Galois Theory of Equations

Jacobson BAI chap. 4

Fall, 2018, course at NTU

4.1 Field Ext.

F field $\supset$ prime ring $\begin{cases} \mathbb{Z} & \Rightarrow F \supset \mathbb{Q} \leftarrow \text{prime field} \\ \mathbb{Z}_p & \leftarrow \text{prime field} \end{cases}$

field ext (inclusion)

$F \subset E$ $\quad$ $S \subset E$ subset $\quad$ $F[S]$ sub ring $\quad$ $F(S)$ sub field $\quad$ gen by S

$S = \{u\}$: $F[x] \xrightarrow{\eta} F[u]$

$\ker \eta = 0$ transcendental $\qquad f(u) = 0$ algebraic

$\ker \eta = (f(x))$ $\quad$ f prime = irred (monic)

$F[x]/(f(x)) \xrightarrow{\sim} F[u] = F(u)$ is in fact already a field

Called a simple field ext (if $\deg f \geq 2$)

Notation : E/F $\quad$ $[E:F] = \dim_F E$

Fact : $u \in E$ alg. $/F \Leftrightarrow [F(u):F] = n < \infty$

and then $F(u) = F[u]$ with min poly $f(x)$ of u with $\deg f = n$.

Thm : $K \supset E \supset F \Rightarrow [K:F] = [K:E][E:F]$

finite iff both finite

pf : $[K:F] < \infty \Rightarrow [E:F] < \infty$ (subspace)

$[K:E] < \infty$ base$/F \Rightarrow$ gen$/E$

Conversely : K/E base $v_1 \cdots v_m$

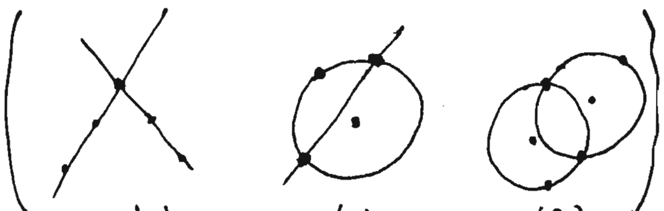
E/F base $w_1 \cdots w_r$

$K \ni z = \sum \underline{a_i} v_i = \sum v_i \underline{b_{ij} \cdot w_j}$

$\{v_i w_j\}$ generators. Easy to check li. ind. $\#$

4.2 Ruler & Compass

$S_1 := S = \{P_1, \dots, P_n\} \subset \omega$ $\quad n \geq 2$ pts on a plane ω

$S_{r+1} := S_r \cup \Big($  $\Big)$

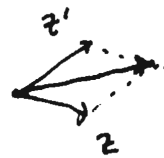
(1) (2) (3)

Def^n constructible pts $:= C(P_1, \dots, P_n) = \bigcup_{r=1}^{\infty} S_r$.

~~Thm~~ : Identify $\omega = \mathbb{C}$, $P_i = z_i$ with $z_1 = 0$, $z_2 = 1$

then $C(z_1, \dots, z_n)$ = the smallest subfield in $\mathbb{C}$ containing z_i's closed under $\sqrt{z}$ and $\bar{z}$.

pf: C is a ab. gp by



a ring (zz') and $z^{1/2}$

by using polar coordinates

to separate the constructions. $\bar{z}$ is easy.

Conversely, if $\mathbb{C} \supset C' \supset \{z_1, \dots, z_n\}$ and closed under $z^{1/2}$ and $\bar{z}$, then it contains all points arising from (1), (2), (3).

~~Key point~~ : $z = x + iy \in C' \Rightarrow x, y \in C'$

Hence all eq^n (deg $= 1, 2$) are real coeff in C' #

Rmk: $C \supset \mathbb{Q} + \mathbb{Q}i$, hence dense in $\mathbb{C}$!

Also dense in all lines and circles in the constructions.

Criterion (Square root tower) A*

Let $F = \mathbb{Q}(z_1, \dots, z_n, \bar{z}_1, \dots, \bar{z}_n)$. Then $z \in \mathbb{C}$ is constructable from F $\Leftrightarrow$ $\exists\, u_1, \dots, u_r \in \mathbb{C}$, $u_1^2 \in F$, $u_2^2 \in F(u_1)$, $\dots$, $u_i^2 \in F(u_1, \dots, u_{i-1})$ and z is contained in such a tower.

Cor: $[F(z) : F] = 2^s$ for some $s \geq 0$.

Many cases $F = \mathbb{Q}$

App 1. Trisection of angles:

Solve $4x^3 - 3x - \cos\theta = 0$ $\quad (x = \cos \theta/3)$

eg. $\theta = \pi/3$, $4x^3 - 3x - \frac{1}{2} \in \mathbb{Q}[x]$ is irr.

$\Rightarrow$ a root a has degree 3 ※

App 2. Duplication of the cube:

Solve $x^3 - 2 = 0$, which is irr. in $\mathbb{Q}[x]$. ※

App 3. Regular p-gons: (preliminary, p prime)

Solve $z^p = 1$, or $z^{p-1} + \dots + z + 1 = 0$

irr. in $\mathbb{Q}[x]$ (Eisenstein criterion)

hence constructible $\Rightarrow$ $p = 2^s + 1$

but then $s = 2^t$. let $F_n = 2^{2^n} + 1$

• Known Fermat primes are $F_0, F_1, \underset{17}{F_2}, F_3, F_4 = 65537$

Euler 1732: $F_5 = 641 \times 6700417$ is not.

not for $5 \leq n \leq 24$ (2014, computer)

Thm (Gauss 1796) n-gon constr. $\Leftrightarrow$ $n = 2^r \prod P_i$, P_i: Fermat

need study on cyclotomic ext to prove it.

Rmk: Squaring the circle $\sqrt{\pi}$: Will see more generally that π is transcendental!

Example 1. Regular pentagon (5-gon)

$x^4 + x^3 + x^2 + x + 1 = 0$ let $u = x + \frac{1}{x}$

$\Rightarrow u^2 + u - 1 = 0$ i.e. $u = \frac{1}{2}(-1 + \sqrt{5})$

$x^2 - ux + 1 = 0 \Rightarrow x = \frac{1}{4}(-1+\sqrt{5}) + \frac{1}{2}\sqrt{\frac{5+\sqrt{5}}{2}}\, i$

Example 2. Gauss' 17-gon (19 yr old)

$$16\cos\frac{2\pi}{17} = -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34-2\sqrt{17}} - 2\sqrt{34+2\sqrt{17}}}$$

4.3 Splitting Field

Def'n: Let $f(x) \in F[x]$. Then $E \supset F$ is a splitting field of $f(x)$ over F if

$(*)$ $f(x) = \prod_{i=1}^{n}(x - r_i)$ in $E[x]$ and $E = F(r_1, \cdots, r_n)$.

Lemma: Splitting field exists.

pf: If $f(x) = f_1(x) \cdots f_r(x)$ irred decomp

Take $K = F[x]/\langle f_1(x)\rangle$ if $\deg f_1 \geq 2$

Kronecker's magic $= F(r)$ with $r = x + \langle f_1(x)\rangle$

$f(r) = 0 \Rightarrow f(x) \in K[x]$ decomposes further.

Repeat the process at most $n = \deg f$ times we get a field $E \supset F$ st. $f(x)$ splits as $(*)$.

Since we add only roots of $f \Rightarrow E = F(r_1, \cdots, r_n)$ ※

Caution: Better to use diff symbol "X" in the process to avoid confusion?

Examples:

(1) $f(x) = x^6 - 1 = (x+1)(x-1)(x^2+x+1)(x^2-x+1) \in \mathbb{Q}[x]$

$x^2 + x + 1$ has a root $r = \frac{1}{2}(-1 + \sqrt{3}i)$

join $r \Leftrightarrow$ join $\sqrt{3}i \Leftrightarrow f(x)$ splits.

(2) $f(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$

Join $r = \sqrt{2}$ does not split $x^2 - 3$: if it splits, then $\exists\, a, b \in \mathbb{Q}$ st. $(ar+b)^2 - 3 = 0 \dashrightarrow$ ※.

In general the splitting pattern is complicate.

To get "uniqueness" of splitting field,

Lemma: let $\eta : F \xrightarrow{\sim} F'$ isom of fields E/F, E'/F'. $r \in E$ alg $/F$ with min. poly $g(x)$.
Then $\exists\, \zeta : F(r) \hookrightarrow E'$ extending η
$\iff g'(x) := \eta(g(x))$ has a root in E'.
Moreover, # of ζ = # dist. roots of $g'(x)$ in E'.

pf: ζ exists $\Rightarrow g'(\zeta(r)) = \zeta(g(r)) = 0$.
conversely, if $g'(r') = 0$, $r' \in E'$, get
$\varphi : F[x] \longrightarrow E'$ by $h(x) \mapsto h'(r')$
with $g(x) \in \ker \varphi$, hence get

$F(r) \underset{\psi}{\xrightarrow{\sim}} F[x]/\langle g(x) \rangle \underset{\bar\varphi}{\longrightarrow} E'$ $F(r)$ field $\Rightarrow \bar\varphi$ inj.

Hence $\zeta := \bar\varphi \circ \psi$ is the extension of η.
Also it is clear that $\# \zeta = \# r'$ ✻

Thm: let $\eta : F \xrightarrow{\sim} F'$. $f(x) \in F[x]$ monic, E, E' be splitting fields of $f(x)/F$, $f'(x)/F'$.
Then $\exists$ ext $E \xrightarrow{\sim} E'$ of η.
# of ext $\le [E:F]$. "=" iff $f(x)$ has dist roots.

pf: By induction on $[E:F]$ using Lemma ✻
Key: Think: what does this mean! Use same f.
$[E:F] = 1$ ok. Let $[E:F] > 1$, $g(x)$ irr. factor of $f(x)$ with $m = \deg \ge 2$. Let $g(r_1) = 0$, $[K = F(r_1) : F] = m$.
$\exists\, k$ ext $\zeta_i : K \to E'$, k = # dist. roots of $g(x)$.
Now replace F, F' by $K, \zeta_i(K)$ and apply ind. ✻

4.4 Multiple Roots

Def: $f(x) \in F[x] \Rightarrow f(x+h) \equiv f(x) + f'(x)h \mod h^2$

Fact: $f(x)$ has simple roots in any splitting field $E/F \iff (f, f') = 1$.

pf: $\Leftarrow$: $f(x) = (x-r)^k g(x)$ in $E[x]$, $k \ge 2 \Rightarrow x - r \mid f'(x)$
$\Rightarrow$: $f(x) = \prod (x - r_i)$ $\Rightarrow$ $f'(x) = \sum_{i=1}^{n} (x-r_1)\cdots\widehat{(x-r_i)}\cdots(x-r_n)$
$r_i \ne r_j$ for $i \ne j$
hence $x - r_i \nmid f(x)$ $\forall i$ ✻

Def^n (1) $f(x) \in F[x]$ is separable if all its irreducible factors have simple roots.
(2) F is perfect if all $f(x) \in F[x]$ are separable.

Thm (i) If char $F = 0$ then F is perfect.
(ii) If char $F = p \ne 0$, then F is perfect $\iff F = F^p$ (eg. finite).

pf: (i) is easy: f irr. $\Rightarrow (f, f') = 1$ since $f'(x) \not\equiv 0$.
(ii) Since $f'(x) = n a_n x^{n-1} + \cdots + a_1$ has $\deg f' < \deg f$, $(f, f') \ne 1 \Rightarrow f'(x) \equiv 0$
i.e. $f(x) = a_0 + a_p x^p + \cdots + a_{mp} x^{mp}$
$\Leftarrow$: write $a_{kp} = b_k^p$, get $= (b_0 + b_1 x + \cdots + b_m x^m)^p$
hence f is not irr. ✻

(Lemma: in char $F = p$, $x^p - a$ is irr. or p-power.) $\Rightarrow$: If $\exists\, a \in F \setminus F^p$ then $f = x^p - a$ is irr. but $f'(x) \equiv 0$ ✻

pf: If $f = x^p - a = g(x) h(x)$
in splitting field E/F get a root b, $a = b^p$
$f = (x-b)^p \Rightarrow g(x) = (x-b)^k \Rightarrow b^k \in F \Rightarrow b \in F$.

4.5 Galois Groups / Fund. Thm

Def'n: $\mathrm{Gal}\, E/F := \mathrm{Aut}_F E \subset \mathrm{Aut}\, E$

Given a field E, 2 operations

$E \supset F$ subfield $\mapsto \mathrm{Gal}\, E/F$

$\mathrm{Aut}\, E \supset G$ subgp $\mapsto \mathrm{Inv}\, G \equiv E^G$

Fact: $G_1 \supset G_2 \Rightarrow E^{G_1} \subset E^{G_2}$

$F_1 \supset F_2 \Rightarrow \mathrm{Gal}\, E/F_1 \subset \mathrm{Gal}\, E/F_2$

Q: "="? $\mathrm{Inv}(\mathrm{Gal}\, E/F) \supseteq F$; $\mathrm{Gal}\,(E/\mathrm{Inv}\, G) \supseteq G$

Lemma (cor of thm) 1: E/F splitting field of $f(x) \in F[x] \Rightarrow |\mathrm{Gal}\, E/F| \leq [E:F]$, "=" if f sep.

Lemma 2 (Artin): $[E : E^G] \leq |G|$ for G finite

pf: Let $|G| = n$, $F := E^G$. For $m > n$

we claim any $u_1, \cdots, u_m \in E$ are l.d. $/F$.

Let $G = \{\eta_1 = 1, \eta_2, \cdots, \eta_n\}$. Then $\sum_{j=1}^m u_j x_j = 0$ ($x_j \in F$)

$\Rightarrow (*)\ \sum_{j=1}^m \eta_i(u_j)\, x_j = 0 \quad \forall i = 1, \cdots, n$

Conversely, $(*)$ has sol in $x_j \in E$, not all 0, may try to get sol in F from it.

By reordering, let $b_1 = 1, b_2, \cdots$ be sol with smallest non-zero elements. Will show $b_i \in F$.

if $\eta_k(b_2) \neq b_2$, then

$(**)\ \sum_{j=1}^m (\underline{\eta_k \eta_i})(u_j) \cdot \eta_k(b_j) = 0. \quad i = 1, \cdots, n$

same as η_i (permutation)

ie. $(1, \eta_k(b_2), \cdots, \eta_k(b_m))$ is also a sol.

$\Rightarrow (\underline{0}, b_2 - \eta_k(b_2), \cdots, b_m - \eta_k(b_m))$ has fewer $\ast$

Def'n E/F is

(1) algebraic if $a \in E$ is [alg] $\forall a$. True if $[E:F] < \infty$

but not nec. eg. $\bar{\mathbb{Q}}/\mathbb{Q}$.

(2) separable if alg + minimal poly of a sep $\forall a$

(3) normal if alg + every irr. $f(x) \in F[x]$ once has a root in E then splits in $E[x]$

ie. E contains a splitting field of $m_a(x)$ $\forall a \in E$.

(4) Galois := normal + separable

Thm (Finiteness) Let $E \supset F$. Then TFAE:

(1) E = splitting field of a sep. $f(x) \in F[x]$.

(2) $F = E^G$ for some finite $G \subset \mathrm{Aut}\, E$.

(3) E/F is finite Galois (ie. normal + sep.)

Moreover, we have $^{*}F = \mathrm{Inv}\,\mathrm{Gal}\, E/F$ & $^{**}G$ in (2) $\underset{\text{must be}}{=} \mathrm{Gal}\, E/F$

pf: (1) $\Rightarrow$ (2): $F' := E^G \supset F$ for $G = \mathrm{Gal}\, E/F$

E is also a splitting field of $f(x)$ over F'

and by def $G = \mathrm{Gal}\, E/F'$ too. So $[F':F] = 1$, $F' = F$.

This also proves ⊛. by lemma 1.

(2) $\Rightarrow$ (3): $[E:F] \leq |G| < \infty$ by lemma 2.

Let $f(x) \in F[x]$ irr. $f(r) = 0$ for some $r \in E$.

Let $Gr = \{r_1, \cdots, r_m\} \Rightarrow f(r_i) = 0 \quad \forall i = 1, \cdots, m$

orbit, distinct

$\Rightarrow g(x) := \prod_{i=1}^m (x - r_i) \mid f(x)$

since $g(x)$ is G-inv & $F = E^G \Rightarrow g(x) \in F[x]$.

ie. $f(x) = g(x)$ and with simple roots.

(3) $\Rightarrow$ (1): Since $[E:F] < \infty$, Write $E = F(r_1, \cdots, r_k)$

r_i is alg $/F$. $m_{r_i}(x)$ = prod. dist. linear factors

So $f(x) = \prod m_{r_i}(x)$ is sep. with splitting field E.

(**) follows from $\mathrm{Gal}\, E/F \supset G$ & $|G| \geq [E:F] = |\mathrm{Gal}\, E/F|$

Fund Thm of Galois : Let E/F finite [illegible]

with $G = \mathrm{Gal}\, E/F$ ① Then $\exists$ 1-1 correspondence

$E \supset K \supset F \mapsto \mathrm{Gal}\, E/K$; $G \supset H \mapsto E^H$. Also

② $H \triangleleft G \iff E^H$ normal $/F$ (hence Galois)

and then $\mathrm{Gal}\ E^H/F \simeq G/H$.

pf : ① $H \Rightarrow E/E^H$ Galois with gp $H = \mathrm{Gal}\, E/E^H$.

$K \Rightarrow E/K$ Galois with $K = \mathrm{Inv}\ \mathrm{Gal}\, E/K$ by (1).

② Let $H \subset G$ with $K = E^H$

for $\eta \in \mathrm{Gal}\, E/F$, $\eta H \eta^{-1} \subset G$ corr to $\eta(K)$:

since $h(k) = k \overset{\circledast}{\iff} (\eta h \eta^{-1})\eta(k) = \eta(k)$.

So $H \triangleleft G \iff \eta(K) = K \quad \forall \eta \in G$.

- If so, then $\bar\eta := \eta|_K \in \mathrm{Gal}\, K/F$

i.e. $G \xrightarrow{\rho} \mathrm{Gal}\, K/F : \eta \mapsto \bar\eta$ with image $\bar G$

Since $K^{\bar G} = F$, prev thm $\Rightarrow$ <u>K/F Galois</u> & $\bar G = \mathrm{Gal}\, K/F$ i.e. normal + sep.

Now $\eta \in \ker \rho \iff \eta|_K = \mathrm{id}_K$, ie. $\eta \in \mathrm{Gal}\, E/K = H$

$\Rightarrow \mathrm{Gal}\, K/F \simeq G/H$.

- Conversely, if K/F normal , let $a \in K$, then

$m_a(x) = (x-a_1)\cdots(x-a_m) \in K[x]$, $a_1 = a$.

$\eta \in G \Rightarrow f(\eta(a)) = 0 \Rightarrow \eta(a) = a_i \in K$, ie $\eta(K) \subset K$.

As in $\circledast$, this $\Rightarrow H \triangleleft G$ for $H = \mathrm{Gal}\, E/K$ #

Example : Any finite gp is a Galois gp .

Let $E = F(x_1, \cdots, x_n)$, $g(x) = \prod_{i=1}^{n} (x - x_i) = x^n - p_1 x^{n-1} + \cdots (-1)^n p_n$

$G = S_n \subset \mathrm{Aut}\, E$, E is a splitting field of $g(x)$

over $F(p_1, \cdots, p_n)$ with <u>dist. roots</u>. $\eta \in \mathrm{Gal}\, E/F(p_1 \cdots p_n) \Rightarrow \eta \in S_n$

$\Rightarrow$ Any $H \subset G$ is $\mathrm{Gal}\, E/K$ for $K = E^H$ #

4.6 Results on finite gps (solvable gps)

Def^{n}: G is solvable if $\exists$ normal series

(*) $G = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{s+1} = 1$ st. G_i/G_{i+1} ab .

Examples (1) G ab. (2) $|G| = p^n$ via centers .

Recall : $G' := [G, G]$ gen by $[g, h] = g^{-1}h^{-1}gh$

since $I_a[g, h] = [I_a g, I_a h]$; $K \triangleleft G \Rightarrow K' \triangleleft G$.

get derived series $G \triangleright G' \triangleright G'' \triangleright \cdots \triangleright G^{(k)}$

G ab $\iff G' = 1$, So G/K ab $\iff K \supset G'$.

<u>Thm:</u> G solvable $\iff G^{(k)} = 1$ for some k .

pf : $\Leftarrow$ is trivial . $\Rightarrow$: Given (*)

$G_{i+1} \supset G_i' \ \forall i$ so $G_2 \supset G_1' = G^{(1)}$

if $G_k \supset G^{(k)}$ (ok for $k=1$) , then

$G_{k+1} \supset G_k' \supset (G^{(k)})' = G^{(k+1)} \Rightarrow G^{(s+1)} = 1$ #

Cor. Let $G \triangleright K$. Then G sol. $\iff K$ and G/K are .

pf : In fact, any $H \subset G \Rightarrow H^{(i)} \subset G^{(i)}$

Also any $\eta : G \to \bar G \Rightarrow \eta G^{(i)} = \eta(G)^{(i)}$

This gives a strong form of $\Rightarrow$.

$\Leftarrow$: $(G/K)^{(k)} = 1 \Rightarrow G^{(k)} \subset K \Rightarrow G^{(k+l)} = 1$ #

Example / Thm : $n \geq 5 \Rightarrow A_n$ simple , S_n not solvable.

pf : If $1 \neq K \triangleleft A_n$, will show $K = A_n$.

if $(123) \in K$ then $(ijk) \in K$ via γ or $(lm)\gamma$

where $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ i & j & k & l & m & \cdots \end{pmatrix}$ then done .

Let $1 \neq \alpha \in K$ which fixes maximal elements .

then (1) $\alpha = (123\cdots)\cdots$ or (2) $\alpha = (12)(34)\cdots$

if α is not a 3-cycle, then in case (1) α

moves 2 more elements say 4, 5 .

Let $\beta = (345)$, $\alpha_1 = \beta\alpha\beta^{-1}$ then

$\alpha_1 = (124\cdots)\cdots$ or $(12)(45)\cdots \neq \alpha$

let $\alpha_2 = \alpha_1\alpha^{-1} \neq 1$ $(= \beta\alpha\beta^{-1}\alpha^{-1})$

if $k > 5$ is fixed by α, then also fixed by α_2

in (1), $\alpha_2(2) = 2$, in (2) $\alpha_2(1) = 1$, $\alpha_2(2) = 2$ *

To get criterion using any series, need

Def'n: A composition series is $G = G_1 \triangleright G_2 \triangleright \cdots \triangleright 1$ st. G_i/G_{i+1} is simple $(\neq 1)$. $|G| < \infty \Rightarrow \exists$.

~~Thm (Jordan-Hölder)~~ The factors G_i/G_{i+1} are unique up to permutations $\forall$ comp. series.

Cor. Let $|G| < \infty$, then G sol. $\Leftrightarrow$ all factors $\cong \mathbb{Z}_p$'s.

Pf: By induction on $|G| < \infty$: Given

① $G = G_1 \triangleright G_2 \triangleright G_3 \triangleright \cdots \triangleright G_{s+1} = 1$

② $ = \tilde{G}_1 \triangleright \tilde{G}_2 \triangleright \tilde{G}_3 \triangleright \cdots \triangleright G_{t+1} = 1$

if $G_2 = \tilde{G}_2$ then done. Otherwise

$G \trianglerighteq G_2\tilde{G}_2 \ntrianglerighteq G_2 \Rightarrow G = G_2\tilde{G}_2$. Let $K_3 = G_2 \cap \tilde{G}_2$

and $G_2\tilde{G}_2/\tilde{G}_2 \cong G_2/K_3$, also $G_1/G_2 \cong \tilde{G}_2/K_3$

* $G_1/\tilde{G}_2$ simple — simple

Get 2 more intermediate comp. series via K_3:

①' $G = G_1 \triangleright G_2 \triangleright \underline{K_3 \triangleright K_4 \triangleright \cdots \triangleright K_{u+1} = 1}$

②' $ = \tilde{G}_1 \triangleright \tilde{G}_2 \triangleright \underline{K_3 \triangleright K_4 \triangleright \cdots \triangleright K_{u+1} = 1}$

Now ① ~ ①' since $|G_2| < |G|$, hence $s = u$

①' ~ ②' by the basic isom thm *.

②' ~ ② since $|\tilde{G}_2| < |G|$, hence $t = u = s$ *

4.7 Solutions by Radicals / in char 0

~~Def'n~~: $f(x) \in F[x]$ sol. by rad. if $\exists$ ~~root tower~~

$F = F_1 \subset F_2 \subset \cdots \subset F_{r+1} = K$ st (i) $F_{i+1} = F_i(d_i)$, $d_i^{n_i} = a_i \in F_i$

and (ii) K contains a splitting field of $f(x)/F$.

Lemma 1. Let $f(x) = x^n - 1$ then ~~G_f is ab~~ if char $F = 0$ — Gal of its splitting field (here cyclotomic)

Pf: $(f', f) = (nx^{n-1}, x^n - 1) = 1$

$\Rightarrow$ dist. roots $U_n = \{z_1, \dots, z_n\} \subset F^\times$ is a cyclic gp $\cong \mathbb{Z}_n$

$G_f \hookrightarrow \mathrm{Aut}\, U_n : \eta \mapsto \eta|_{U_n}$ is inj, $\mathrm{Aut}\, \mathbb{Z}_n = U(\mathbb{Z}_n)$ is the gp of units, hence abelian *

Lemma 2. ($*_n$) If F contains all n-th roots of 1 and all dist. (eg. char 0)), then G_f cyclic, $|G_f| \mid n$ where $f(x) = x^n - a$, $a \in F$.

Pf: Let E/F a splitting field, $f(r) = 0$, $r \in E$.

Then $z_1 r, \dots, z_n r$ are all roots of $f(x) = 0$.

So $E = F(r)$ and $G_f \hookrightarrow U_n : \eta \mapsto z$ if $\eta(r) = \underline{z} r$. *

Lemma 3. Assume ($*_p$), p a prime. If E/F is cyclic (i.e. Galois with cyclic gp) of dim p, then $E = F(d)$ with $d^p = a \in F$. (cf. (4.5) Ex. 5, $*_p$ fails) Artin-Schreier

Pf: $E = F(c)$ for any $c \in E \setminus F$.

Let $G = \mathrm{Gal}\, E/F = \langle \eta \rangle$, ~~Lagrange resolvent~~

$d_i \equiv \underline{(z_i, c)} := \sum_{j=0}^{p-1} \eta^j(c) z_i^j$; $i = 1, \dots, p$, $U_p = \{z_i\}$

$\eta d_i = d_i / z_i \Rightarrow \eta d_i^p = d_i^p \Rightarrow d_i^p \in F$, Hence

$E = F(c) = F(d_1, \dots, d_p) = F(d)$ where $d = d_i \notin F$

Vandermonde det of $(z_i^j) = \prod_{i>j}(z_i - z_j) \neq 0$ *

Lemma 4. (Extending base)

Let $f(x)\in F[x]$, $K\supset F \Rightarrow G_f/K \hookrightarrow G_f/F$.

pf: Let L splits f/K, then $L\supset E$ splits f/F.

Eg. $f(x)=\prod_1^n (x-r_i) \Rightarrow L=K(r_1,\dots,r_n)$, $E=F(r_1,\dots,r_n)$

Then $\eta\in \mathrm{Gal}\,L/K \mapsto \eta|_E \in \mathrm{Gal}\,E/K$ injectively since η is determined by its action on r_i's *

Def^n: (Normal closure).

Let $[E:F]<\infty$, then $E=F(a_1,\dots,a_n)$, and The splitting field K of $m_{a_1}(x)\cdots m_{a_n}(x)$ is normal

(if $\prod m_{a_i}(x)$ is ~~sep~~ then done; in general: Ex. 6)

Facts: (1) $\tilde K\supset E$ normal $\Rightarrow \tilde K \supseteq K' \cong K$ as splitting fields

(2) $K=K'$ gen by $\eta(E)$'s, $\eta\in \mathrm{Gal}\,K/F = G$

pf: $G\to \mathrm{Aut}_F K' = G'$ determines $H'\subset G'$ with $K'^{H'}=F \Rightarrow K'$ normal *

Lemma 5. (Reduction to Galois ext.)

Let $E=F(a_1,\dots,a_n)$, $\prod m_{a_i}(x)$ sep. with a root tower $F=F_1\subset\cdots\subset F_{r+1}=E$, $F_{i+1}=F_i(d_i)$, $d_i^{n_i}\in F_i$. Then the normal closure K of E/F has a root tower with same $\{n_i\}$ (repeated).

pf: K is gen. by $\eta_j(E)$, $\eta_j\in \mathrm{Gal}\,E/F$, $1\le j\le m$.

$\Rightarrow \eta_j(F_\cdot)$ is a root tower of $\eta_j(E)/F$

$\Rightarrow K=F(\eta_1(d_1),\dots,\eta_1(d_r),\dots,\eta_m(d_1),\dots,\eta_m(d_r))$ which obviously has a root tower as said *

Theorem (Galois): Let char $F=0$, $f(x)\in F[x]$.

Then $f(x)=0$ is solvable by rad $\Leftrightarrow G_f$ is solvable.

pf: $\Rightarrow$ By Lemma 5, $\exists\, K/F$ finite Galois, $\supset$ a splitting field E of f/F and has a root tower.

Let $n=\mathrm{l.c.m}(n_i)$, $z^n=1$ primitive.

$K(z)/F$ is Galois (if $K\leftrightarrow g(x)$, $K(z)\leftrightarrow g(x)(x^n-1)$)

Also we may rearrange the tower as

$F=F_1\subset F_2 := F_1(z)\subset F_3=F_2(d_1)\subset\cdots\subset K(z)$.

abelian by Lemma 1 all ab. by Lemma 2

Let $G_f=G=\mathrm{Gal}\,E/F$, $H=\mathrm{Gal}\,K(z)/F$,

$H_j := \mathrm{Gal}\,K(z)/F_j$ F_{i+1}/F_i Galois, ab.

Galois $\Rightarrow H_{i+1}\triangleleft H_i$ and H_i/H_{i+1} ab $\Rightarrow H$ solvable.

Now E/F Galois $\Rightarrow G\cong H/\mathrm{Gal}(K(z)/E)$ sol.

$$\begin{array}{c} K(z) \\ | \\ K \\ | \\ E \\ | \\ F \end{array} \quad H,\ G$$

$\Leftarrow$: Let E a splitting field of f/F, $G=G_f$

$n=|G|=[E:F]$, $F_1:=F$, $F_2:=F(z)$, $K:=E(z)$

Lemma 4 $\Rightarrow H:=\mathrm{Gal}\,E(z)/F(z)\subset \mathrm{Gal}\,E/F=G$

hence solvable, say $H=H_1\triangleright H_2\triangleright\cdots\triangleright H_{r+1}=1$.

$H_i/H_{i+1}\cong \mathbb{Z}_{p_i}$, hence $\leftrightarrow$ $F_2\subset\cdots\subset F_{r+2}=K$

$H_i=\mathrm{Gal}\,K/F_{i+1}$

$\Rightarrow F_{i+1}/F_i$ normal, gp $\cong \mathbb{Z}_{p_i}$

Since $F_i\supset F_2$ contains n-th (hence p_i-th) roots of 1, $p_i \mid n$

Lemma 3 $\Rightarrow F_{i+1}=F_i(d_i)$, $d_i^{p_i}\in F_i$ *

4.8 Two Simple Facts on Gal $\subset S_n$ acting on roots

Fact 1: Let char $F\neq 2$, E/F splits f, dist roots r_i

Then $G_f\cap A_n \leftrightarrow F(D)$, $D:=\prod_{i<j}(r_i-r_j)$

Fact 2: f simple roots. Then f irr. $\Leftrightarrow G_f$ trans. on $\{r_i\}$

4.9 General Eq'n of deg n

Had seen $g(x) := \prod^n (x - x_i) = x^n - t_1 x^{n-1} + \cdots (-1)^n t_n$

$E := F(x_1, \cdots, x_n)$ splits $g(x)$ over $F(t_1, \cdots, t_n) =: K$

with $G_g = S_n$. This is not sol. if $n \geq 5 \Rightarrow$

Thm (Ruffini-Abel) if char $F = 0$, then general eq'n of deg ≥ 5 is not sol. by radicals.

Example ($n=3$). $g(x) = x^3 - t_1 x^2 + t_2 x - t_3$

$G_g = S_3 \triangleright A_3 \triangleright 1$ sol. $A_3 \mapsto K(\sqrt{d})$.

Assume char $F \neq 2, 3$ contains $U_3 = \{1, w, w^2\}$

let $y_i = x_i - \frac{1}{3} t_1$, get $f(y) = y^3 + py + q$

$D^2 =: d = -4p^3 - 27q^2$ (cf. J. p. 258-259) $d \in \mathbb{Z}[t_1, \cdots, t_n]$.

We seek for E cyclic ($A_3 \simeq \mathbb{Z}_3$) over $K(\sqrt{d})$:

ie. join a root of Lagrange resolvent (Lem 3).

$$* \begin{cases} d_1 = y_1 + y_2 w + y_3 w^2 \\ d_2 = y_1 + y_2 w^2 + y_3 w^4 = y_1 + y_3 w + y_2 w^2 \\ d_3 = y_1 + y_2 + y_3 = 0 \end{cases}$$

$\Rightarrow d_1^3 = \sum y_i^3 - \frac{3}{2} u + \frac{3}{2}\sqrt{-3}\sqrt{d} + 6 y_1 y_2 y_3$

where $u := (y_1^2 y_2 + y_2^2 y_3 + y_3^2 y_1) \pm (y_1 y_2^2 + y_2 y_3^2 + y_3 y_1^2)$

$\sqrt{d}$ = "−" sign (anti-sym)

$$\Rightarrow \begin{cases} d_1^3 = -\frac{27}{2} q + \frac{3}{2}\sqrt{-3d} \\ d_2^3 = -\frac{27}{2} q - \frac{3}{2}\sqrt{-3d} \end{cases} \quad \text{under } d_1 d_2 = \sum y_i^2 - \sum_{i<j} y_i y_j = -3p$$

Finally, it is easy to solve y_i from $*$ via

Cardan: $y_1 = \frac{1}{3}(d_1 + d_2)$, $y_2 = \frac{1}{3}(w^2 d_1 + w d_2)$, $y_3 = \frac{1}{3}(w d_1 + w^2 d_2)$

4.10 Eq'n /$\mathbb{Q}$ with $G_f \simeq S_n$

Lemma: $G \subset S_p$. if $G \ni \sigma_1, \sigma_2$ (p: prime) with ord $\sigma_1 = p$, ord $\sigma_2 = 2$ then $G = S_p$.

pf: After reordering, $\sigma_1 = (1\ 2 \cdots p)$, $\sigma_2 = (1\ i)$ since $\sigma_1^i = (1\ i \cdots)$, may further assume $i = 2$. hence done $*$

Thm: Let $f(x) \in \mathbb{Q}[x]$ irr. deg $f = p$: prime. if $f(x) = 0$ have exactly 2 roots $\notin \mathbb{R}$ then $G_f \cong S_p$

pf: Let $f(x) = \prod_{i=1}^p (x - r_i)$ in $\mathbb{C}[x]$

$E = \mathbb{Q}(r_1, \cdots, r_p)$ then $p \mid [E:\mathbb{Q}]$

Sylow (or Cauchy) $\Rightarrow \exists \sigma \in G_f$, ord $\sigma = p$.

Now "bar" interchange $\mathbb{C} \setminus \mathbb{R}$ roots, ord "$-$" $= 2$.

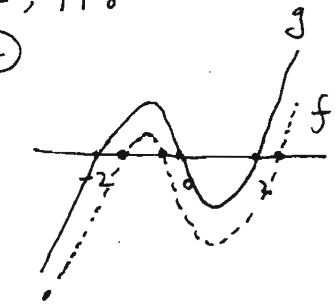
hence $G_f \simeq S_p$ by lemma $*$

Example: $f(x) = (x^2 + \underset{\vee\, 0}{2}) \cdot (x+2) x (x-2) - 2 = g(x) - 2$

$= x^5 - 2x^3 - 8x - 2$

Now for $p = 2$, $p \nmid 1$, $p \mid 2$, $p \mid 8$

but $p^2 \nmid 2$



Eisenstein criterion

$\Rightarrow f(x)$ is irr in $\mathbb{Q}[x]$.

in general, need to take $x^2 + m$ with m large & even

to make sure not all roots real.

$\Rightarrow G_f \simeq S_5$ $*$

This works for every odd degree $k \geq 5$, if k prime then get $G_f \simeq S_k$ $*$

4.11 Cyclotomic fields / constr of n-gons

Thm: Let $z_1 = 0$, $z_2 = 1$, $F = (z_1, \cdots, z_n, \bar{z}_1, \cdots, \bar{z}_n)$

Then $z \in C(z_1, \cdots, z_n) \iff z$ is alg. $/F$ and the normal closure K of $F(z)/F$ has dim $2^k /F$.

pf: $\Rightarrow$: Consider

$$\underset{\substack{\| \\ L_0}}{F} \subset \underset{\substack{\| \\ L_1}}{F(u_1)} \subset F(u_1, u_2) \subset \cdots \subset \underset{\substack{\| \\ L_r = L}}{F(u_1, \cdots, \overset{z}{\underset{\wedge}{}} u_r)}$$

Lemma 5 $\Rightarrow$ may assume L/F Galois ($n_i = 2$)

$L \supset K \Rightarrow [K:F] \mid [L:F] = 2^l \Rightarrow [K:F] = 2^k$.

$\Leftarrow$: let $G = \mathrm{Gal}\, K/F$, $|G| = 2^k \Rightarrow G$ solvable

$G = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{t+1} = 1$, $G_i / G_{i+1} \simeq \mathbb{Z}_2$

fund. thm: $F = F_1 \subset F_2 \subset \cdots \subset F_{t+1} = K$

$F_{i+1} = F_i(u_i)$ with $u_i^2 + a u_i + b = 0$

$= F_i(v_i)$ with $v_i^2 \in F_i$ $\left(v_i = u_i + \frac{a}{2}\right)$ *

~~Thm (Gauss)~~ A regular n-gon is constr*.

$\iff n = 2^e p_2 \cdots p_s$ where p_i's are Fermat prime (distinct).

*ie. Let $\zeta_n = e^{2\pi i/n}$, $\zeta_n \in C(0,1)$.

pf: Let $n = 2^{e_1} p_2^{e_2} \cdots p_s^{e_s}$; $p_1 = 2$

$\varphi(n) = \varphi(2^{e_1}) \cdots \varphi(p_s^{e_s}) = \prod p_i^{e_i - 1}(p_i - 1)$

$= 2^m \iff e_i = 1$ and p_i is Fermat for $i \neq 1$.

let $\lambda_n(x) := \prod_{\substack{r:\text{ primitive} \\ n\text{-th root of } 1}} (x - r)$, $\deg \lambda_n = \varphi(n)$.

Gauss' thm follows from: *

Thm: $\lambda_n(x) \in \mathbb{Z}[x]$ is irr. (in $\mathbb{Q}[x]$)
ie. $\lambda_n(x) = m_{\zeta_n}(x)$ min. poly.

Pf: By def'n, we get $x^n - 1 = \prod_{d|n} \lambda_d(x)$.

$\lambda_d(x) \in \mathbb{Q}[x]$ since it is inv. under $\mathrm{Gal}\, \mathbb{Q}(\zeta_n)/\mathbb{Q}$

By induction, we see $\lambda_n(x) \in \mathbb{Z}[x]$ since

$$\underset{\text{monic}}{x^n - 1} = \lambda_n(x) \underbrace{\prod_{d|n,\, d<n} \lambda_d(x)}_{\in \mathbb{Z}[x]}$$ and use div.

If $\lambda_n(x) = f(x) g(x)$ in $\mathbb{Z}[x]$ f irr. monic $= m_{\zeta_n}(x)$

Let $f(\zeta) = 0$, p a prime $\nmid n$

if $g(\zeta^p) = 0$ then ζ is a root of $g(x^p)$

$\Rightarrow f(x) \mid g(x^p)$. write $g(x^p) = f(x) \cdot h(x)$

Mod p: in $\mathbb{Z}_p$ get $\bar{g}(x^p) = \bar{f}(x) \bar{h}(x)$
$\quad \| \; \bar{g}(x)^p$

$\Rightarrow \bar{g}, \bar{f}$ has a common root $\Rightarrow \bar{\lambda}_n$ has mult. root

$\Rightarrow x^n - \bar{1}$ has mult root, but $\bar{n} x^{n-1} \neq 0$ ✗

hence $g(\zeta^p) \neq 0$, ie. $f(\zeta^p) = 0$ $\forall p \nmid n$

Induction $\Rightarrow f(\zeta^{p^r}) = 0$ $\forall r \in \mathbb{N}_{>0}$

$\Rightarrow f(\zeta^{p_1^{r_1} \cdots p_s^{r_s}}) = f\left(\left(\zeta^{p_1^{r_1} \cdots p_s^{r_s - 1}}\right)^{p_s}\right) = 0$

$\forall p_i \nmid n$, $r_i \in \mathbb{N}_{>0}$.

ie. $f(\zeta^k) = 0$ $\forall$ $1 \leq k < n$, $\gcd(k,n) = 1$ *

Examples: $\lambda_1(x) = x - 1$, $\lambda_2(x) = (x^2 - 1)/\lambda_1 = x + 1$

$\lambda_3(x) = (x^3 - 1)/\lambda_1 = x^2 + x + 1$, $\lambda_4(x) = (x^4 - 1)/\lambda_1 \lambda_2 = x^2 + 1$

$\lambda_6(x) = (x^6 - 1)/\lambda_1 \lambda_2 \lambda_3 = x^2 - x + 1$, $\lambda_{12} = \underset{\text{irr}}{\underline{x^4 - x^2 + 1}}$

But $\lambda_{105 = 3 \cdot 5 \cdot 7} = x^{48} \cdots -2x^{41} + \cdots 1$. The 1st $\neq 0, \pm 1$.

The str. of $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, i.e. $G_{x^n} \cong U_n$

Since $U_n = U(\mathbb{Z}/n) = \prod U(\mathbb{Z}/p_i^{e_i})$, may set $n = p^e$.

Prop 1. If p is odd prime, then $(\mathbb{Z}_{p^e})^\times \cong (\mathbb{Z}_{p^{e-1}(p-1)}, +)$

pf: It is easy to see that

$\operatorname{ord}(1+p) = p^{e-1}$. Since $|(\mathbb{Z}_{p^e})^\times| = p^{e-1}(p-1)$

So the p-Sylow is cyclic.

consider the ring homo $\phi : \mathbb{Z}_{p^e} \twoheadrightarrow \mathbb{Z}_p$

$\Rightarrow \phi : (\mathbb{Z}_{p^e})^\times \twoheadrightarrow \mathbb{Z}_p^\times \Rightarrow |\operatorname{Ker}\phi| = p^{e-1}$

cyclic order $= p-1$

$\forall$ prime $q \neq p$, q-Sylow of $\mathbb{Z}_{p^e}^\times \cong q$-Sylow of $\mathbb{Z}_p^\times$

hence is also cyclic.

$\Rightarrow \mathbb{Z}_{p^e}^\times \cong$ product of Sylow $=$ cyclic ※

~~Prop 2.~~ U_2, U_{2^2} are cyclic (trivial)

and $\mathbb{Z}_{2^e}^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{e-2}}$ $\forall e \geq 3$.

pf: Easy to check $\operatorname{ord}(1+2^2) = 2^{e-2}$

i.e. $H := \langle \bar{5} \rangle \leq \mathbb{Z}_{2^e}^\times$, $|H| = 2^{e-2}$

Now $x^2 - 1 = 0$ has 4 roots $1, -1, 1+2^{e-1}, -1+2^{e-1}$

hence $\mathbb{Z}_{2^e}^\times$ is a direct prod of ≥ 2 cyclic gps

$|\mathbb{Z}_{2^e}^\times| = 2^{e-1} \Rightarrow \mathbb{Z}_{2^e}^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{e-2}}$ ※

4.12 Lindemann-Weierstrass Thm (skip)

$u_1, \dots, u_n \in \bar{\mathbb{Q}}$, lin. indep $/\mathbb{Q} \Rightarrow e^{u_i}$ alg. ind. $/\bar{\mathbb{Q}}$.

Cor: $u \in \bar{\mathbb{Q}} \Rightarrow e^u \notin \bar{\mathbb{Q}}$, hence $e \notin \bar{\mathbb{Q}}$.

$e^{\pi i} = -1 \in \mathbb{Q} \Rightarrow \pi i \notin \bar{\mathbb{Q}} \Rightarrow \pi \notin \bar{\mathbb{Q}}$

Cor: $\pi, \sqrt{\pi}$ is not constructible. (圓化方).

4.13 Finite Fields

Thm: for $q = p^m$, $\exists !$ F, up to isom, st $|F| = q$.

Pf: Any finite field F satisfies $x^q - x = 0$ since $x^{q-1} = 1$ in $F^\times$. The uniqueness follows from uniq of splitting field up to isom ※

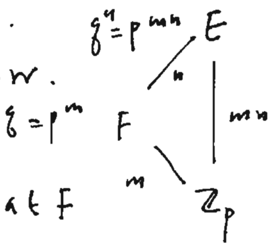
Thm': $|F| = q$, $E \supset F$ st $[E:F] = n$. Then E/F is cyclic, $Gal\ E/F = \langle \eta \rangle$, $\eta : a \mapsto a^q$.

Pf: Let $q = p^m$. Thm' holds for $m = 1$:

then $\eta = Fr : a \mapsto a^p \in Gal\ E/F = \mathbb{Z}_p$

$\langle Fr \rangle \cong \mathbb{Z}_n \Rightarrow \langle Fr \rangle = Gal\ E/\mathbb{Z}_p$.

for general $m \in \mathbb{N}$: use Galois' corr.



$Gal\ E/F \subset Gal\ E/\mathbb{Z}_p = \langle Fr \rangle$

is gen by $Fr^{m'}$. Since $a^{p^m} = a$, $a \in F$

$\Rightarrow m' | m \Rightarrow m' = m$ by Thm ※

Cor 1. $E \supset K \supset F \iff |K| = q^{n'}$ with $n' | n$.

(Since $n = [E:F] = [E:K]\cdot[K:F] = [E:K]\cdot n'$)

Cor 2. $|F| = q$, $N(n,q) = \#(\text{monic irr. deg } n \text{ in } F[x])$

Then $N(n,q) = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d}) q^d$. (Gauss)

Pf: $x^{q^n} - x = \prod g(x)$ all monic irr $\deg | n$

$\Rightarrow q^n = \sum_{d|n} \underline{N(d,q)\, d}$ by Cor 1 applied to splitting field of g

$\Rightarrow n N(n,q) = \sum_{d|n} \mu(\frac{n}{d}) q^d$ by Möbius inv ※

Cor 3. $E = F(z)$ for some z.

Pf: Indeed, $E^\times$ is finite and cyclic $= \langle z \rangle$ ※

4.14 Special Basis

Thm (Primitive elements). Let $[E:F]<\infty$.
Then $E=F(z) \Leftrightarrow \#(E\supset K\supset F)<\infty$ (Steinitz)

pf: $\Rightarrow$: Let $f(x)=m_z^F(x)\in F[x]$, $g(x)=m_z^K(x)\in K[x]$
Then $g(x)\mid f(x)$.
Let $E\supset K'\supset F$ gen by coeff of $g(x)$ $\Rightarrow$ $K'\subset K$
$\Rightarrow K'=K$ (since $E=F(z)=K(z)=K'(z)$, $[E:K]=\deg g=[E:K']$)
i.e. $K\leftrightarrow g$ $\Rightarrow$ finite #. as splitting fields

$\Leftarrow$: May assume $|F|=\infty$.
Consider $F(u,v)\supset F(u+av)\supset F$, $a\in F$
$\exists\, a\neq b$ st $F(u+av)=F(u+bv)$
clearly then $v\in F(u+av)\Rightarrow u$ $\Rightarrow$ let $z=u+av$
Since E/F is f.g. induction $\Rightarrow$ Thm ✱

Cor. E/F f.d. & sep $\Rightarrow$ $\exists$ primitive element.
pf: Take normal closure $K\supset E\supset F$, K/F Galois
$\exists$ finite sub field $\leftrightarrow$ finite sub gps in Gal K/F ✱

~~Thm~~ (~~Dedekind independence of characters~~)
$\chi_i: H\to F^\times$ hom. $\sum_{i=1}^{n} a_i\chi_i=0 \Rightarrow a_i=0\ \forall i$.
monoid (e.g. $F_1^\times\to F_2^\times$)
pf: Induction on n and prune by ✱.

Def'n Let K/F Galois, $G=\{\eta_1,\cdots,\eta_n\}$, $|G|=n$
$K=F(z)\Leftrightarrow \eta_1(z),\cdots,\eta_n(z)$ distinct.
It is called a Normal Basis if l-indep.

Thm: K/F finite Galois $\Rightarrow$ $\exists$ normal basis.

The pf uses Dedekind's thm and is left for reading

4.16 Mod p Reduction

Thm (Tate): Let $f(x)\in\mathbb{Z}[x]$ monic, $E/\mathbb{Q}$ splits f. f_p has* ~~dist roots in E_p~~ (splitting f_p) $/\mathbb{Z}_p$
(a) $\exists\,\psi: D\to E_p$, $D=\mathbb{Z}[r_1,\cdots,r_n]$, $f(x)=\prod_i^n(x-r_i)$, $r_i\in E$
(b) Any ψ gives $r_i\longrightarrow\psi(r_i)$ root of f_p, 1-1 onto
(c) Any ψ,ψ', $\exists\,\sigma\in$ Gal $E/\mathbb{Q}$ st $\psi'=\psi\sigma$.

pf (a): $r_i\neq$ since $d(f_p)\neq 0$
· it is clear that $D=\sum_{e_i=0}^{n-1}\mathbb{Z}\, r_1^{e_1}\cdots r_n^{e_n}$
f.g. and Tor $D=0$ $\Rightarrow$ free $D=\mathbb{Z}u_1\oplus\cdots\oplus\mathbb{Z}u_N$
$E\supset\mathbb{Q}D\supset\mathbb{Q}$ and $r_i\in D$ $\Rightarrow$ $E=\mathbb{Q}D$ with base $u_i/\mathbb{Q}$
alg. subring $\Rightarrow$ sub field (why?)
Now $|D/pD|=p^N$, $\exists$ max ideal M/pD ($D\supsetneq M\supset pD$)
$\nu: D\twoheadrightarrow D/M\simeq(D/pD)/(M/pD)$ finite field$/\mathbb{Z}_p$
$\mathbb{Z}\twoheadrightarrow\mathbb{Z}_p$ $\simeq\mathbb{Z}_p[\bar r_1,\cdots,\bar r_n]$, $\bar r_i=r_i+M$
Then $^{\oplus}\ \nu(f(x))=:\bar f(x)=\prod_i^n(x-\bar r_i)=f_p(x)$. $=\nu(r_i)$
i.e. we have constructed the splitting field $D/M\simeq E_p$
(b) trivial (by $\oplus$) $\psi:=\nu$ ✱
(c): $G=$ Gal $E/\mathbb{Q}=\{\sigma_1,\cdots,\sigma_N\}$ gives $\psi_j=\psi\sigma_j$
if $\exists\,\psi_{N+1}$. Then Dedekind $\Rightarrow$ l-ind of $\psi_1,\cdots,\psi_{N+1}$
But $\exists\,(a_1,\cdots,a_{N+1})\neq 0$ st. $\sum_{i=1}^{N+1}a_i\psi_i(u_j)=0$, $1\le j\le N$
$a_i\in E_p$ $\Rightarrow \sum a_i\psi_i=0$ ✗

~~Cor/Thm (Dedekind)~~: If * and f_p factors into irr. factors of degree $n_1,\cdots,n_r$ in $\mathbb{Z}_p[x]$, then G_f contains a cycle of type $(n_1,\cdots,n_r)$.
pf: Indeed, $G_{f_p}=\langle Fr\rangle\subseteq G_f$ on roots:
via $\pi:=Fr\mapsto\pi\psi=\psi\sigma$, i.e. $\sigma=\psi^{-1}\pi\psi$ ✱

Example : $f(x) = x^5 - x - 1$, ($d = 19 \times 151$, $G \not\subset A_5$)

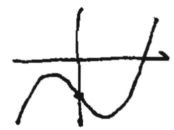
In $\mathbb{Z}_2[x]$, $\bar{f}(x) = (x^2+x+1)(x^3+x^2+1)$

$\Rightarrow (ab)(cde) \in G \Rightarrow (ab) \in G$ (take cubic)

In $\mathbb{Z}_3[x]$ $\bar{f}(x)$ irred : if $\bar{f} = hg$, $\deg h = 2$

then $h(x) | (x^9 - x) \Rightarrow h | (x^4 \pm 1) \Rightarrow *$

$\Rightarrow G \ni 5$ cycle $\Rightarrow G \simeq S_5$.



classical Algorithm / Galois resolvent

Let $f(x) = \prod_1^n (x - r_i)$, $\theta = u_1 r_1 + \cdots + u_n r_n$

$$\varphi(x,u) := \prod_{\sigma \in S_n} (x - \sigma(\theta)) \in F[x,u]$$

$$= \underbrace{\varphi_1(x,u) \cdots \varphi_\ell(x,u)}_{\text{acts on } u_i}$$ irr. Sym fcn of r_i

Thm : $G_f \simeq G := \{ \sigma \in S_n \mid \sigma\varphi_1 = \varphi_1 \}$, or any φ_i .

pf : Say , $(x - \theta) | \varphi_1$. Let σ_r = "σ acts on r_i"

$\Rightarrow \sigma\sigma_r\theta = \theta$ or $\underline{\sigma_r \theta = \sigma^{-1}\theta}$.

if $\sigma \in G$ then it maps a linear factor of φ_1 to another one in φ_1 , This also characterizes $\sigma \in G$.

But $\sigma_r \in G_f$ is characterized by sending θ to its conjugate , hence the same irred equation as θ . ie. $\sigma_r(x - \theta) | \varphi_1$

$\Rightarrow \sigma^{-1} \in G \Rightarrow \sigma \in G$ \#

Cor / Thm : Mod $\mathfrak{p}$ reduction for $f(x) \in R[x]$, R UFD.

$\Rightarrow G_{\bar{f}} \subset G_f$ if $\bar{f}$ has no double root .

Rmk (1) G_i for φ_i are conjugate to G , $G_i = \tau G \tau^{-1}$ if $\varphi_i = \tau\varphi_1$.

(2) For $f(x) \in \mathbb{Z}[x]$, fact algorithm exists. How?

4.15 Trace / Norm & Hilbert's Satz 90

Def'n : E/F Galois $G = \{\eta_1 = 1, \cdots \eta_n\}$

$T_{E/F}$ $u \mapsto \sum \eta_i(u)$ $E \to F$ F-linear

$N_{E/F}$ $u \mapsto \prod \eta_i(u)$ $E^\times \to F^\times$

eg. $E = \mathbb{Q}(\sqrt{m})$, $T(a + b\sqrt{m}) = 2a$. $N(a+b\sqrt{m}) = a^2 - b^2 m$.

Q : Im N = ? Ex. $\mathbb{Q}(\sqrt{-1})$.

~~Thm (Hilbert)~~ Let E/F cyclic , $G = \langle \eta \rangle$

Then $N(u) = 1 \iff u = v \cdot \eta(v)^{-1}$ for some $v \in E$.

Thm' (Galois cohomology) : E/F finite Galois

$G = \mathrm{Gal}\, E/F \longrightarrow E^\times ; \eta \mapsto a_\eta$ be a map st

$a_{\zeta\eta} = a_\zeta \zeta(a_\eta)$ (twisted hom. cocycle condi)

Then $\exists\, v \in E^\times$ st. $a_\eta = v \cdot \eta(v)^{-1}$. (co-boundary)

pf : $\exists\, w \in E$ st. $\underset{\text{constructive}}{v} := \sum_{\eta \in G} a_\eta \eta(w) \neq 0$ by Dedekind l-ind.

$\Rightarrow \zeta(v) = \sum_\eta \zeta(a_\eta)(\zeta\eta)(w)$

$= \left(\underline{\sum_\eta a_{\zeta\eta}(\zeta\eta)(w)}\right) a_\zeta^{-1} = v\, a_\zeta^{-1}$ $\forall \zeta \in G$ \#

~~pf of Hilbert~~ : Let $N(u) = 1$. $G = \langle \eta \rangle \simeq \mathbb{Z}_n$.

Define $u_{\eta^i} = u \cdot \eta(u) \cdot \eta^2(u) \cdots \eta^{i-1}(u)$, $1 \le i \le n$.

Then $u_{\eta^j}\, \eta^j(u_{\eta^i}) = u\, \eta(u) \cdots \eta^{j-1}(u)$
$\eta^j(u)\, \eta^{j+1}(u) \cdots \eta^{i+j-1}(u)$

$= u_{\eta^{i+j}}$ if $i + j \le n$.

if $i + j > n$ this also holds since $N(u) = 1$.

Thm' $\Rightarrow u = u_\eta = v\eta(v)^{-1}$ \#

Structure of Cyclic ext'n.

Thm: E/F cyclic of dim $= n$, and $F \supset n$ dist. root of 1

Then $E = F(u)$ with $u^n \in F$. (gen Lemma 3)

pf: Let z be a prim. root of 1. $z \in F \Rightarrow N(z) = z^n = 1$.

so $z = u\, \eta(u)^{-1}$, $G = \langle \eta \rangle$, $u \in E$.

$\Rightarrow \eta(u) = z^{-1} u \Rightarrow \eta(u^n) = \eta(u)^n = z^{-n} u^n = u^n$

$\Rightarrow u^n \in F$.

Also $\eta^i(u) = z^{-i} u$ all dist. under G

$\Rightarrow \deg m_u(x) = n = |G| \Rightarrow E = F(u)$ ✱

Additive Analogue:

Thm'-A: $G \to E: \eta \mapsto d_\eta$ st. $d_{\xi\eta} = d_\xi + \xi(d_\eta)$

$\Rightarrow \exists\, c \in E$ st. $d_\eta = c - \eta(c)$, $\forall \eta \in G$.
constructive

pf: $\exists u$ st $T(u) \neq 0$. Let $c = \left(\sum_\eta d_\eta\, \eta(u)\right)/T(u)$

$c - \xi(c) = \sum_\eta \left(d_\eta\, \eta(u) - \xi(d_\eta)(\xi\eta)(u)\right)/T(u)$

$= \sum_{\eta \in G} \left(\cancel{d_\eta \eta(u)} + d_\xi\, (\xi\eta)(u) - \cancel{d_{\xi\eta}\, (\xi\eta)(u)}\right)/T(u)$

$= d_\xi\, T(u)/T(u) = d_\xi$ ✱

cor / Thm-A: Let E/F cyclic, $G = \langle \eta \rangle$, $d \in E$

$T(d) = 0 \Rightarrow d = c - \eta(c)$ for some $c \in E$.

pf: $d_{\eta^i} := d + \eta(d) + \cdots + \eta^{i-1}(d)$, apply Thm'-A ✱

Rmk: here we do not need cond. on roots of 1.

Thm (Artin-Schreier): Let char $F = p \neq 0$,

E/F cyclic, dim $= p \Rightarrow E = F(c)$, $c^p - c \in F$.

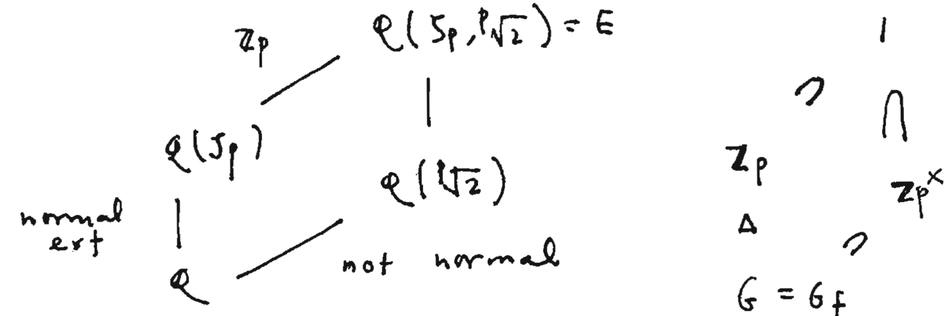
pf: $T(1) = 0 \Rightarrow \exists c$ st $1 = c - \eta(c) \Rightarrow \eta^i(c) = c - i$ ‡

$\Rightarrow E = F(c)$ and $\eta(c^p - c) = (c-1)^p - (c-1) = c^p - c \in F$ ✱

Examples of Galois Groups

I. More on "$x^n - a$" (realizations of Lem 1, 2, 3)

Example: $f = x^p - 2$ / $\mathbb{Q}$ (cf. J (4.5)-4, (4.7)-2)



$G/\mathbb{Z}_p \simeq \mathrm{Gal}\, \mathbb{Q}(\zeta_p)/\mathbb{Q} \simeq \mathbb{Z}_p^\times \simeq (\mathbb{Z}_{p-1}, +)$.

in fact, $G \simeq \mathbb{Z}_p \cdot \mathrm{Aut}\, \mathbb{Z}_p \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$

i.e. $\tau_{ab}(k) = ak + b$ $\quad (\overset{\psi}{b}, a)$

gp of holomorphy: $\mathrm{Hol}(H) := H_L \cdot \mathrm{Aut}(H)$

roots $(r_1, \cdots, r_p) = (\sqrt[p]{2}, \sqrt[p]{2}\,\zeta_p, \sqrt[p]{2}\,\zeta_p^2, \cdots, \sqrt[p]{2}\,\zeta_p^{p-1})$

$\mathbb{Z}_p = \langle \cdot \zeta_p \rangle: \zeta_p^k \mapsto \zeta_p^{k+b}$ $\longrightarrow$

$\mathbb{Z}_p^\times =$ power : $\zeta_p^k \mapsto (\zeta_p^k)^a$ $\uparrow$

Clearly, $\mathbb{Q}(\sqrt[p]{2})$ is the fixed field of $\mathbb{Z}_p^\times$.

Q: How about $x^6 - 2$, $x^8 - 2$?

Ex (Remark): for $f(x) = x^n + px + q$ $\quad \left(\begin{array}{l} \eta_n = 1 \text{ if } n \equiv 0, 1 \bmod 4 \\ = -1 \text{ otherwise} \end{array} \right)$

$\underline{d = \eta_{n+1}\, n^n q^{n-1} - \eta_n (n-1)^{n-1} p^n}$ $\quad \left(d := \prod_{i>j} (r_i - r_j)^2 = D^2\right)$

clearly $D = \begin{vmatrix} 1 & \cdots & 1 \\ r_1 & \cdots & r_n \\ r_1^{n-1} & \cdots & r_n^{n-1} \end{vmatrix}$ $\quad$ ($i > j$ conv.) $= \det V$

$\Rightarrow d = \det V^t V = \begin{vmatrix} n & s_1 & \cdots & s_{n-1} \\ s_1 & & & \vdots \\ s_{n-1} & \cdots & & s_{2n-2} \end{vmatrix}$, $\quad s_i = r_1^i + \cdots + r_n^i$ Newton Sym poly.

II. All transitive subgps in S_5 (cf. (4.16)-6) are realized as Galois gps $/\mathbb{Q}$

$\mathbb{Z}_5$ $\quad x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$

from $x^{11} - 1 = (x-1)(x^{10} + x^9 + \cdots + x + 1)$

$\mathbb{Z}_{10} \supset \mathbb{Z}_5$, consider m_α, $\underline{\alpha = x + \frac{1}{x}}$. $G \cong \mathbb{Z}_{10}$

• D_{10} (or D_5 in J)

$x^5 - 5x + 12$ $\quad d = 2^{12} 5^6 \Rightarrow G_f \subset A_5$, In $\mathbb{Z}_3$:

$= x(x^2 + x - 1)(x^2 - x - 1)$ $\quad G_{\bar{f}} = \mathbb{Z}_2 \subset G_f$. So D_{10} or

$W = \mathbb{Z}_5 \cdot \mathbb{Z}_5^\times$ $\quad A_5$. [J Ex (4.16)-7 $\Rightarrow D_{10}$]

$x^5 - 2$ or any $x^5 - a$ irr. as studied in I.

A_5 $\quad x^5 + 20x + 16$ $\quad d = 2^{16} 5^6 \Rightarrow G_f \subset A_5$

In $\mathbb{Z}_7 \Rightarrow \bar{f}(x) = (x+2)(x+3)\underbrace{(x^3 + 2x^2 - 2x - 2)}_{\text{irred}}$

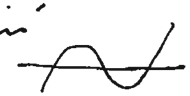
$\Rightarrow \exists$ 3-cycle $\in G_f \Rightarrow A_5$

S_5 $\quad$ This is true for "generic eq'n":

3 $\mathbb{R}$-roots $\cdot$ $(x^2+2)x(x-2)(x+2) - 2 = x^4 - 6x^2 + 8x - 2$

$\cdot$ or more simply $\quad x^5 - 4x + 2$

irred by Eisenstein's criterion



1 real root. $\quad x^5 - x - 1$

By mod 2, 3 as studied in mod p example.

Final remarks:

(1) All solvable transitive gp in S_p have the form $W \cong \mathbb{Z}_p \cdot H$ for $H \subset \mathbb{Z}_p^\times$ acts as $ak + b$

(2) Shafarevich: All appear as $G_f/\mathbb{Q}$. (1954).