15.5-2024

We first show how to apply Thm 7.6 1,
to show **Thm** there is a quintic poly
$f(x) \in \mathbb{Q}[x]$ that is not soluble by radicals.

By serie 9, Question 1.
If p is prime, $f \in \mathbb{Q}[x]$ irred of
degree p with exactly $p-2$ real roots
then $Gal(f) \cong S_p$

Let $f = x^5 - 4x + 2$ which is irred with
exactly $5-2=3$ real roots
Hence $Gal\, f \cong S_5$ which is not soluble
Hence $x^5 - 4x + 2$ is not solv. by radicals.

Rmk. A poly of degree ≥ 5 will
sometimes be soluble by radicals
But the problem we posed in the
beginning is stronger. We do not want
to be able to find roots of a given
poly in terms of radicals but we want
a general formula in terms of the
coefs of the poly: which applies to
any polynomial as in the quadratic
case for example $f = ax^2 + bx + c$
then $x_{1,2} = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

Consider a monic poly of degree n with n zeroes counting multiplicities

$$f_n(x) = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$$

$$= x^n - s_1 x^{n-1} + \dots + (-1)^n s_n$$

with $s_1 = (\alpha_2 + \dots + \alpha_n)$

$$s_2 = (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_{n-1}\alpha_n)$$

$$s_n = \alpha_1 \dots \alpha_n.$$

$s_0, \dots s_{n-1}$ are the elementary symmetric polys, interpreted as elements of $K[\alpha_1, \dots \alpha_n]$ $\subset K(\alpha_1, \dots \alpha_n)$

Defn A poly $q \in K[x_1, \dots x_n]$ is symmetric if

$$q(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = q(x_1, \dots x_n) \text{ for all}$$

permutation $\sigma \in S_n$.

$x_1^2 + \dots + x_n^2$ is another sym poly but it can be expressed in terms of the elementary ones

eg $x_1^2 + x_2^2 = \underbrace{(x_1 + x_2)}_{s_1}{}^2 - 2\underbrace{x_1 x_2}_{s_2}$

This is true in general

Thm Over a field K any symmetric poly in $x_1, \ldots x_n$ can be expressed as a polynomial of smaller or equal degree in the elementary symmetric polynomial $s_r(x_1, \ldots x_n)$ $r=0, \ldots, n$.

Defn The general polynomial of degree n "over K" is the polynomial

$$f_n(x) = x^n - s_1 x^{n-1} + \ldots + (-1)^n s_n \text{ over the field } K(s_1, \ldots s_n).$$

Rmk Technically the poly f_n is over the field $K(s_1 \ldots s_n)$

If we want to find roots of any given poly in terms of radicals using a general formula in terms of the coefs, we should view the coefs as indeterminates and consider

$$\begin{aligned} f(x) &= (x-\alpha_1) \ldots (x-\alpha_n) \\ &= x^n - s_1 x^{n-1} + \ldots + (-1)^n s_n \in K(s_1, \ldots s_n) \end{aligned}$$

Then having a universal formula for the roots of any poly g of degree n in terms of radicals and coefs of g means that the general poly f_n is solvable by radicals.

But we have

Thm (Abel) Let $L = K(\alpha_1, \ldots \alpha_n)$ be a splitting field of general polynomial f_n over $K(s_1 \ldots s_n)$. Then the Galois group of $L : K(s_1 \ldots s_n)$ is the symmetric group S_n.

For a proof see I. Stewart Galois theory Chapter 18.

This gives, together with the fact that S_n, $n \geq 5$, is not soluble, that

Thm (Abel) The general polynomial of degree n is not soluble by radicals for $n \geq 5$.

Proof of f solv by radicals $\Longrightarrow$ $Gal\,f$ is solvable.

We first note the following lemma.

Lemma 7.7. If $L:K$ is a radical extension then $L = K(\alpha_1, \ldots \alpha_n)$, with $\alpha_i^{p_i} \in K(\alpha_1, \ldots \alpha_{i-1})$ with p_i prime $\forall\ 1 \leq i \leq n$.

Proof. Exercise

Hint: Note that any simple radical ext. $K(\alpha):K$ with $\alpha^n \in K$ can be replaced with a radical extension $K \subset K(\beta_1) \subset \cdots \subset K(\beta_1 \ldots \beta_r)$ so that $\beta_r = \alpha$ and $\beta_i^{p_i} \in K(\beta_1 \ldots \beta_{i-1})$ with prime p_i's.

eg. let $\alpha = 2^{1/2.3.5}$ so that $\alpha^{30} \in \mathbb{Q} \subset \mathbb{Q}(\alpha)$

let $\beta_1 := \alpha^{15} = \alpha^{30/2}$ $\quad \beta_1^2 \in \mathbb{Q}$.

1. $\beta_2 := \alpha^5$ so that $\beta_2^3 = \beta_1 \in \mathbb{Q}(\beta_1)$

$\beta_3 := \alpha$, $\alpha^5 = \beta_3^5 = \beta_2 \in \mathbb{Q}(\beta_1, \beta_2)$

We then have the tower of fields

$$\mathbb{Q} \subset \mathbb{Q}(\beta_1) \subset \mathbb{Q}(\beta_1, \beta_2) \subset \mathbb{Q}(\beta_1, \beta_2, \beta_3) = \mathbb{Q}(\beta_1, \beta_2, \alpha) = \mathbb{Q}(\alpha)$$

To prove thm 7.6 we'll use Galois correspondence but since a radical extension need not be a Galois extension, we need

Lemma 7.8 If $L:K$ is a radical extension N a normal closure of $L:K$, then $N:K$ is a radical extension.

Proof. Suppose $L = K(\alpha_1, \dots \alpha_r)$ with $\alpha_i^{p_i} \in K(\alpha_1, \dots, \alpha_{i-1})$ for each i

let f_i be the minimal poly of α_i over K.

Then we know that N is the splitting field of $f = \prod_{i=1}^{r} f_i$, that is

$N = K(\{\beta_{ij}\})$ where $i = 1, \dots, r$ and $\beta_{i1}, \dots, \beta_{id_i}$ are the roots of f_i, including α_i

let $K_i = K(\{\beta_{\ell j}\})_{\ell \leq i}$ Te splitting field of $\prod_{\ell=1}^{i} f_\ell$

K_i clearly contains $K(\alpha_1, \dots \alpha_i)$, so that $\alpha_i^{p_i} \in K_{i-1}$

Since β_{ij}, and α_i have the same minimal poly over K, $\exists$ a K-hom $\tau : N \to N$ s.t $\tau(\alpha_i) = \beta_{ij}$

Hence $\beta_{ij}^{p_i} = \tau(\alpha_i^{p_i}) \in \tau(K_{i-1})$

On the other hand K_{i-1} is also a splitting field, hence is normal. So $\tau(K_{i-1}) = K_{i-1}$

Hence $\beta_{ij}^{p_i} \in K_{i-1}$. Hence $K_{i-1} \subset K_i$ is radical since it is made by sucessively adjoining the β_{ij}, each of which has p_i th power in K_{i-1}

$K_i = K(\{\beta_{lj}\})_{l \leq i}$

$\boxtimes$

The next 2 lemmas give certain abelian extensions

Lemma 7.9 Let K be a field of char 0, L a splitting field of $f(x) = x^p - 1$ over K, p a prime. Then $Gal(L:K)$ is abelian (Hence solvable)

Proof $f'(x) = px^{p-1}$. Since f, f' have no common factor f has no multiple root. Since its zeroes form a finite subgroup of $L^\times$, it is a cyclic group. Let ξ be a generator of this group. Then $L = K(\xi)$ and any K-autom of L is determined by its effect on ξ.

Any K-autom σ of L also permute the zeroes of $x^p - 1$, hence it is of the form

$\alpha_i : \xi \longmapsto \xi^i$

But then clearly $\alpha_i \alpha_j = \alpha_j \alpha_i$

since both send ξ to ξ^{ij}

Hence the Galois group is abelian.

Lemma 7.10 Let K be a field of char 0 in which $X^n - 1$ splits. Let $a \in K$ and L be a splitting field of $x^n - a$ over K. Then the Galois group of $L:K$ is abelian (hence soluble)

Proof Let α be a zero of $x^n - a$, $\xi \in K$ a zero of $x^n - 1$ (exists since $x^n - 1$ splits in K). All zeroes of $x^n - a$ are of the form $a\xi_i$ with ξ_i being zero's of $x^n - 1$ in K.

Hence $L = K(\alpha)$ and any K-autom of L is determined by its action on α.

Let τ, σ be 2 such automorphisms with

$$\tau(\alpha) = \alpha\xi \quad , \quad \sigma(\alpha) = \alpha\omega \quad \text{where}$$

$\xi, \omega \in K$ are zeros of $x^n - 1$,

Then

$$(\tau\sigma)(\alpha) = \tau(\alpha\omega) = \omega\tau(\alpha) = \omega\xi\alpha$$

and

$$\sigma\tau(\alpha) = \sigma(\alpha\xi) = \xi\sigma(\alpha) = \xi\omega\alpha$$

Hence $\tau\sigma = \sigma\tau$ and $Gal(L:K)$ is abelian $\boxtimes$

Now we can use fund thm to prove

Thm 7.11 Let K be a field of char 0, $L:K$ a normal radical extension. Then $Gal(L:K)$ is soluble.

Proof. The idea is to use splitting fields $M, M(\alpha)$ of $x^p - 1$ and $x^p - a$ to have intermediate subfields with abelian Galois groups and use an inductive argument.

Suppose $L = K(\alpha_1 \ldots \alpha_n)$ with $\alpha_i^{p_i} \in K(\alpha_1 \ldots \alpha_{i-1})$ with p_i's prime (using Lemma 7.7) $\forall i$

In particular there is a prime p s.t $\alpha_1^p \in K$.
We use induction on n.
($n=0$: nothing to prove)
If $\alpha_1 \in K$ then $L = K(\alpha_2 \ldots \alpha_n)$ and $Gal(L:K)$ is soluble by induction.
So we can assume $\alpha_1 \notin K$.
Let f be the minimal poly of α_1 over K.

Since $L:K$ is normal and $\alpha \in L$, f splits in L.
It is also separable since we are in char 0.

Since $\alpha_1 \notin K$, $\deg f \geq 2$. Let β be another zero of f, $\beta \neq \alpha_1$

Since $\alpha_1^p \in K$, α_1 is a zero of $x^p - \alpha_1^p \in K[x]$. Since $f(\alpha_1) = 0$, $f \mid x^p - \alpha_1^p$. Since $f(\beta) = 0$ β is also a zero of $x^p - \alpha_1^p$. Hence $\beta^p = \alpha_1^p$. let $\varepsilon = \alpha_1/\beta$. Then $\varepsilon \neq 1$ and

$\varepsilon^p = 1$. Thus ε has order p in $L^\times$, and

$1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-1}$ are distinct roots of $x^p - 1$ in L. let $M \subset L$ be splitting field of $x^p - 1$ So that $M = K(\varepsilon)$ and $[M:K]$ is a normal sep. extension, hence Galois, and by lemma 7.9 $Gal(M:K)$ is abelian

Consider the extensions $K \subseteq M \subseteq M(\alpha_1) \subseteq L$.

$$\begin{array}{c} L \\ | \\ K(\varepsilon, \alpha_1) = M(\alpha_1) \\ \text{Abelian by lemma 7.10} \leftarrow | \\ M = K(\varepsilon) \\ \text{Abelian by lemma 7.9.} \leftarrow | \\ K \end{array}$$

Now since $x^p - 1$ splits in M and $\alpha_1^p \in K \subset M$ $x^p - \alpha_1^p$ has splitting field $M(\alpha_1)$ over M.

By lemma 7.10 $Gal(M(\alpha_1) : M)$ is abelian

Both $L:K$ and $L:M$ normal sep. extensions. Hence Fund thm applies to both.

We first apply it to $M \subset M(\alpha_1) \subseteq L$. $M(\alpha_1) : M$, being a splitting field of $x^p - \alpha_1^p$ over M, is also normal. Hence viewing $M(\alpha_1)$ as a subfield of $L:M$ we have $Gal(L : M(\alpha_1)) \trianglelefteq Gal(L:M)$

and

$$\mathrm{Gal}(M(\alpha_1):M) \cong \mathrm{Gal}(L:M)/\mathrm{Gal}(L:M(\alpha_1))$$

Note $L = M(\alpha_1)(\alpha_2 \ldots \alpha_n)$ so that

$L : M(\alpha_1)$ is a normal radical extension

By induction $\mathrm{Gal}(L:M(\alpha_1))$ is soluble.

$\mathrm{Gal}(M(\alpha_1):M)$ being abelian is also soluble.

Recall: if N and G/N are soluble then G is solu.

Hence we get that $\mathrm{Gal}(L:M)$ is soluble.

Now consider

$$\begin{array}{c} L \\ | \\ M \\ | \\ K \end{array}$$

M is splitting field of $x^p - 1$ over K

Hence $M:K$ is normal

$\mathrm{Gal}(M:K)$ is abelian by lemma 7.9, hence soluble

Now $\mathrm{Gal}(M:K) \cong \mathrm{Gal}(L:K)/\mathrm{Gal}(L:M)$

We've proved $\mathrm{Gal}(L:M)$ is soluble

Applying N, G/N solu $\Rightarrow G$ solu. one more time we get (with $N = \mathrm{Gal}(L:M)$)

$\mathrm{Gal}(L:K)$ is soluble

$\blacksquare$

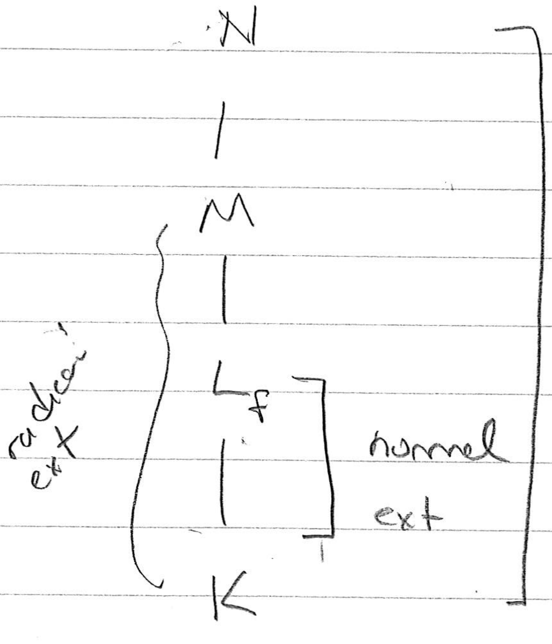
We can now prove Thm 7.6

Proof of Thm 7.6: Let $f \in K[x]$ be a poly soluble by radicals.

Then by defn the splitting field L_f of f over K is contained in a radical extension $K \subset L_f \subset M$.

Let N be the normal closure of $M:K$ so that $K \subset L_f \subset M \subset N$ and $N:K$ is a radical extension, which is normal.

By Thm 7.11, $\tilde{G} = Gal(N:K)$ is soluble.



normal radical ext.

Since $L_f:K$ is normal ext. $Gal(N:L_f)$ is a normal subgp of $Gal(N:K) = \tilde{G}$

and $Gal(L_f:K) \cong \tilde{G}/Gal(N:L_f)$

Recall If G is solu, $N \triangleleft G$ then G/N is solv.

Hence $Gal(L_f:K)$ is soluble

$\blacksquare$

§8. Application of Galois theory: fund. thm of algebra

The proof assumes the following facts about the real numbers, and polys over reals.

(1) If $f(x) \in \mathbb{R}[x]$ and $\exists\ a, b \in \mathbb{R}$ s.t $f(a) > 0$ and $f(b) < 0$ then $f(x)$ has a real root.

This is just intermediate value thm for the continuous function f.

(2) Every positive real $r > 0$ has a real square root

Let $f(x) = x^2 - r$, then $f(1+r) = (1+r)^2 - r$
$= r^2 + r + 1 > 0$

$f(0) < 0$

Hence by (1) $\exists\ x \in \mathbb{R}$ s.t $x^2 = r$.

(3) Every $f(x) \in \mathbb{R}[x]$ of odd degree has a real root

$f(x) = a_0 + a_1 x + \dots + x^n \in \mathbb{R}[x]$

Let $T := 1 + \sum |a_i|$

Then $|a_i| \leq T - 1$ $\forall i$ and

$|a_0 + a_1 T + \dots + a_{n-1} T^{n-1}| \leq (T-1)(1 + T + \dots + T^{n-1})$
$= T^n - 1 < T^n$

For any n (not necessarily odd)

$f(T) > 0$ since the sum of the first $n-1$ terms is dominated by T^n

If n is odd then $f(-T) < 0$ ~~because~~

$(-T)^n = (-1)^n T^n < 0$ and $f(-T) < 0$
(once again since the sum of the first $n-1$ terms is dominated by T^n

Hence by (1) f has a real root.

Next we have the following about quadratic polys in $\mathbb{C}[x]$

(4) If $q(x) \in \mathbb{C}[x]$ is a quadratic poly then q has a root in $\mathbb{C}$.
Equivalently there are no quadratic extensions of $\mathbb{C}$ since such an extension would contain an element whose irreducible polynomial is a quadratic poly in $\mathbb{C}[x]$.

First note any quadratic poly ax^2+bx+c can be transformed to $Y^2 - A$ by completing the square.
Hence it is enough to show that any complex number A has a square root in $\mathbb{C}$

If $A = re^{i\theta}$ then $B = \sqrt{r}\, e^{i\theta/2}$ satisfy $B^2 = A$.

Finally note

5 There is no field extension $K : \mathbb{R}$ s.t $[K : \mathbb{R}]$ is odd and > 1.

Since if $\alpha \in K$ then its irred. poly must be even by 3.
But then $[K : \mathbb{R}] = [K : \mathbb{R}(\alpha)][\mathbb{R}(\alpha) : \mathbb{R}]$ is also even.

Finally we can prove

Thm (Fundamental thm of algebra)
Every non-constant poly $f(x) \in \mathbb{C}[x]$ has a complex root.

Proof let σ denote the complex conjugation
If f has no root in $\mathbb{C}$ then neither does

$$\bar{f} = \sigma(f) = \sigma(a_0) + \sigma(a_1)x + \dots \sigma(a_n)x^n$$

$$= \bar{a}_0 + \bar{a}_1 x + \dots + \bar{a}_n x^n$$

The product $f(x)\bar{f}(x)$ has coefs which are invariant under σ hence coef of $f\bar{f}$ are real

Hence it is enough to prove that a poly $f \in \mathbb{R}[x]$ has a root in $\mathbb{C}$.

let $f(x) = a_0 + \cdots + a_n x^n \in \mathbb{R}[x]$

let K be its splitting field over $\mathbb{R}$

Then $K(i)$ is a Galois extension since it is a splitting field of $f(x)(x^2+1)$

let $G = Gal(K(i) : \mathbb{R})$

<u>w.t.s.</u> $K(i) = \mathbb{C}$

If $|G| = 2^m k$ where k is odd, let

P_2 denote the 2-sylow s/gp of G.

$Fix(P_2)$ is an extension of $\mathbb{R}$ of odd degree

Since $k = \dfrac{|G|}{|P_2|} = [Fix(P_2) : \mathbb{R}]$

But then by (5) $\mathbb{R}$ has no extension of odd degree >1. Hence $k=1$ and G is a 2-group.

$$\begin{tikzcd}[column sep=small]
 & K(i) \arrow[dl, dash] \arrow[dr, dash, "\text{Galois}"] \arrow[dd, dash, "\text{Galois}" description] & \\
K \arrow[dr, dash] & & \mathbb{R}(i) = \mathbb{C} \arrow[dl, dash] \\
 & \mathbb{R} &
\end{tikzcd}$$

Since $[K(i) : \mathbb{R}] = |G| = 2^m$

$[K(i) : \mathbb{R}(i)] = 2^\ell$ for some ℓ

Since $K(i) : \mathbb{R}(i)$ is also a Galois ext.

$Gal(K(i) : \mathbb{C})$ is also a 2-gp.

We know from group theory that a non-trivial p-group of order p^ℓ has subgroups of all orders p^f, $0 \leq f \leq \ell$

$$\begin{tikzcd}
K(i) \arrow[d, dash] & & \{e\} \arrow[d, dash] \\
\mathrm{Fix}(H) \arrow[d, dash] & & H \arrow[ll] \arrow[d, dash] \\
\mathbb{C} & & Gal(K(i) : \mathbb{C})
\end{tikzcd}$$

ℓ

Hence if $Gal(K(i) : \mathbb{C})$ is not trivial. ~~then~~ there is a subgroup of $Gal(K(i) : \mathbb{C})$ s.t

$$[\mathrm{Fix}(H) : \mathbb{C}] = 2$$

But by 4 there is no quad ext of $\mathbb{C}$

Hence $[K(i) : \mathbb{C}] = 1$, $K(i) = \mathbb{C}$, f splits in $\mathbb{C}$.

$\boxtimes$