \alpha^{q^n} = \alpha$ so $\sigma_q^n = Id$
  If $\sigma_q^m = Id$ with $1 \le m < n$, then $\sigma_q^m(\alpha) = \alpha^{q^m} = \alpha$ $\forall \alpha \in \mathbb{F}_{q^n} \Rightarrow$ number of $x^{q^m} - x = q^m < q^n$ —✗—
- $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \sigma_q \rangle$ since $|\langle \sigma_q \rangle| = n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = |Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)|$ □

REMARK

1. The subfields of $\mathbb{F}_{p^n}$ are Galois over $\mathbb{F}_p$ and they are $\mathbb{F}_{p^d}$, $d|n$, fixed by $\langle \sigma_p^d \rangle$
2. $\bigcup_{n \ge 1} \mathbb{F}_{p^n} = \overline{\mathbb{F}_p}$ is also a field ($\because \forall n_1, n_2$, $\mathbb{F}_{p^{n_1}}, \mathbb{F}_{p^{n_2}} \subseteq \mathbb{F}_{p^{n_1 n_2}}$)

THEOREM 3

$x^{p^n} - x$ = the product of all distinct monic irr poly in $\mathbb{F}_p[x]$ of deg d where d runs through all the divisors of n

Proof

Since $\mathbb{F}_p$ is a perfect field ($\mathbb{F}_p = \mathbb{F}_p^p$), all irr poly in $\mathbb{F}_p[x]$ are separable (no multiple root)

Also, if $f(x), g(x)$ are two monic irr poly in $\mathbb{F}_p[x]$ with $f(\alpha) = g(\alpha)$, then $f = m_{\alpha, \mathbb{F}_p} = g$

Hence, we can get the equality by checking that they have the same roots

"LHS|RHS": $\forall \alpha \in \mathbb{F}_{p^n}$, $\deg m_{\alpha, \mathbb{F}_{p^n}} = [\mathbb{F}_p(\alpha) : \mathbb{F}_{p^n}(\alpha)] \mid [\mathbb{F}_{p^n}(\alpha) : \mathbb{F}_p] = n$ and $m_{\alpha, \mathbb{F}_p}$ appears in RHS

"RHS|LHS": If β is a root of $p(x)$ in RHS with $d = \deg p | n$, then $p(x) = m_{\beta, \mathbb{F}_p}$
We have $|\mathbb{F}_p(\beta)| = p^d$ and $\beta^{p^d} = \beta$, so $\beta = \beta^{p^d} = (\beta^{p^d})^{p^d} = \beta^{p^{2d}} = \ldots = \beta^{p^n}$

EXAMPLE

$p = 2$, deg $1 \Rightarrow x^2 - x = x(x-1) \Rightarrow x, x-1$
deg $2 \Rightarrow x^{2^2} - x = x(x-1)(x^2+x+1) \Rightarrow x^2+x+1$
deg $3 \Rightarrow x^{2^3} - x = x(x-1)(x^3+x+1)(x^3+x^2+1) \Rightarrow x^3+x+1, x^3+x^2+1$

} corr. irr. poly

($2 \nmid 3$, so no repeated factors from deg 2)

REMARK

(Yes I've gone insane, don't question my sanity pls ty ボクは問題ない(www))

If $\psi_p(d)$ = number of irr poly of deg d in $\mathbb{F}_p[x]$, then $p^n = \sum_{d|n} d\psi_p(d)$ (The following part of this note will try to prove it)

DEFINITION

Möbius μ-function:

$$\mu(n) = \begin{cases} 1 & , n = 1 \\ 0 & , n \text{ has square power} \\ (-1)^n & , n \text{ is a product of distinct prime factors} \end{cases}$$

FACT 1

If $n \ge 1$, then $\sum_{d|n} \mu(d) = [\frac{1}{n}] = \begin{cases} 1, & n = 1 \\ 0, & n > 1 \end{cases}$

Proof

- $n = 1$: OK
- $n > 1$: Write $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then $\sum_{d|n} \mu(d) = \mu(1) + \mu(p_1) + \ldots + \mu(p_k) + \mu(p_1 p_2) + \ldots + \mu(p_1 p_2 \cdots p_k)$
  $= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \ldots + \binom{k}{k}(-1)^k = (1 + (-1))^k = 0$ □

DEFINITION

Let f, g be two arithmetic functions

The Dirichlet product of f and g is defined to be $f * g(n) = \sum_{d|n} f(d) g(\frac{n}{d})$ ($\Rightarrow f*g = g*f$, $(f*g)*h = f*(g*h)$)

- $I(n) = [\frac{1}{n}]$ is called the identity function
- $u(n) = 1$ $\forall n$ is the inverse of μ: $\mu * u(n) = \sum_{d|n} \mu(d) = I(n)$, $u * \mu = I$

FACT 2

Möbius inversion formula: $f(n) = \sum_{d|n} g(d) \Rightarrow g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$

Proof

$f(n) = g * u(n)$ $\forall n \Rightarrow f = g * u \Rightarrow f * \mu = g * u * \mu = g$ □

By fact 2, $n\psi_p(n) = \sum_{d|n} \mu(d) p^{\frac{n}{d}} \Rightarrow \psi_p(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}} \Rightarrow \psi_2(3)=2,\ \psi_3(3)=8,\ \psi_3(2)=3$

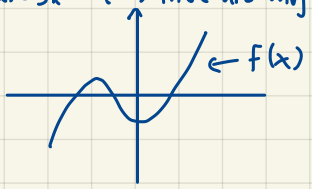
Shun/翔海 (@shun4midx)

GALOIS POLYNOMIAL EXAMPLE

Let $f(x) \in \mathbb{Q}[x]$ be irr of deg p, where p is a prime.
If f has exactly $p-2$ real roots and 2 complex roots, then the Galois group G of f over $\mathbb{Q}$ is S_p

EXAMPLE OF USAGE

Consider $f(x) = x^5 - 4x + 2$
↳ It is irr by Eisenstein criterion
↳ $f'(x) = 5x^4 - 4 \Rightarrow$ There are only two real turning points
∴



∴ The Galois group is S_5, so it is unsolvable.

PROOF

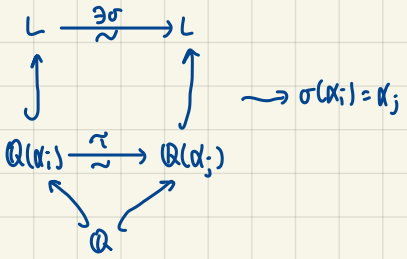
Let $R = \{\alpha_1, \dots, \alpha_p\}$ be the set of roots of f
$\alpha_i \sim \alpha_j \Leftrightarrow (\alpha_i : \alpha_j) \in G$
- $\alpha_i \sim \alpha_i$
- $\alpha_i \sim \alpha_j \Rightarrow \alpha_j \sim \alpha_i$
- $\alpha_i \sim \alpha_j,\ \alpha_j \sim \alpha_k \Rightarrow (\alpha_i : \alpha_j)(\alpha_j : \alpha_k)(\alpha_i : \alpha_j)^{-1} = (\alpha_i : \alpha_k) \in G$ ✓

$[\cdot]$ is equivalence class

Claim: $|[\alpha_i]| = |[\alpha_j]|$

Proof

$\sigma : [\alpha_i] \hookrightarrow [\alpha_j]$
$\alpha_k \mapsto \sigma(\alpha_k) \longrightarrow (\alpha_j\ \sigma(\alpha_k)) = (\sigma(\alpha_i)\ \sigma(\alpha_k)) = \sigma(\alpha_i : \alpha_k)\sigma^{-1}$
$(\alpha_i : \alpha_k) \in G$; $\sigma \in G$; $\sigma \in G$; $\sigma^{-1} \in G$



$\rightsquigarrow \sigma(\alpha_i) = \alpha_j$

Now, since $f(\overline{\alpha_i}) = \overline{f(\alpha_i)} = 0$,
$\tau : L \longrightarrow L$
$\alpha_i \mapsto \overline{\alpha_i}$
$\tau \in G$

Then, $\alpha_1, \dots, \alpha_{p-2} \in \mathbb{R}$, $\alpha_{p-1}, \alpha_p \in \mathbb{C}$ $\Rightarrow (\alpha_{p-1}, \alpha_p) \in G$ $\therefore |[\alpha_{p-1}]| \geq 2$

$R = \cup [\alpha_i] \Rightarrow |[\alpha_i]| \mid p \Rightarrow |[\alpha_i]| = p$
$[\alpha_1] = R$, $(\alpha_1, \alpha_2), (\alpha_1, \alpha_3), \dots, (\alpha_1, \alpha_p) \in G$, so $G = S_p$ □

5-14-25 (WEEK 13)

Shun / 郑翔海 (@shun4midx)

HILBERT THEOREM 90

- Trace and norm: Let $L=K(\alpha)$, $f(x)=m_{\alpha,K}=x^n+a_{n-1}x^{n-1}+\dots+a_0$

↳ f is separable and $\exists$ exactly n monomorphisms $\sigma_i: L \to \bar{K}$ fixing K and $\{\sigma_1(\alpha),\dots,\sigma_n(\alpha)\}$ consists of all roots of $f(x)$

$\Rightarrow x^n+a_{n-1}x^{n-1}+\dots+a_0=(x-\sigma_1(\alpha))\cdots(x-\sigma_n(\alpha))$

Norm: $(-1)^n a_0=\sigma_1(\alpha)\cdots\sigma_n(\alpha)$

Trace: $-a_{n-1}=\sigma_1(\alpha)+\dots+\sigma_n(\alpha)$

Moreover, we can take the K-linear transformation $T_\alpha: K(\alpha) \to K(\alpha)$, $v \mapsto \alpha v$

Then,

$$[T_\alpha]_{\{1,\dots,\alpha^{n-1}\}}=\begin{pmatrix} & & -a_0 \\ 1 & & -a_1 \\ & \ddots & \vdots \\ & 1 & -a_{n-1} \end{pmatrix} \Rightarrow \begin{cases} \text{Trace}=-a_{n-1} \\ \text{Norm}=(-1)^n a_0 \end{cases}$$

Here, we call $\sigma_1(\alpha)+\dots+\sigma_n(\alpha)=\mathrm{Tr}_{L/K}(\alpha)$ (trace of α) and $\sigma_1(\alpha)\cdots\sigma_n(\alpha)=N_{L/K}(\alpha)$ (norm of α)

↳ f is inseparable, $\mathrm{char}\,K=p>0$, $f(x)=\underset{\text{irr}}{f_1}(x^p)$, $f_1(x)=\underset{\text{irr}}{f_2}(x^p) \Rightarrow f(x)=f_2(x^{p^2})$, …, $f(x)=f_{sep}(x^{p^k})$, $\deg f_{sep}=m$

If $f_{sep}(x)=(x-\beta_1)\cdots(x-\beta_m)$, then $f(x)=(x^{p^k}-\beta_1)\cdots(x^{p^k}-\beta_m)$ and $\beta_i=\alpha_i^{p^k}$

$\therefore f(x)=[(x-\alpha_1)\cdots(x-\alpha_m)]^{p^k}$

Note that $\beta=\alpha^{p^k}$ is separable over K with $[K(\alpha^{p^k}):K]=m$ and α is purely inseparable over $K(\alpha^{p^k})$

$\Rightarrow K(\alpha^{p^k}) \subseteq L_{sep}$ and $L=K(\alpha)/K(\alpha^{p^k})$ is purely inseparable

DEFINITION

- α is purely inseparable over K if $\exists n\geq 0$, s.t. $\alpha^{p^n}\in K$ (separable is a type of purely inseparable)
- L/K is purely inseparable if $\forall \alpha\in L$, α is purely inseparable

FACT

- α purely insep $\Rightarrow$ $K(\alpha)/K$ purely insep

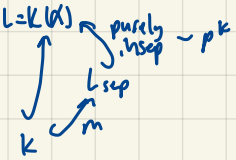
$(k_1\alpha_1^{r_1}+k_2\alpha_2^{r_2})^{p^n}=k_1^{p^n}(\underset{\in K}{\alpha_1^{p^n}})^{r_1}+k_2^{p^n}(\underset{\in K}{\alpha_2^{p^n}})\in K$

- β: sep + purely insep $\Rightarrow \beta\in K$

$\beta^{p^n}\in K \Rightarrow m_{\beta,K}=(x-\beta)^\lambda \mid x^{p^n}-\underset{\in K}{a}=(x-\beta)^{p^n}$

But β is sep $\Rightarrow \lambda=1$, i.e. $\beta\in K$.

Now, $L=K(\alpha) \longleftarrow L_{sep}$. By fact, $L_{sep}=K(\alpha^{p^k})$, $m=\deg f_{sep}=[L:K]_{sep}$, $p^k=[L:K]_i$



Also, $\exists$ exactly n monomorphisms $\sigma_i: L \to \bar{K}$ fixing K and $f(x)=[(x-\sigma_1(\alpha))\cdots(x-\sigma_m(\alpha))]^{p^k}$

Thus, $N_{L/K}(\alpha)=(\prod_{i=1}^{m}\sigma_i(\alpha))^{p^k}=[L:K]_i\,(\prod_{i=1}^{m}\sigma_i(\alpha))$

$\mathrm{Tr}_{L/K}(\alpha)=[L:K]_i\,(\sum_{i=1}^{m}\sigma_i(\alpha))$

Moral of the story: We don't always need "separable"

Shun / 舜海 (@shun4midx)

HILBERT THEOREM 90

If L/K is a cyclic extension of deg n with $G=\langle\sigma\rangle$, then $\alpha\in L\setminus\{0\}$. $N_{L/K}(\alpha)=1 \iff \exists \beta\in L\setminus\{0\}$, s.t. $\alpha=\frac{\sigma(\beta)}{\beta}$

$\Downarrow$

$H^1(\mathrm{Gal}(L/K)=G, L^\times)=\{1\}$

Proof

"$\Leftarrow$": $N_{L/K}(\alpha)=\prod_{i=0}^{n-1}\frac{\sigma^{i+1}(\beta)}{\sigma^i(\beta)}=1$

"$\Rightarrow$": We know $\exists c\in L$, s.t. $\beta^{-1}=\mathrm{id}(c)+\alpha\sigma(c)+\{\alpha\sigma(\alpha)\}\sigma^2(c)+\dots+\{\alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)\}\sigma^{n-1}(c)\neq 0$

$\therefore \alpha\sigma\beta^{-1}=\beta^{-1}\Rightarrow \alpha=\frac{\beta^{-1}}{\sigma\beta^{-1}}=\frac{\sigma(\beta)}{\beta}$. $\square$

"$H^1(\mathrm{Gal}(L/K)=G, L^\times)=\{1\}$" (Derivation / Image)

$$H^1(\mathrm{Gal}(L/K), L^\times):=\frac{Z^1(G,L^\times)}{B^1(G,L^\times)}=\frac{\{\phi: G\to L^\times \mid \forall\sigma,\tau\in G,\ \phi(\sigma\tau)=\phi(\sigma)\sigma(\phi(\tau))\}}{\{\phi: G\to L^\times \mid \exists b\in L^\times \text{ s.t. } \phi(\sigma)=\frac{b}{\sigma(b)}\ \forall\sigma\in G\}}$$

Now, $G=\langle\sigma\rangle$, $\phi\in Z^1$, $\phi(\sigma)=a$, $\phi(\sigma^2)=a\sigma(a)$, $\phi(\sigma^3)=a\sigma(a)\sigma^2(a)\dots$

$\therefore 1=\phi(1)=\phi(a^n)=a\sigma(a)\cdots\sigma^{n-1}(a)=N(a)$

$\therefore \exists b\in L$, s.t. $a\in\frac{b}{\sigma(b)}$, i.e. ϕ ✓

STATEMENT 2 OF HILBERT THEOREM

(II) $\alpha\in L$, $\mathrm{Tr}_{L/K}\alpha=0 \iff \exists\beta\in L$, s.t. $\alpha=\sigma(\beta)-\beta$

Proof

"$\Leftarrow$": $\mathrm{Tr}_{L/K}(\alpha)=\sum_{i=0}^{n-1}\sigma^i(\sigma(\beta)-\beta)=0$

"$\Rightarrow$": $\exists c\in L$, s.t. $\beta_1:=c+\sigma(c)+\dots+\sigma^{n-1}(c)\neq 0\Rightarrow\sigma(\beta_1)=\beta_1$

Let $\beta_2:=\alpha\sigma(c)+\{\alpha+\sigma(\alpha)\}\sigma^2(c)+\dots+\underbrace{\{\alpha+\sigma(\alpha)+\dots+\sigma^{n-2}(\alpha)\}}_{-\alpha}\underbrace{\sigma^n(c)}_{c}$

Then, $\beta_2-\sigma(\beta_2)=\alpha\beta_1\Rightarrow\alpha=\frac{\beta_2}{\beta_1}-\sigma\left(\frac{\beta_2}{\beta_1}\right)$ $\square$

COROLLARY

If $[L:K]=n$ with $\mathrm{char}\,K\nmid n$ and $\zeta_n\in K$, then "L/K is cyclic $\Rightarrow L=K(\alpha)$, α is a root of $x^n-a^{\in K}$"

Proof

Let $\mathrm{Gal}(L/K)=\langle\sigma\rangle$. Since $N_{L/K}(\zeta_n)=\zeta_n\sigma(\zeta_n)\cdots\sigma^{n-1}(\zeta_n)=\zeta_n\cdots\zeta_n=\zeta_n^n=1$, thus $\zeta_n=\frac{\sigma(\alpha)}{\alpha}$ for some α.

↳ Here, $\zeta_n=\frac{\sigma(\alpha)}{\alpha}\Rightarrow\sigma(\alpha)=\zeta_n\alpha\Rightarrow\sigma(\alpha^n)=\alpha^n\Rightarrow\alpha^n\in K$

Note that $\alpha, \zeta_n\alpha, \dots, \zeta_n^{n-1}\alpha$ are n roots of $x^n-a=x^n-\alpha^n$

$\because m_{\alpha,K}(\zeta_n^i\alpha)=m_{\alpha,K}(\sigma^i(\alpha))=\sigma^i(m_{\alpha,K}(\alpha))=\sigma^i(0)=0$

$\therefore$ We can conclude that $(x^n-a)\mid m_{\alpha,K}\Rightarrow m_{\alpha,K}=x^n-a\Rightarrow[K(\alpha):K]=n\Rightarrow L=K(\alpha)$ $\square$

PROPOSITION

Let $\mathrm{char}K=p$ and $[L:K]=p$. Then, L/K is cyclic $\iff L=K(\alpha)$ where α is a root of $x^p-x-a=0$

Proof

"$\Leftarrow$": All roots of x^p-x-a are $\alpha, \alpha+1, \dots, \alpha+p-1$

Let $\sigma:\alpha\mapsto\alpha+1\Rightarrow\sigma^i:\alpha\longmapsto\alpha+i$. Hence, $\mathrm{Gal}(L/K)=\langle\sigma\rangle$

"$\Rightarrow$": $\because \mathrm{Tr}_{L/K}(1)=p=0$

$\therefore \exists\alpha\in L$, s.t. $1=\sigma(a)-\alpha\Rightarrow\sigma(a)=\alpha+1$

On one hand, $\sigma^i(\alpha)=\alpha+i\Rightarrow\alpha, \alpha+1, \dots, \alpha+p-1$ are roots of $m_{a,K}$.

On the other hand, $\alpha, \alpha+1, \dots, \alpha+p-1$ are all roots of x^p-x-a, $a=\alpha^p-\alpha$

Similarly, $x^p-x-a\mid m_{a,K}\Rightarrow m_{a,K}=x^p-x-a\Rightarrow[K(\alpha):K]=p\Rightarrow L=K(\alpha)$. $\square$

GALOIS GROUP EXAMPLE

If $|G|=pq$, p,q are distinct primes: WLOG assume $p>q$. By Sylow thm, $n_p=1+p\mid q\Rightarrow n_p=1\Rightarrow\exists H\in Syl_p(G)$ s.t. $H\trianglelefteq G\Rightarrow|H|=p\Rightarrow H$ is solvable

As $|G/H|=q$, thus G/H is also solvable. $\therefore G$ is solvable.

Shun/翔海 (@shun4midx)

Case: $|G|=pqr$, primes $p>q>r$.
Assume none of $n_p, n_q, n_r = 1$.
Then, $n_p = 1+kp \mid qr \Rightarrow n_p = qr$
$n_q = 1+kq \mid pr \Rightarrow n_q \geq p$
$n_r = 1+kr \mid pq \Rightarrow n_r \geq q$
$\therefore \exists\, n_p = 1$ or $n_q = 1$ or $n_r = 1$
Then by similar logic as "$|G|=pq$", thus G is solvable

Case: $|G|=p^2q$
If $p>q$, we know similarly $n_p = 1$, so $|H| = p^2 \Rightarrow H$ is abelian $\Rightarrow H$ is solvable (solvable if normal or abelian)
If $p<q$, then assume $n_p \neq 1$ and $n_q \neq 1$.
Thus, $n_p = q$, $n_q = p^2 \Rightarrow p^2 = 1+kq \Rightarrow q \mid p^2-1 = (p-1)(p+1) \Rightarrow q = p+1 \Rightarrow p=2, q=3 \Rightarrow |G|=12$. However $|G|=12$ has a normal subgroup ~~$\times$~~

5-16-25 (WEEK 13)

Shun/舜海 (@shun4midx)

GALOIS RESULTANT

Given $f(x)$ separable in $K(x)$ and $\alpha_1, \dots, \alpha_n$ all roots of $f(x)$, let $L = K(\alpha_1, \dots, \alpha_n)$, how can we find $\mathrm{Gal}(L/K)$?

DEFINITION

Define $\theta = y_1\alpha_1 + \dots + y_n\alpha_n$

$\forall \sigma \in S_n$, $\sigma_y(\theta) = y_{\sigma(1)}\alpha_1 + \dots + y_{\sigma(n)}\alpha_n$, $\sigma_\alpha(\theta) = y_1\alpha_{\sigma(1)} + \dots + y_n\alpha_{\sigma(n)}$

Notice, $\sigma_y\sigma_\alpha(\theta) = \sigma_\alpha\sigma_y(\theta) = \theta \Rightarrow \sigma_\alpha(\theta) = \sigma_y^{-1}(\theta)$, $\sigma_y(\theta) = \sigma_\alpha^{-1}(\theta) = (\sigma^{-1})_\alpha(\theta)$

In $L(x, y_1, \dots, y_n)$, consider $F(x,y) = \prod_{\sigma\in S_n}(x - \sigma_y(\theta)) = \prod_{\sigma\in S_n}(x - (\sigma^{-1})_\alpha(\theta)) = \prod_{\sigma\in S_n}(x - \sigma_\alpha(\theta))$

EXAMPLE

$f(x) = x^3 - 3x + 1 \Rightarrow D = 81 \Rightarrow \sqrt{D} \in \mathbb{Q} \Rightarrow G(f) \cong A_3$ ($[\mathbb{Q}(\alpha):\mathbb{Q}] = 3 \mid |G(f)|$, $\sqrt{D} \in \mathbb{Q} \Rightarrow$ no intermediate field $\Rightarrow A_3$!)

($f(x) = x^3 + 3x + 1 \Rightarrow D = -135 \Rightarrow \sqrt{D} \notin \mathbb{Q} \Rightarrow G(f) \cong S_3$)

Consider $F(x,y) = (x - (y_1\alpha_1 + y_2\alpha_2 + y_3\alpha_3))(x - (y_1\alpha_2 + y_2\alpha_3 + y_3\alpha_1))(x - (y_1\alpha_3 + y_2\alpha_1 + y_3\alpha_2))(x - (y_1\alpha_2 + y_2\alpha_1 + y_3\alpha_3))(x - (y_1\alpha_1 + y_2\alpha_3 + y_3\alpha_2))$
$(x - (y_1\alpha_3 + y_2\alpha_2 + y_3\alpha_1)) \in \mathbb{Z}[x, y_1, y_2, y_3]$ (UFD)

FORMALIZATION

Each coefficient of F is a symmetric function of $\alpha_1, \dots, \alpha_n$, so it can be expressed in terms of the coef of $f(x)$, thus $F(x,y) \in K[x, y_1, \dots, y_n]$ (UFD)

We can decompose $F(x,y)$ into irr factors in $K(x, y_1, \dots, y_n)$: $F(x,y) = F_1(x,y)\cdots F_r(x,y)$

Note that $\forall \sigma \in S_n$, $F = \sigma_y F = (\sigma_y F_1)(\sigma_y F_2)\cdots(\sigma_y F_r)$ and F_i is irr $\Rightarrow \sigma_y F_i$ is irr (otherwise, $\sigma_y F_i = PQ \Rightarrow F_i = \sigma_y^{-1}P\,\sigma_y^{-1}Q$), so σ induces a permutation of $F_1, \dots, F_r$.

We may assume that $(x-\theta) \mid F_1$.

LEMMA

$Q = \{\sigma \in S_n \mid \sigma_y F_1 = F_1\} = \{\sigma \in S_n \mid x - \sigma_y(\theta) = \sigma_y(x-\theta) \mid F_1\}$

Proof

"$\subseteq$": $x - \theta \mid F_1 \Rightarrow \sigma_y(x-\theta) = x - \sigma_y$

"$\supseteq$": $\sigma_y(F_1) = F_i$ for some i and $x - \sigma_y(\theta) \mid F_i \Rightarrow F_1 = F_i$

PROPOSITION

$\mathrm{Gal}(L/K) = Q = \{\sigma \in S_n \mid \sigma_y F_1 = F_1\}$

Proof

"$\subseteq$": For $\sigma \in \mathrm{Gal}(L/K) \subseteq S_n$, we extend σ to an action,

$$\begin{aligned} \sigma^e : L(y_1, \dots, y_n) &\longrightarrow L(y_1, \dots, y_n) \\ y_i &\longmapsto y_i \\ \alpha \in L &\longmapsto \sigma(\alpha) \\ \theta &\longmapsto \sigma_\alpha(\theta) \end{aligned}$$

which fixes $K(y_1, \dots, y_n)$

Observe that $\sigma^e(\theta) = \sigma_\alpha(\theta)$ and θ share the same min poly over $K(y_1, \dots, y_n)$, and F_1 is irr in $K[y_1, \dots, y_n][x] \Rightarrow$ irr in $K(y_1, \dots, y_n)[x]$,

so $F_1 = m_{\theta, K(y_1,\dots,y_n)} = m_{\sigma(\theta), K(y_1,\dots,y_n)} \Rightarrow (x - \sigma_\alpha(\theta)) \mid F_1 \Rightarrow \sigma^{-1} \in Q$, i.e. $(\sigma^{-1})_y F_1 = F_1 \Rightarrow F_1 = \sigma_y F_1 \Rightarrow \sigma \in Q$ ✓

($\sigma_\alpha = (\sigma^{-1})_y$)

"$\supseteq$": $\forall \sigma \in Q$, i.e. $x - \sigma_y(\theta) \mid F_1$ ($\sigma_\alpha^{-1} = \sigma_y$), we have $F_1 = m_{\theta, K(y_1,\dots,y_n)}$

Hence, $\exists \tau \in \mathrm{Aut}(L(y_1,\dots,y_n)/K(y_1,\dots,y_n))$ s.t. $\tau(\theta) = \sigma_\alpha^{-1}(\theta)$

Here, we find that $\tau|_L \in \mathrm{Gal}(L/K)$ and $\tau|_L(\alpha_i) = \alpha_{\sigma^{-1}(i)} \Rightarrow \sigma^{-1} \in \mathrm{Gal}(L/K) \Rightarrow \sigma \in \mathrm{Gal}(L/K)$ (group) □

THEOREM

Shun/翔海 (@shun4midx)

Given $f(x)$ monic and separable in $\mathbb{Z}[x]$, assume that $p \nmid D := \prod_{i<j} (\alpha_i - \alpha_j)^2 \in \mathbb{Z}$. Then, the Galois group of $F(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$ is a subgroup of the Galois group of $f(x)$

Proof

By assumption, the discriminant of $\bar{f}(x)$ is $\bar{D} \pmod p \neq 0$, so $\bar{f}(x)$ is still separable

$\because D = (-1)^{\frac{n(n-1)}{2}} R(f, f')$

$\therefore \bar{D} = (-1)^{\frac{n(n-1)}{2}} R(\bar{f}, \bar{f}')$

As above, $F(x,y) = F_1(x,y) \cdots F_r(x,y)$ in $\mathbb{Z}[x, y_1, \cdots, y_n]$

Observe that if $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ has roots $\alpha_1, \cdots, \alpha_n$, then $\bar{f}(x) = x^n + \bar{a}_{n-1}x^{n-1} + \cdots + \bar{a}_0$ has roots $\beta_1, \cdots, \beta_n$ with $S_i(\beta_1, \cdots, \beta_n) = \overline{S_i(\alpha_1, \cdots, \alpha_n)}$ in $\mathbb{Z}/p\mathbb{Z}$

Also, $\theta_\rho = y_1\beta_1 + \cdots + y_n\beta_n$, $F_\rho(x,y) = \prod_{\sigma \in S_n} (x - \sigma_y(\theta_\rho)) = \bar{F}(x,y) = \bar{F}_1 \cdots \bar{F}_r$ in $\mathbb{Z}/p\mathbb{Z}[x, y_1, \cdots, y_n]$

$= (G_{1,1} \cdots G_{1,s_1})(G_{2,1} \cdots G_{2,s_2}) \cdots (G_{r,1} \cdots G_{r,s_r})$, G_{ij} : irr

Since the Galois group of $\bar{f} = \{\sigma \in S_n \mid \sigma_y G_{1,j} = G_{1,j}\}$ $\forall j$ and $G_{1,j} \mid \bar{F}_1$, Gal group of $f \subseteq \{\sigma \in S_n \mid \sigma_y \bar{F}_1 = \bar{F}_1\} = \{\sigma \in S_n \mid \sigma_y F_1 = F_1\}$ = Galois group of f □

KEY FACTS (STRATEGY TO EVALUATE GALOIS GROUPS)

- Every finite extension of $\mathbb{Z}/p\mathbb{Z}$ is cyclic
- If $f(x)$ is irr, then the Galois group of $f(x)$ is transitive on its roots
- If $\bar{f}(x)$ is in $\mathbb{Z}/p\mathbb{Z}[x]$ and its Galois group is $\langle \sigma \rangle \subseteq S_n$, then σ must be a cycle of length n

CONCLUSION

If $\bar{f}(x) = \bar{f}_1(x) \cdots \bar{f}_r(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$ with $\bar{f}_i$ irr of deg m_i, then the Galois group of $f(x)$ contains a permutation of the type $(\alpha_{1,1} \cdots \alpha_{1,m_1}) \cdots (\alpha_{r,1} \cdots \alpha_{r,m_r})$

EXAMPLE

1. $f(x) = x^5 - x - 1$ (If $\delta = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j) \in K$, then $\delta \in \mathrm{Fix} G \Rightarrow G \subseteq A_n$. $\therefore \delta \notin k \Rightarrow G \not\subseteq A_n$)
   - $D = 2869 = 19 \times 151 \Rightarrow \sqrt{D} \notin \mathbb{Q} \Rightarrow G(f) \not\subseteq A_5$
   - In $\mathbb{Z}/2\mathbb{Z}[x]$, $\bar{f}(x) = x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$ ← Got from factoring $x^{2^2} - x$, $x^{2^3} - x$
     $\Rightarrow (ab)(cde) \in G$, $(a\ b) = [(ab)(cde)]^3 \in G$
   - In $\mathbb{Z}/3\mathbb{Z}[x]$, $\bar{f}(x) = x^5 - x - 1$
     - No linear factor
     - No quadratic factor. If $\bar{f} = h \cdot g$, $\deg h = 2$, then $h(x) \mid x^{3^2} - x \Rightarrow h(x) \mid x^8 - 1$ or $h(x) \mid x^4 + 1$ ✗ ($x^5 - x \Rightarrow (x^5 - x - 1) - (x^5 - x) = -1 \Rightarrow h(x) \mid -1$ ✗; $x^5 + x \Rightarrow 2x + 1$ ✗)
     - $\therefore (a'\ b'\ c'\ d'\ e') \in G$

   $\therefore G \cong S_5$.

LEMMA

A transitive subgroup G of S_n containing a 2-cycle and $(n-1)$-cycle is S_n.

Proof

Say $(i\ j)$, $(1\ 2 \cdots (n-1)) \in G$ (σ)

$\because G$ is transitive

$\therefore \exists \sigma \in G$ s.t. $\sigma(j) = n$

Then, $\tau = \sigma(i\ j)\sigma^{-1} = (k\ n)$, where $\sigma(i) = k$, $1 \le i \le k-1$

Notice, $(1\ 2 \cdots n-1)(k\ n)(1\ 2 \cdots n-1)^{-1} = (k+1\ n) \in G \Rightarrow$ By induction, $(i\ n) \in G$ $\forall i$

$\therefore G = \langle (1\ n), (2\ n), \cdots, (n-1\ n) \rangle = S_n$ □

EXAMPLE

Shun / 翔海 (@shun4midx)

$f(x)=x^6+22x^5+21x^4+12x^3-37x^2-29x-15$

In $\mathbb{Z}/2\mathbb{Z}[x]$, $\bar{f}(x)=x^6+x^4+x^2+x+1$ is irr $\Rightarrow$ $G(f)$ is transitive

In $\mathbb{Z}/3\mathbb{Z}[x]$, $\bar{f}(x)=x^6+x^5-x^2+x=x(x^5+x^4-x+1)$ is irr $\Rightarrow$ $(1\ 2\ 3\ 4\ 5) \in G(f)$ (deg 5)

In $\mathbb{Z}/5\mathbb{Z}[x]$, $\bar{f}(x)=x^6+2x^5+x^4+2x^3-2x^2+x=x(x-1)(x+1)(x+2)(x^2+2) \Rightarrow (a\ b) \in G(f)$

$\therefore$ By lemma, $G(f)\cong S_6$

5-21-25 (WEEK 14)

Shun / 舜海 (@shun4midx)

COMPUTATIONS

Let $G \leq S_n$

- If G contains an n-cycle, then G is transitive
- If G is transitive, then H may NOT contain an n-cycle (e.g. $V_4 \leq S_4$)
- When $n=p$: a prime, if G is transitive, then G must contain a p-cycle
  - ↳ Let $G \curvearrowright \{1, \dots, p\}$, then $p = |\text{orb}(1)| = \frac{|G|}{|\text{Stab}_G(1)|} \Rightarrow p \mid |G|$
  - ∴ By Cauchy thm, $\exists \sigma \in G$, s.t. $\text{ord}(\sigma) = p \Rightarrow \sigma$ is a p-cycle

Notice, all subgroups of S_5 have order 5, 10, 20, 60, 120.

The transitive subgroups of S_5:

- $\langle (1\ 2\ 3\ 4\ 5) \rangle \cong C_5$ (rotation) } solvable
- $\langle (1\ 2\ 3\ 4\ 5), (2\ 5)(3\ 4) \rangle \cong D_{10}$ (reflection) } solvable
- $\langle (1\ 2\ 3\ 4\ 5), (1\ 2\ 3) \rangle \cong A_5 = \langle (1\ 2\ 3), (1\ 2\ 4), (1\ 2\ 5) \rangle$
- $\langle (1\ 2\ 3\ 4\ 5), (1\ 2) \rangle \cong S_5$
- $\langle (1\ 2\ \overset{a}{3}\ 4\ 5), (1\ 2\ \overset{b}{3}\ 4) \rangle \cong C_5 \rtimes C_4 = \langle a, b \mid a^5=1, b^4=1, bab^{-1}=a^2 \rangle$ ← order $20 = 2^2(5) \Rightarrow$ solvable ✓ (≅: F)

EXAMPLE

Notice, $[\mathbb{Q}(\zeta_{11}) : \mathbb{Q}] = 10$ ($\because x^{10}+x^9+\dots+x^2+x+1=0$)

Say $\alpha = \zeta_{11} + \zeta_{11}^{-1}$, notice the original equation becomes $x^5+x^{-5}+x^4+x^{-4}+x^3+x^{-3}+x^2+x^{-2}+x+x^{-1}+1=0$

↳ $(x+x^{-1})^2 = x^2+x^{-2}+2 \Rightarrow x^2+x^{-2} = (x+x^{-1})^2-2$

↳ $(x+x^{-1})^3 = x^3+3x+3x^{-1}+x^{-3} = x^3+x^{-3}+3(x+x^{-1}) \Rightarrow x^3+x^{-3} = (x+x^{-1})^3-3(x+x^{-1})$

↳ $(x+x^{-1})^4 = x^4+x^{-4}+4(x^2+x^{-2})+6 \Rightarrow x^4+x^{-4} = (x+x^{-1})^4-4(x+x^{-1})^2-2$

↳ $(x+x^{-1})^5 = x^5+x^{-5}+5(x^3+x^{-3})+10(x+x^{-1}) \Rightarrow x^5+x^{-5} = (x+x^{-1})^5-5(x+x^{-1})^3-5(x+x^{-1})$

∴ Original equation: $(x+x^{-1})^5+(x+x^{-1})^4-4(x+x^{-1})^3-3(x+x^{-1})^2+3(x+x^{-1})+1=0$

As $x^5+x^4-4x^3-3x^2+3x+1$ is irr, thus $x^{10}+x^9+\dots+x+1=0$ corr to C_5 (We can use this method to construct any cyclic Galois group)

S_5: x^5-4x+2 (3 real roots, 2 complex roots)

F: $x^5-2 \rightsquigarrow L = \mathbb{Q}(\sqrt[5]{2}, \zeta_5) \Rightarrow$ roots: $\sqrt[5]{2}, \sqrt[5]{2}\zeta_5, \dots, \sqrt[5]{2}\zeta_5^4$

∴ $\sqrt[5]{2} \longmapsto$ 5 choices

$\zeta_5 \longmapsto \zeta_5^i$, $i = 1, 2, \dots, 4$

∴ $\text{Gal}(L/\mathbb{Q}) = F$

A_5: $x^5+20x+16 \Rightarrow D = 2^{16}5^6 \Rightarrow \sqrt{D} \in \mathbb{Q} \Rightarrow \text{Gal}(f) \leq A_5 \Rightarrow \text{Gal}(f) = A_5$

D_{10}: $x^5-5x+12$

HILBERT'S THEOREM

$\forall n \in \mathbb{N}$, $\exists$ infinitely many $f(x)$ of deg n in $\mathbb{Z}[x]$, s.t. $\text{Gal}_{\mathbb{Q}}(f) \cong S_n$

RECALL

A transitive subgroup of S_n containing a 2-cycle and an $(n-1)$-cycle is S_n

Shun/舜海 (@shun4midx)

PROOF OF THEOREM

We choose some monic poly as follows:

- $f_1(x)$ in $\mathbb{Z}[x]$ s.t. $\deg f_1 = n$ and $\bar{f}_1(x)$ is irr in $\mathbb{Z}/2\mathbb{Z}[x]$ (in $x^{2^n}-x$)
- Let $g(x)$ be irr in $\mathbb{Z}/3\mathbb{Z}[x]$ of deg $n-1$ (in $x^{3^{n-1}}-x$) and $f_2(x)$ of deg n s.t. $\bar{f}_2(x) = xg(x)$ in $\mathbb{Z}/3\mathbb{Z}[x]$
- Let $h(x)$ be irr in $\mathbb{Z}/5\mathbb{Z}[x]$ of deg 2 (in $x^{5^2}-x$)

If n is odd, let $p(x)$ be irr in $\mathbb{Z}/5\mathbb{Z}[x]$ of deg $n-2$ (in $x^{5^{n-2}}-x$) and choose $f_3(x)$ of deg n s.t. $\bar{f}_3(x) = h(x)p(x)$ in $\mathbb{Z}/5\mathbb{Z}[x]$ (will have a 2-cycle since $[(a\,b)(c_1\cdots c_{n-2})]^{n-2} = (a\,b)$)

If n is even, let $p_1(x)$ and $p_2(x)$ be irr in $\mathbb{Z}/5\mathbb{Z}[x]$ of deg 1 and $n-3$ respectively and choose $f_3(x)$ of deg n, s.t. $\bar{f}_3(x) = h(x)p_1(x)p_2(x)$ ($(a\,b)(c_1\cdots c_{n-3})]^{n-3} = (a\,b)$)

Now, let $f(x) = -15f_1(x) + 10f_2(x) + 6f_3(x)$ which is monic and $G = \mathrm{Gal}(f)$

$\Rightarrow \bar{f}(x) = \bar{f}_1(x)$ in $\mathbb{Z}/2\mathbb{Z}$, $\bar{f}(x) = \bar{f}_2(x)$ in $\mathbb{Z}/3\mathbb{Z}$, $\bar{f} = \bar{f}_3(x)$ in $\mathbb{Z}/5\mathbb{Z}$

$\therefore G = S_n$

Notice, there are infinitely many $f(x)$ s.t. $\bar{f}(x) = \bar{f}_1(x)$ in $\mathbb{Z}/2\mathbb{Z}[x]$ (e.g. $f_1(x) = x^3+x+1 \Rightarrow x^3+(2k+1)x+1$ $\forall k \in \mathbb{Z}$)

WHAT IS F?

- Say $G \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$
  Let $G = G_0 \cong \langle 0\rangle \times G_1 \cong \langle 0\rangle \times \langle 0\rangle \times G_2 \cdots$
  $\therefore$ All abelian G are solvable
- G is solvable $\Leftrightarrow \exists\, 1 = H_0 \lhd H_1 \lhd \cdots \lhd H_s = G$, H_{i+1}/H_i is abelian

DERIVED SERIES: $G^{(0)} = G$, $G^{(1)} = [G,G]$, $G^{(2)} = [G^{(1)}, G^{(1)}]$, ...

G is solvable $\Leftrightarrow \exists n$, s.t. $G^{(n)} = 1$ for some $n \geq 1$

Proof

"$\Leftarrow$": $G^{(0)} = G \rhd G^{(1)} \rhd \cdots \rhd G^{(n)} = 1$

"$\Rightarrow$": $\exists\, 1 = H_0 \lhd H_1 \lhd \cdots \lhd H_s = G$, where H_{i+1}/H_i : abelian

Claim: $G^{(i)} \leq H_{s-i}$

Proof

By induction on i,

- $i=0$: $G^{(0)} = G = H_s$
- $G^{(i+1)} = [G^{(i)}, G^{(i)}] \leq [H_{s-i}, H_{s-i}] \leq H_{s-i-1}$ ($\because H_{s-i}/H_{s-i-1}$: abelian)
- $H_0 = 1 \Rightarrow G^{(s)} = 1$ ✓

GOAL

Let G be a transitive (contains a p-cycle) solvable subgroup of S_p.

The derived series: $1 = G^{(n)} \lhd G^{(n-1)} \lhd \cdots \lhd G^{(1)} \lhd G_0 = G$ (abelian; $\rhd \langle (1\cdots n)\rangle \lhd$)

We have $G^{(n-1)} \lhd G$

Claim: $p \mid |G^{(n-1)}|$ (abelian)

Proof

Let $H = \mathrm{Stab}_G(1)$

- $p = |\mathrm{orb}(1)| = \frac{|G|}{|H|} \Rightarrow H$ is max in G
- $H \cap G^{(n-1)} \lhd G$:
  - $G^{(n-1)} \leq H \Rightarrow G^{(n-1)} \cap H = G^{(n-1)} \lhd G$
  - $G^{(n-1)} \not\subseteq H \Rightarrow \because H$ is max $\therefore HG^{(n-1)} = G$

$\forall x \in H \cap G^{(n-1)}$, $g = ha \in G \Rightarrow gxg^{-1} = h(axa^{-1})h^{-1} = hxh^{-1} \in H \cap G^{(n-1)}$ ($a \in G^{(n-1)}$)

- H has no nontrivial subgroup in G
- $\therefore H \cap G^{(n-1)} = \{1\} \Rightarrow HG^{(n-1)} = G \Rightarrow \sigma = (1\ldots p) \in G^{(n-1)}$

Shun/翔海 (@shun4midx)

Assume that $\langle e\rangle = G^{(n)} \lhd \langle (1\ 2\cdots p)\rangle = G^{(n-1)} \lhd G^{(n-2)} \lhd \cdots \lhd G^{(1)} \lhd G^{(0)} = G$ ($\langle\sigma\rangle$)

Consider $\sigma: \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $i \mapsto i+1$, an affine transformation of $\mathbb{Z}/p\mathbb{Z}$ $\tau_{(a,b)}(k) = ak+b \in S_p$ (order $p(p-1)$), $a \neq 0$

$\{0,\dots,p-1\} \mapsto \{0,\dots,p-1\}$

$\therefore \{\tau_{(a,b)} \mid a \in (\mathbb{Z}/p\mathbb{Z})^\times,\ b \in \mathbb{Z}/p\mathbb{Z}\},\ \circ\}$ forms a subgroup F of S_p of order $p(p-1)$

THEOREM

$G \leq F$

Proof

- $G^{(n-1)} \leq F \Rightarrow G_{j-1} \leq F$
- Suppose $G_j \leq F$ and $\tau \in G_{j-1}$. Then, $\tau\sigma\tau^{-1} = \tau_{(a,b)} \in G_j$ (since σ is a p-cycle, thus $\tau\sigma\tau^{-1}$ is a p-cycle, so it doesn't fix x, i.e. no sol)

  Thus, $\tau\sigma\tau^{-1}(x) = ax+b = x$ has no solution in $\mathbb{Z}/p\mathbb{Z} \Rightarrow a=1,\ b\neq 0 \Rightarrow \tau\sigma\tau^{-1} \in G^{(n-1)} \setminus \{id\}$

  So, $\tau(k+1) = \tau\sigma(k) = \tau\sigma\tau^{-1}\tau(k) = \tau(k)+b \Rightarrow \tau \in F$

  ↳ $\tau(k+1) = \tau(k)+b,\ \tau(k) = \tau(k-1)+b, \dots \Rightarrow \tau(k+1) = \tau(0)+b(k+1)$

5-23-25 (WEEK 14)

Shun / 舜海 (@shun4midx)

INFINITE GALOIS GROUPS (Welcome to Shun's insanity :D)

PROPOSITION 1

Let L/K be algebraic. TFAE:

(A) L/K is normal

(B) L is a splitting field of some set S (possibly infinite)

(C) $\forall \sigma: L \hookrightarrow \bar{K}$ which fixes K induces an automorphism of L

Proof

"(A)⇒(B)": $S = \{m_{\alpha,K} \mid \alpha \in L\}$

On one hand, $\because m_{\alpha,K}$ splits over L $\therefore$ All roots of $m_{\alpha,K}$ lie in L

On the other hand, if $K \subseteq L' \subsetneq L$, then $\forall \alpha \in L \setminus L'$, $m_{\alpha,K}$ can't split over L' (at least, $\alpha \notin L'$)

$\therefore L$ is the smallest among field/K which contains all roots of $f \in S$

"(B)⇒(A)": Let $A = \{\alpha \in L \mid f(\alpha) = 0 \text{ for some } f \in S\}$. Then, $L = K(A)$

$\forall \beta \in L$, say $\beta \in K(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in A$.

If L' is a splitting field of $f(x) = m_{\alpha_1,K} \cdots m_{\alpha_n,K}$ over K, then $m_{\beta,K}$ also splits over L'. Here, $\forall i$, $m_{\alpha_i,K} \mid f_i$ for some $f_i \in S$

Certainly, $L' \subseteq L$

"(A)⇒(C)": $\forall \alpha \in L$, $\sigma(\alpha)$ is also a root of $m_{\alpha,K}$, so $\sigma(\alpha) \in L$

Hence, $\sigma: L \hookrightarrow$ "L" fixes K & "L/K is algebraic" ⇒ σ is onto, so $\sigma(L) = L$

"(C)⇒(A)": For $\alpha \in L$, β is a root of $m_{\alpha,K}$. Then $\exists \tau: K(\alpha) \to K(\beta) \hookrightarrow \bar{K}$, $\tau \neq 0$, $\alpha \mapsto \beta$

We know τ can be extended to $\sigma: L \hookrightarrow \bar{K}$. By assumption, $\sigma(L) = L$ and $\beta = \tau(\alpha) = \sigma(\alpha) \in L$ □

THE FUNDAMENTAL THEOREM OF GALOIS THEORY DOES NOT HOLD FOR INFINITE ALGEBRAIC EXTENSIONS

EXAMPLE

Let $A = \{\sqrt{p} \mid p: \text{prime}\}$ and $L = \mathbb{Q}(A)$

- $L/\mathbb{Q}$ is normal: L is a splitting field of $\{x^2 - p \mid p: \text{prime}\}$
- $L/\mathbb{Q}$ is separable: $\because \operatorname{char} \mathbb{Q} = 0$
- $\mathrm{Gal}(L/\mathbb{Q})$ has uncountably many groups of index 2 (There are only countably many quadratic field extensions $\mathbb{Q}(\sqrt{q})$, q: square free of $\mathbb{Q}$ in L)

  ↳ $\forall \sigma \in \mathrm{Gal}(L/\mathbb{Q})$, $\sigma: \sqrt{p} \mapsto \sqrt{p}$ or $-\sqrt{p}$, $\sigma^2 = \mathrm{id}$, so $\mathrm{Gal}(L/\mathbb{Q})$ is abelian

  $\cong \prod \mathbb{Z}/2\mathbb{Z}$ can be seen as a $\mathbb{Z}/2\mathbb{Z}$ vector space V

  We know $V^* = \{\phi: V \to \mathbb{Z}/2\mathbb{Z} \mid \phi \text{ is a } \mathbb{Z}/2\mathbb{Z}\text{-linear transformation}\} \leftrightarrow \ker\phi \leq V$ is uncountable

  $\therefore$ $\{\ker\phi \mid \phi \in V^*\}$ (index 2) is uncountable

GOAL

Consider a Galois extension L/K,

$\mathcal{F} = \{E \mid L \supseteq E \supseteq K\} \longrightarrow \mathcal{G} = \{H \mid H \leq \mathrm{Gal}(L/K)\}$

$E \longmapsto \mathrm{Gal}(L/E)$

$L^H \longleftarrow H$

FACT 1

$E \mapsto \mathrm{Gal}(L/E) \to E = L^{\mathrm{Gal}(L/E)}$

Proof

For $\alpha \in L \setminus E$, let E_1 be a splitting field of $m_{\alpha,E}$.

Then, we have E_1/E: finite Galois ⇒ $E_1^{\mathrm{Gal}(E_1/E)} = E \Rightarrow \exists \tau \in \mathrm{Gal}(E_1/E)$, $\alpha \notin E$, $\tau(\alpha) \neq \alpha$

Extend, then we have $\sigma \in \mathrm{Gal}(L/E)$, $\sigma(\alpha) \neq \alpha$

FACT 2

Let L/K be Galois and $G = \mathrm{Gal}(L/K)$

If E/K is Galois and $H = \mathrm{Gal}(L/E)$, then $\mathrm{Gal}(E/K) \cong G/H$

Shun/翔海 (@shun4midx)

Proof

Define $\varphi: G \twoheadrightarrow \mathrm{Gal}(E/k)$

$\sigma \longmapsto \sigma|_E$ ← well-defined since E/k is normal

It is onto due to the important extension property

By extension, $\ker\varphi = H \Rightarrow G/H \cong \mathrm{Gal}(E/k)$ □

GOAL

To find a good formulation for $\mathrm{Gal}(L/k) = G$

STRATEGY

$\{k \subseteq E_i \subseteq L \mid E_i/k : \text{finite Galois}\} = \{E_i \mid i \in I\}$

$\forall i$, $H_i := \mathrm{Gal}(L/E_i) \trianglelefteq G$, $G_i := G/H_i \cong \mathrm{Gal}(E_i/k)$ ← $|G_i| < \infty$ ⇝ $\{G_i \mid i \in I\}$ (finite)

- $i \le j \Leftrightarrow E_i \subseteq E_j \Leftrightarrow H_i \supseteq H_j$, $\varphi_{ji}: G_j = G/H_j \longrightarrow G_i := G/H_i$ (big → small)

$\sigma \in \mathrm{Gal}(E_j/k)$ (i.e. $\bar\sigma$) $\longmapsto \bar\sigma \in \mathrm{Gal}(E_i/k) \ni \sigma|_{E_i}$

MAIN THEOREM

Let L/k be Galois. Then, $\mathrm{Gal}(L/k) \cong \varprojlim G_i$ (inverse limit)

Proof

$\forall i$, $\mathrm{Gal}(L/k) \xrightarrow{\rho_i} \mathrm{Gal}(E_i/k) \cong G_i$

$\sigma \longmapsto \sigma|_{E_i}$

$E_i \subseteq E_j$, φ_{ji}, ρ_{id}

$\mathrm{Gal}(E_j/k) \cong G_j$

$\sigma|_{E_j}$

By the universal property of $\varprojlim G_i$, $\exists!\, f: \mathrm{Gal}(L/k) \longrightarrow \varprojlim G_i$, s.t. $\varphi_i \circ f = \rho_i$

$\sigma \longmapsto (\sigma|_{E_i})_{i \in I}$

- f is 1-1: $\sigma \in \ker f \Leftrightarrow \sigma|_{E_i} = \mathrm{id}_{E_i}\ \forall i \in I \Leftrightarrow \sigma = \mathrm{id}_L$

  Claim: $\forall \alpha \in L$, $\exists i \in I$, s.t. $\alpha \in E_i$

  ($\Uparrow$ $k(\beta_1, \dots, \beta_n) = E_i$)
- f is onto: For $(\sigma_i)_{i \in I} \in \varprojlim G_i$, define $\sigma: L \longrightarrow L$

  $E_i \ni \alpha \longmapsto \sigma_i(\alpha)$

  ↳ Well-defined: If $\alpha \in E_j$ too, then $\alpha \in E_i \cap E_j = E_t$, $\sigma_i(\alpha) = \sigma_i|_{E_t}(\alpha) = \sigma_t(\alpha) = \sigma_j|_{E_t}(\alpha) = \sigma_j(\alpha)$ ✓ (σ_t is hom)

  ↳ Homo: $\alpha, \beta \in L$, say $\alpha \in E_i$, $\beta \in E_j$, then, $\alpha, \beta \in E_i E_j = E_k$, so $\sigma(\alpha\beta) = \sigma_k(\alpha\beta) = \sigma_k(\alpha)\sigma_k(\beta) = \sigma(\alpha)\sigma(\beta)$ (σ_k is hom)

  ↳ 1-1: If $\sigma(\alpha) = 0$, $\alpha \in E_i$, then $\sigma_i(\alpha) = 0 \Rightarrow \alpha = 0$ (σ_i is autom)

  ↳ onto: $\forall \beta \in L$, say $\beta \in E_i$ and $\sigma_i(\alpha) = \beta \Rightarrow \sigma(\alpha) = \beta$ ✓

p-ADIC INTEGERS (Yes, I've gone insane stfu this is typical Shun <2 weeks before finals)

$I = \mathbb{N}$, for $i \le j$, $\varphi_{ji}: \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z} \rightsquigarrow \mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \mathbb{Z}/p^3\mathbb{Z} \leftarrow \dots$

$\bar a \longmapsto \bar a$ $\qquad a_0 + p\mathbb{Z} \longleftarrow a_0 + a_1 p + a_2 p^2 + p^3\mathbb{Z}$

$\therefore \varprojlim \mathbb{Z}/p^i\mathbb{Z} = \{a_0 + a_1 p + a_2 p^2 + \dots + a_i p^i \mid 0 \le a_i \le p-1\} =: \mathbb{Z}_p$ (that's why we shouldn't write $\mathbb{Z}/p\mathbb{Z}$ as $\mathbb{Z}_p$ lol... $\mathbb{F}_p$ is better)

LIMITS IN ALGEBRA (From here on, everything goes downhill, pls don't reference this, I'm 99% sure it's wrong)

Consider a sequence of objects $\dots \to X_n \to X_{n-1} \to \dots \to X_1$ in $\mathcal{C}$, we want to consider a "X_∞"

but I don't wanna erase this lol so enjoy my insanity :)

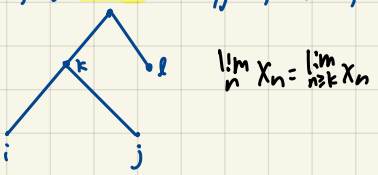
General: 1. A directed set I

2. $\{X_i\}_{i \in I}$ objects in a category

Shun / 舜海 (@shun4midx)

DEFINITION (POSET)

$(I, \leq)$ is directed if $\forall i, j \in I, \exists k \in I, k \geq j, k \geq i$

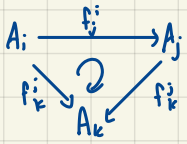


$\varprojlim_n x_n = \varprojlim_{n \geq k} x_n$

DEFINITION (FAMILIES)

$\mathcal{C}$: A category, I: A directed set $(\mathbb{N}, \geq)$

Then, $A = \{A_i \in \mathcal{C}\}_{i \in I}$ is directed if $\forall i \leq j$ in I, $i \leq j \leq k$, we have the universal property



Note: "inversely directed": $\rightarrow \Rightarrow \leftarrow$

LIMIT BY UNIVERSAL PROPERTY (ACTUALLY JUST UNION/INTERSECTION)

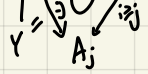
"$\bigcap A_i$": $\rightarrow \dots \rightarrow A_k \rightarrow A_{i-1} \rightarrow \dots \rightarrow A_1$

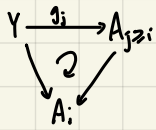
$B_1 \dots \rightarrow B_{i-1} \rightarrow B_i \rightarrow \dots \rightarrow$ "$\bigcup B_i$"

DEFINITION (UNIVERSAL PROPERTY)

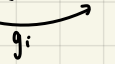
A is inversely directed if

- $\varprojlim A \in \mathcal{C}$
- $\varprojlim A \rightarrow A_i$





$\forall C \in Y \Rightarrow \exists! \varprojlim A \rightarrow A_i$



Directed: $Y \leftarrow A_{i \geq j}$, $Y \leftarrow \varprojlim A$

EXAMPLE

Let $I = \mathbb{N}$, $A_n := \mathbb{Z}/p^n\mathbb{Z}$

Inversely directed: $\mathbb{Z}/p^{n+1}\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$, $\bar{z} \longmapsto \bar{z}$

$\Rightarrow$ limit $= \{a_0 + pa_1 + p^2a_2 + \dots \mid 0 \leq a_i \leq p-1\} = \mathbb{Z}_p$

Directed: $\mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^{n+1}\mathbb{Z}$, $\bar{z} \longmapsto \overline{pz}$

$\frac{1}{p^n}\mathbb{Z}/\mathbb{Z} \longrightarrow \frac{1}{p^{n+1}}\mathbb{Z}/\mathbb{Z} \Rightarrow \varinjlim A = \bigcup_{n \in \mathbb{N}} \frac{1}{p^n}\mathbb{Z}/\mathbb{Z} \hookrightarrow \mathbb{Q}/\mathbb{Z}$

THEOREM (EXISTENCE)

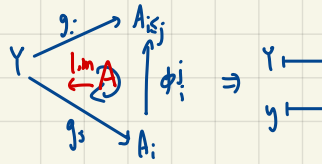
Inverse limit exists uniquely in Mr, groups, rings

Proof

Let A be an inversely directed family

A has $\begin{cases} I: \text{direct set} \\ A_i \in \mathcal{C},\ i \in I \\ i \leq j,\ A_j \xrightarrow{\phi_i^j} A_i \end{cases}$

$\phi_j^k \circ \phi_i^j = \phi_i^k$



$\Rightarrow$ $Y \longmapsto \prod_{i \in I} A_i = \{I \xrightarrow{\pi} \bigcup_{i \in I} A_i \mid \pi(i) \in A_i\}$

$y \longmapsto (g_i(y))_i$

Shun / 翔海 (@shun4midx)

Define $\varprojlim A = \{(a_i) \in \prod_i A_i \mid a_i = \phi_j^i(a_j)\ \forall j \le i\}$

$\uparrow$ Y, $\downarrow$ A_i

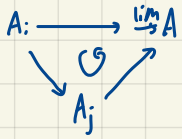
$\Rightarrow$ Satisfies universal property ✓

In other words, we can think of "inverse limit" as "consists of compatible tuples (a_i)"

DIRECT LIMIT

$A = \{A_i\}$: direct family, then we define the following: (✓ can prove it is an equivalence relation)

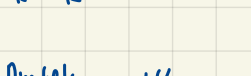
$\varinjlim A = \bigsqcup A_i / a_i \sim f_j^i(a_j)$



We define $[a_i] + [a_j] = [f_k^i a_i + f_k^j a_j]$ if $k \ge i, j$

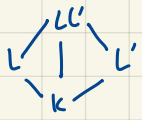
EXAMPLE

K: field, $I = \{K \subset L$: finite Galois extension$\}$



wtf is this

Directed:



$\mathrm{Gal}(L'/K) \longrightarrow \mathrm{Gal}(L/K)$

$\sigma \longmapsto \sigma|_L$ (finite)

$\Rightarrow \mathrm{Gal}(K^{sep}/K) = \varprojlim \mathrm{Gal}(L/K)$

EXAMPLE

$P \in \mathrm{Spec}\, A \Rightarrow A_P = \varinjlim_{f \notin P} A_f$ idk don't ask me why

EXAMPLE

$\mathbb{Z}_{10} = \cdots 99999 = -1$ ($\because \cdots 99999 + 1 = 0$)

5-28-25 (WEEK 15)

Shun / 舜海 (@shun4midx)

FUNDAMENTAL THEOREM FOR INFINITE CASE (Final Algebra Note by Shun :))

L/k: Galois, $G = Gal(L/k)$, $\{E_i \mid i \in I\} = \{K \subseteq E \subseteq L \mid E/k : \text{finite Galois}\}$

$H_i = Gal(L/E_i)$, $G_i = Gal(E_i/k) \cong G/H_i$: finite group $\Rightarrow$ Result: $G \cong \varprojlim G_i$ ($i \le j \Leftrightarrow E_i \subseteq E_j$, $\varphi_{ji} : G_j \to G_i$)

THE NATURAL TOPOLOGY

- G_i : finite $\Rightarrow$ discrete topology (discrete points that are open and closed)
  - ↳ $\prod_i G_i$: the product topology

$\prod_i G_i \supseteq p_i^{-1}(g_i)$: open basis

p_i (proj) ↓ ↑

$G_i \ni g_i$

So, $\widetilde{\varphi_i^{-1}(g_i)} \in \varprojlim G_i \subseteq \prod_i G_i$ (「open basis」)

φ_i ↘ ↙ p_i

$g_i \in G_i$

DEFINITION (ぶりは全然分かない...)

G is called a **topological group** if G is both a topological space and group s.t. $G \times G \xrightarrow{m} G$, $(x, y) \mapsto xy$ and $G \xrightarrow{i} G$, $g \mapsto g^{-1}$ are continuous

CLAIM

$\varprojlim G_i$ is a topological group

Proof

- m is cont.:

$$\begin{array}{ccc} \varprojlim G_i \times \varprojlim G_i & \xrightarrow{m} & \varprojlim G_i \supseteq \varphi_i^{-1}(g_i) \\ \downarrow \varphi_i \quad \downarrow \varphi_i & & \downarrow \varphi_i \\ G_i \times G_i & \longrightarrow & G_i \ni g_i \\ \downarrow \quad \downarrow & & \\ g_i h_i^{-1} & & \\ \text{「deduced」} & & \end{array}$$

$\therefore m^{-1}(\varphi_i^{-1}(g_i)) = \bigcup_{h \in G_i} \varphi_i^{-1}(g_i h^{-1}) \times \varphi_i^{-1}(h)$ is open in the product space $\varprojlim G_i \times \varprojlim G_i$

- i is cont.:

$$\begin{array}{ccc} \varprojlim G_i & \xrightarrow{i} & \varprojlim G_i \\ \downarrow \varphi_i & & \downarrow \varphi_i \\ g_i^{-1} \in G_i & \longrightarrow & G_i \ni g_i \end{array}$$

$\therefore i^{-1}(\varphi_i^{-1}(g_i)) = \varphi_i^{-1}(g_i)$ is open

OBSERVE

As G_i has autom, we write σ_i here for its elems, where $G \xrightarrow{f} \varprojlim G_i$ (「want to be open」 「open」)

$f^{-1}(\varphi_i^{-1}(\sigma_i)) = \{\sigma \in G \mid \sigma|_{E_i} = \sigma_i\} = \bigcup_{\sigma|_E = \sigma} \sigma\, Gal(L/E_i) \rightsquigarrow \sigma H_i$: open set

($\varprojlim G_i$ ∩ ; $Gal(L/E_i) = H_i$)

DEFINITION

Krull topology on G is the topology with basis consisting of all left cosets σH_i, $\sigma \in G$, $i \in I$

Shun / 舜海 (@shun4midx)

CHECK IT IS A TOPOLOGY

ok since infinite

- $\emptyset$ is open: For some $H_i \neq G$, take $\sigma_1 H_i \neq \sigma_2 H_i \Rightarrow \sigma_1 H_i \cap \sigma_2 H_i = \emptyset$
- G is open: $G = \mathrm{Gal}(L/k)$, $[k:k]=1$ is open
- An arbitrary union sets is open
- $\sigma_i H_i \cap \sigma_j H_j$ is open $\Rightarrow \sigma H_i = \sigma_i H_i$, $\sigma H_j = \sigma_j H_j \Rightarrow \sigma_i H_i \cap \sigma_j H_j = \sigma(H_i \cap H_j)$, $H_i \cap H_j = \mathrm{Gal}(L/E_i E_j)$
  ($\neq \emptyset$, $\exists \sigma$)

PROPOSITION

G is a topological group with the Krull topology

- f is cont.
- f^{-1} is cont.: $f(\sigma H_i) = \{((\sigma\tau_i)|_{E_j})_{j\in I} \mid \tau_i \in H_i\} = \{(\sigma|_{E_j} w_j) \mid w_j|_{E_j} = \mathrm{id}_{E_i \cap E_j}\} = \{(v_j)_{j\in I} \mid (\sigma|_{E_j})^{-1} v_j|_{E_i} = \mathrm{id}_{E_i\cap E_j}\} = \{(v_j)_{j\in I} \mid v_j|_{E_i} = \sigma|_{E_i\cap E_j}\} = \varphi_i^{-1}(\sigma|_{E_i})$

  (v_j, $G_j = \mathrm{Gal}(E_j/k)$)

  $\tau_i \in \mathrm{Gal}(L/k_i)$

  $\downarrow$

  $\tau_i|_{E_j} \in \mathrm{Gal}(E_j/E_i \cap E_j)$

  $\hookrightarrow$

  $w_j \in \mathrm{Gal}(E_j/k)$ □

FUNDAMENTAL THEOREM

$\mathcal{F} = \{E \mid k \subseteq E \subseteq L\} \leftrightarrow \mathcal{G}_0 = \{H \mid H: \text{closed subgroup of } G\}$

KEY LEMMA

If $H \leq G$, $E = L^H$ and $H \leq H' = \mathrm{Gal}(L/E)$, then $H' = \bar{H}$ is the closure of H in the Krull topology on G

(if H is closed, $H' = \bar{H} = H$)

Proof

($H' \supseteq \bar{H}$)

- H' is closed, i.e. $G \setminus H'$ is open: For $\sigma \in G \setminus H'$, by def, $\exists \alpha \in E$, s.t. $\sigma(\alpha) \neq \alpha$
  We can choose E_i, $i \in I$, s.t. $\alpha \in E_i$. Now, $\forall \tau \in H_i := \mathrm{Gal}(L/E_i) \Rightarrow \sigma\tau(\alpha) = \sigma(\alpha) \neq \alpha \Rightarrow \sigma\tau \in G \setminus H'$ (fix E_i)
  $\therefore \sigma H_i \subseteq G \setminus H'$ and σH_i can be regarded as an open neighborhood of σ, so $G \setminus H'$ is open.
- $H' \subseteq \bar{H}$: "$\forall \sigma \in H' \setminus H$, $\forall i \in I$, $(\sigma H_i \setminus \{\sigma\}) \cap H \neq \emptyset$"
  Fix $i \in I$. Let $N = \{\rho|_{E_i} \mid \rho \in H\} \leq \mathrm{Gal}(E_i/k)$ (finite)
  Note that E_i/k is finite Galois, so the fundamental thm holds for $\mathrm{Gal}(E_i/k)$
  $\therefore$ We have $N = \mathrm{Gal}(E_i/E_i^N) = \mathrm{Gal}(E_i/E_i \cap E) = \{\rho|_{E_i} \mid \rho \in H\}$, say $\sigma|_{E_i} = \rho|_{E_i}$ for some $\rho \in H$.
  $\Rightarrow \sigma^{-1}\rho|_{E_i} = \mathrm{Id}_{E_i} \Rightarrow \sigma^{-1}\rho \in \mathrm{Gal}(L/E_i) = H_i \Rightarrow \rho \in \sigma H_i \cap H \Rightarrow \rho \in (\sigma H_i \setminus \{\sigma\}) H$ □

FUNDAMENTAL THEOREM

(1) $\mathrm{Gal}(L/E) = H$ is closed: We have known $E = L^H$, so $\mathrm{Gal}(L/E) = H = \bar{H} \Rightarrow H$ is closed ✓

(2) H: closed $\longrightarrow L^H \longrightarrow \mathrm{Gal}(L/L^H) = \bar{H} = H$

$\therefore$ We proved the 1-1 corr of $\mathcal{F}$ and $\mathcal{G}_0$

NOTE

$\forall i \in I$, H_i is open and closed (by def)

($\because [G:H_i] = n_i$, $\therefore G = H_i \cup \sigma_1 H_i \cup \ldots \cup \sigma_{n_i - 1} H_i$; H_i: closed, the rest: open)

FUNDAMENTAL THEOREM CONTINUED

(3) If E corresponds to H, then $[E:k] < \infty \Leftrightarrow H$: open

"$\Rightarrow$": Write $E = k(\alpha_1, \ldots, \alpha_n)$. Consider E' as a splitting field of $m_{\alpha_1,k}, m_{\alpha_2,k}, \ldots, m_{\alpha_n,k} \Rightarrow E \subseteq E' = E_i$ is finite + Galois for some $i \in I$
$E \subseteq E_i \Rightarrow H_i \leq H$ and $[G:H_i] < \infty \Rightarrow [G:H] < \infty$, say

Claim: $\sigma_\ell H$: closed $\forall \ell = 1, \ldots, m$

Proof

$\forall \tau \in G \setminus \sigma_\ell H$, $\tau \notin \sigma_\ell H \Rightarrow \sigma_\ell^{-1}\tau \notin H$ $\because H$ is closed $\therefore \exists i$, s.t. $\sigma_i^{-1}\tau H_i \leq G \setminus H \Rightarrow \tau H_i \subseteq G \setminus \sigma_\ell H \Rightarrow \sigma_\ell H$: closed ✓

"⇐": $e \in H$ (identity) and H: open $\Rightarrow \exists i \in I$, s.t. $H_i = eH_i \subseteq H \Rightarrow E \subseteq E_i$. E_i: is a finite extension $\Rightarrow E$ is a finite extension ✓

(4) E/K: normal $\Leftrightarrow H \lhd G$

"⇒": OK

"⇐": $\forall \alpha \in E$, β is a root of $m_{\alpha,K} \Rightarrow \exists \sigma \in G$, s.t. $\sigma(\alpha) = \beta$

If $\tau \in H$, then $\tau(\beta) = \tau\sigma(\alpha) = \sigma(\sigma^{-1}\tau\sigma)(\alpha) = \sigma(\alpha) = \beta$ ($\sigma^{-1}\tau\sigma \in H$)

$\therefore \beta \in E$. □

EXAMPLE

$\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = ?$

Notice, $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$. $\therefore \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \varprojlim \mathbb{Z}/n\mathbb{Z}$

(Because $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \Leftrightarrow m \mid n$, so $m \le n \Leftrightarrow m \mid n$ for inverse limit)

Actually, $m = pq \Rightarrow \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

$m' = p^2 q \Rightarrow \mathbb{Z}/m'\mathbb{Z} \cong \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

$\downarrow p^i q^j s$

$\vdots$ ⇒ Here, $\mathbb{Z}/p^k\mathbb{Z}$, $\mathbb{Z}/q^l\mathbb{Z}$ are unrelated, so it is a direct product of inverse limit

$\therefore \varprojlim \mathbb{Z}/n\mathbb{Z} = \prod_{p:\text{prime}} \mathbb{Z}_p = \hat{\mathbb{Z}}$ ($\mathbb{Z}_p$: p-adic)