L22

☆: $f(x)\in F[x]$ is solvable by radicals $\rightleftharpoons$ $Gal(f)$ is solvable group ($char=0$)

solvable: $f(x)$的roots是expressible，即可以通过F中元素进行有限次 $+,-,\times,\div,\sqrt{\ }$ 得到 (by radical)

def: $F=F_0\subset F_1\subset\cdots\subset F_n=E$, $F_i=F_{i-1}(a_i)$, $a_i^{p_i}\in F_{i-1}$, p is prime; then:

this chain 称为 radical tower, E is radical extension

def: $f(x)\in F[x]$, f is solvable by radical if: $f(x)$的splitting extension在一个radical extension中

lem: F contains $\forall$ p_i-th primitive root of unity ($x^{p_i}=1$, 所有可以生成循环空间的roots).

then $\forall$ radical extension of F 可以 extend to a normal extension of F

def: E/F is cyclic extension if: $E=F(a)$, $Gal(E/F)$ is cyclic

E is cyclic $\rightleftharpoons$ E is splitting field of x^n-a over F. $a=1$ or F含所有n次单位根

Th1: $f(x)\in F[x]$ solvable by radicals $\Rightarrow$ $Gal(f)$ solvable

proof: 记E is splitting of $f(x)$ over F. E在F的radical extension中

if F contains $\forall p_i$-th primitive of unity, 由lem知: $F=F_0\subset F_1\subset\cdots F_m\subset L$, L/F is normal

$F_i=F_{i-1}(a_i)$ $a_i^{p_i}\in F_{i-1}$; $F_{i-1}\triangleleft F_i$ $\therefore Gal(L/F_{i-1})$ fix F_i also

let $G_0=Gal(L/F)$, $G_i=Gal(L/F_i)$

$\because Gal(L/F_{i-1})$ fix F_i, $\therefore$ then $Gal(L/F_i)\triangleleft Gal(L/F_{i-1})$ 即$G_i\triangleleft G_{i-1}$

故由$F_0\subset F_1\subset\cdots L$可以得到 $1=G_m\triangleleft G_{m-1}\triangleleft\cdots\triangleleft G_0=Gal(L/F)$

$\therefore Gal(L/F)$ solvable

further: $G_{i-1}/G_i=Gal(F_{i-1}/F_i)$ is cyclic of order p_i

Th2: $Gal(f)$ solvable, $\Rightarrow$ $f(x)$ is solvable by radical ($f\in F[x]$, F contains p_i-th roots of unity)

proof: $\exists$ $1=G_m\triangleleft G_{m-1}\triangleleft\cdots\triangleleft G_0=Gal(f)$

其中$G_{i-1}/G_i\cong\mathbb{Z}_{p_i}$, p_i prime.

let E = splitting of f over F. let $F_i=\{a\in E: a^{G_i}=a\}$ G_i的稳定子

then $F\subset F_1\subset F_2\subset\cdots F_m=E$,

F_i/F_{i-1} is normal since $F_i=F_{i-1}(a_1,a_2\cdots)$ G_i fix a but G_{i-1} not; 必有限 since f fixed

$\because F$ contains p_i-th root of $x^{p_i}-1$

$\therefore F_i=F_{i-1}(a_i)$. $a_i^{p_i}\in F_{i-1}$

$\therefore E$ is radical extension of f. f is solvable

Abstract Algebra

: Lecture 22 (proof not in final range)

Leo

2024.12.19

Let Char $F = 0$

proof in Th1.2. 1.2

Theorem 1. *(Galois) $f(x) \in F[x]$ is soluble by radicals if and only if* $\mathrm{Gal}(f)$ *is a solvable group.*

Soluble means the roots of such polynomials are expressible, formally, the roots are algebraic combinations of elements of F and roots of elements of F.

Example 2. *$f(x) = x^n - 2 \in \mathbb{Q}[x]$. Then f is irreducible over $\mathbb{Q}$. Is this polynomial soluble by radicals? The roots of $f(x)$ are $2^{1/n}$, $2^{1/n}\omega$, $\cdots$, $2^{1/n}\omega^{n-1}$, where $\omega = e^{\frac{2\pi i}{n}}$ is a primitive n-th root of unity.*

Definition 3. *Let $F = F_0 \subset F_1 \subset \cdots \subset F_n = E$ where $F_i = F_{i-1}(\alpha_i)$ such that $\alpha^{p_i} \in F_{i-1}$ with p_i prime. Then the chain is called a radical tower, and E is a radical extension.*

Definition 4. *Let $f(x) \in F[x]$. Then $f(x)$ is called soluble by radicals if the splitting field of f is contained in a radical extension.*

Example 5. *Let $F_0 \subset F_1 \subset F_2$ where $F_0 = \mathbb{Q}$, $F_1 = \mathbb{Q}(\sqrt{2})$, $F_2 = F_1(\sqrt[4]{2})$. Then $F_0 \lhd F_1$ and $F_1 \lhd F_2$, but $F_0 \ntriangleleft F_2$.*
$\sigma \in \mathrm{Gal}(F_2/F_1)$ s.t. $\sqrt{2}^{\sigma} = -\sqrt{2}$, so $(x^2 - \sqrt{2})^{\sigma} = x^2 + \sqrt{2}$, and $\pm i2^{1/4}$ are root of this image under σ but not in F_2. So we need to extend F_2.
Let $L = F_2(i) = \mathbb{Q}(i, 2^{1/4})$. Then L is a normal extension of $F_0 = \mathbb{Q}$.

Lemma 6. *Let F contain all the $p_i - th$ primitive roots of unity. Then each radical extension of F can be extended to a normal extension of F.*

Example 7. *$F = \mathbb{Q}$. $f(x) \in F[x]$ is a irreducible polynomial of degree n. Let $E = \mathbb{Q}(\omega_1, \ldots, \omega_t)$ where ω_i is a p_i-th root of unity, with $p_i \leqslant n$, prime. Then $f(x) \in E[x]$ and f is soluble by radicals over $\mathbb{Q}$ is and only if f is soluble by radicals over E. Or the roots of f are expressible over $\mathbb{Q}$ if and only if the roots of f are expressible over E.*

Th1.1 *If $f(x) \in F[x]$ is soluble by radicals, suppose F contains p_i-th roots of unity. Then* $\mathrm{Gal}(f)$ *is a soluble group.*

证明. Let E be the splitting field of $f(x)$ over F. By definition $E \subseteq L$ for some radical extension L of F. By the lemma we may assume that L is a normal extension of F. So we have the following chain:

$$F = F_o \subset F_1 \subset \cdots \subset F_m = L$$

where $F_i = F_{i-1}(\alpha_i)$ s.t. $\alpha_i^{p_i} \in F_{i-1}$. Since F contains all the p_i-th roots of unity. $F_{i-1} \lhd F_i$. Let $G = \mathrm{Gal}(L/F_i)$ then $G_i = \mathrm{Gal}(L/F_i) \lhd G_{i-1}$. So we have the following chain of groups:

$$1 = G_m \lhd G_{m-1} \lhd \cdots \lhd G_0 = \mathrm{Gal}(L/F)$$

Further, $G_{i-1}/G_i = \mathrm{Gal}(L/F_{i-1})/\mathrm{Gal}(L/F_i)$ is a cyclic group of order p_i. So G is soluble. So is $\mathrm{Gal}(f) =$ E/F since this is a subgroup of G which is soluble. □

Th1.2 *If* $\mathrm{Gal}(f)$ *is a soluble group, then* $f(x)$ *is soluble by radicals. (*$f(x) \in F[x]$ *and* F *contains the* p_i*-th roots of unity.)*

证明. Let $G = \mathrm{Gal}(f)$ and G soluble, we have the following chain:

$$G = G_0 \rhd G_i \rhd \cdots \rhd G_m = 1$$

where $G_{i-1}/G_i \simeq Z_{p_i}$ with p_i prime. Let E be the splitting field of f over F and let $F_i = \{a \in E \mid a^{G_i} = a\}$.
Then $F \subset F_1 \subset F_2 \subset \cdots \subset F_m = E$, and F_i is a normal extension of F_{i-1}. Since F contains the p_i-th roots of $x^{p_i} - 1$ we have $F_i = F_{i-1}(\alpha_i)$ s.t. $\alpha_i^{p_i} \in F_{i-1}$. So E is a radical extension of F, and f is soluble by radicals. □

Definition 10. *E is called a cyclic extension of F if $E = F(\alpha)$ and $\mathrm{Gal}(E/F)$ is cyclic.*
Then E is a cyclic extension of F if and only if E is a splitting field of $x^n - a$ s.t. either $a = 1$ or F contains the n-th roots of unity.