

Apr 2

①

MAT401

$\{\text{field extension}\} \longleftrightarrow \{\text{groups}\}$   
 $\{\text{extension by radicals}\} \longrightarrow \{\text{solvable groups}\}$   
 $S_{\mathbb{Q}}(3x^5 - 15x + 5) \longrightarrow S_5 \text{ (not solvable)}$

The Fundamental Theorem (char  $F=0$ )

If  $E/F$  is a splitting field,  
 $\{K : E/K/F\} \longleftrightarrow \{H : H < \text{Gal}(E/F)\}$

$$K \longmapsto \text{Gal}(E/K)$$

$$E_H \longleftarrow H$$

Given

 $E/F$ 

$$E \longleftrightarrow \text{Gal}(E/E) = \{e\}$$

$$[E:K] = |H| \wedge \text{(above is subgroup)}$$

$$K \longleftrightarrow \text{Gal}(E/K) = H$$

$$[K:F] = [\text{Gal}(E/K) : \text{Gal}(E/F)] \wedge \text{(above is subgroup)}$$

$$F \longleftrightarrow \text{Gal}(E/F) = G$$

If  $K$  is splitting, then

$H$  is normal &

$$\text{Gal}(K/F) = G/H$$

$$= \frac{\text{Gal}(E/F)}{\text{Gal}(E/K)}$$

Theorem: If  $E$  is a splitting field of  $x^n - a = 0$  over  $F$ , then  $\text{Gal}(E/F)$  is solvable.

$\text{Gal}(S_F(x^n - a) / F)$  is solvable.

Def'n: A primitive root of unity of order  $n$  is an element  $w \in E$  s.t.  $w^n = 1$  & if  $\eta^n = 1$ , then  $\eta = w^k$  for some  $k$ .

Ex:  $n=4$ ,  $F = \mathbb{C}$

roots of unity of order 4 are  $1, -1, i, -i$

are roots of  $x^4 - 1 = 0$

powers of  $1$  are  $1$  so not primitive

powers of  $-1$  are  $1$  and  $-1$  so not primitive

(but primitive for  $n=2$ )

powers of  $i$  are  $i, i^2 = -1, i^3 = -i, i^4 = 1$  so

it is primitive

powers of  $-i$  are  $-i, (-i)^2 = -1, (-i)^3 = i, (-i)^4 = 1$

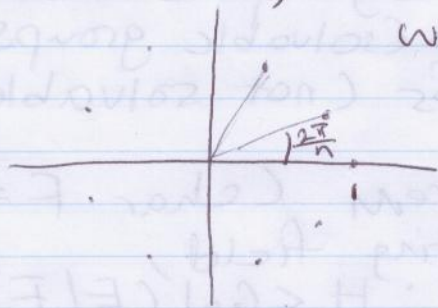
so it is primitive.



General  $n$ ,  $F = \mathbb{C}$

$$w = e^{2\pi i/n} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$$

is primitive.



If  $w$  is a primitive root of unity of order  $n$ , then the other roots of unity are  $w^0, w^1, w^2, \dots, w^{n-1}$

Proof of theorem

Case I:  $F$  already contains  $w$ , a primitive root of unity of order  $n$ .

Let  $b$  be some root of  $x^n - a = 0$ ;  
i.e.  $b^n = a$ .

Then  $b, wb, w^2b, \dots, w^{n-1}b$  are all roots of  $x^n - a = 0$ , so  $E = F(b, wb, w^2b, \dots) = F(b)$ .

Reminder: If  $\sigma \in \text{Gal}(E/F)$ ,  $b$  is a root of  $f \in F[x]$  then  $\sigma b$  is also a root of  $f$ .

If  $\sigma \in \text{Gal}(E/F)$ , then  $\sigma b = w^k b$  for some  $k$ , and that determines  $\sigma$ .

Likewise if  $\tau \in \text{Gal}(E/F)$  then  $\tau b = w^j b$  for some  $j$ .  
 $\sigma \tau b = \sigma(w^j b) = \sigma(w^j) \sigma(b) = w^j w^k b = w^{j+k} b$

$$\tau \sigma b = \tau(w^k b) = w^k w^j b = w^{k+j} b$$

so  $\sigma \tau = \tau \sigma$  so

$\text{Gal}(E/F)$  is abelian and hence solvable.

Case II:  $w \notin F$ .

Debt: Any field has an extension that contains a primitive root of unity

- Obvious for subfields of  $\mathbb{C}$



Apr 2

$E = F(W)$  let  $b \in E$  be a root of  $x^n - a = 0$   
 $E = F(W)$  Then in  $E(W)$ , the roots of  $x^n - a = 0$   
 are  $b, wb, \dots$  but  $E$  was splitting  
 field of  $x^n - a$ ,  $S_F(x^n - a)$ , so  
 $b, wb, w^2b \dots \in E$   
 $\Rightarrow \frac{wb}{b} \in E \Rightarrow w \in E$

So, the inclusions picture is  $\{E\}$   $\uparrow$   $\{F(W)\}$   $\uparrow$   $\{F\}$   
 the splitting field of  $x^n - 1$  over  $F$   $\uparrow$   $G$   $\uparrow$   $\{F\}$   $\uparrow$   $\{F\}$   
 Abelian by previous case  $\uparrow$  Abelian

Claim:  $\text{Gal}(F(W)/F)$  is Abelian

Pf:  $\sigma, \tau \in \text{Gal}(F(W)/F)$

$$\begin{aligned}
 \sigma W &= w^j & \text{so } \tau \sigma W &= \tau(w^j) = (\tau(w))^j = (w^k)^j = w^{kj} \\
 \tau W &= w^k & & \\
 \sigma \tau W &= \sigma(w^k) = (\sigma(w))^k = (w^j)^k = w^{kj}
 \end{aligned}$$

$$\therefore \sigma \tau = \tau \sigma \quad \square$$

$H$  &  $G/H$  are Solvable so  $G$  is Solvable.

Theorem: Let  $f \in F[x]$ . If  $f$  splits over some field  $F(a_1, a_2, \dots, a_k)$  s.t.  $\forall j, a_j^{n_j} \in F(a_1, \dots, a_{j-1})$  i.e.  $a_i^{n_i} \in F()$ . Then  $\text{Gal}(E/F)$ , where  $E$  is a splitting field for  $f$  over  $F$ , is solvable.

Proof: Let  $E_0 = F$ ,  $E_1$  a splitting field of  $x^{n_1} - a_1^{n_1}$  over  $E_0$ .  $F(a_1) \subset E_1$

Let  $E_2$  be a splitting field of  $x^{n_2} - a_2^{n_2}$  over  $E_1$ ,  $F(a_1, a_2) \subset E_2$

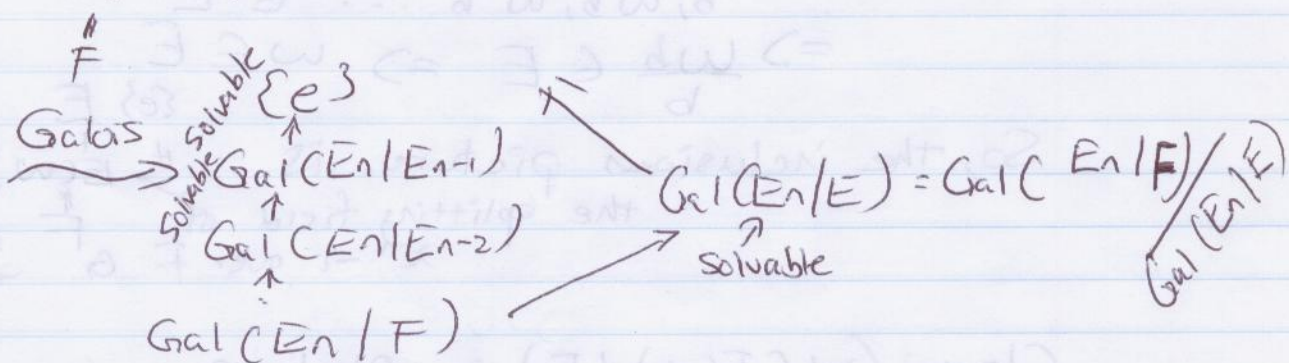
$$\begin{array}{c}
 F(a_1, \dots, a_n) \subset E_n \\
 F(a_1, a_2) \subset E_2 \\
 F(a_1) \subset E_1 \\
 E_0 = F
 \end{array}
 \quad
 \begin{array}{c}
 \nearrow \\
 \nearrow \\
 \nearrow \\
 \nearrow
 \end{array}
 \quad
 \begin{array}{c}
 E = S_F(f) \\
 \sim \rightarrow
 \end{array}
 \quad
 \begin{array}{c}
 \text{Apply} \\
 \text{Galois Theorem}
 \end{array}$$



Defn: A splitting extension of a splitting extension is

i.e.  $E_2 = S_{E_2}(f_2) = S_F(g)$

$E_1 = S_F(f_1)$



$$\text{Gal}(E/F) = \text{Gal}(E_n/F) / \text{Gal}(E_n/E)$$

As a quotient of a solvable group  $\text{Gal}(E/F)$  is solvable

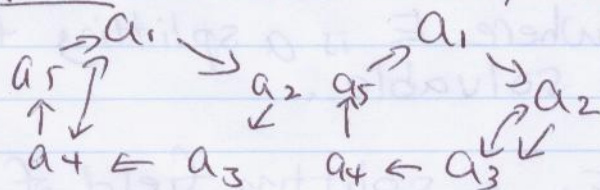
Claim: Suppose  $H < S_5$  contains a 5-cycle.

$$1 \rightarrow 4 \rightarrow 3 \rightarrow 5 \rightarrow 2 \rightarrow 1$$

a 2-cycle:  $1 \leftrightarrow 2, 2 \leftrightarrow 3, 3 \leftrightarrow 4, 4 \leftrightarrow 5, 5 \leftrightarrow 1$

In that case  $H = S_5$

Proof: This is a baby Rubik's cube exercise



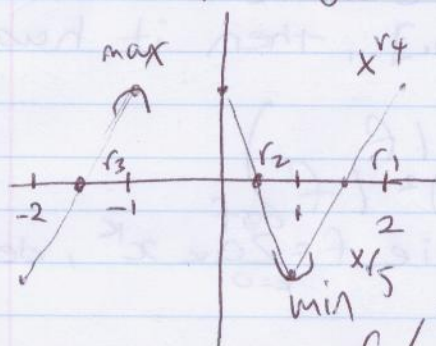
$$\{a_1, \dots, a_5\} = \{1, \dots, 5\}$$

can flip any non-neighbouring pair

can flip any neighbouring pair



Apr 2

Consider  $3x^5 - 15x + 5$ 

zero; root between -1 and -2

0 and 1

1 and 2

$$f' = 15x^4 - 15 = 15(x^4 - 1)$$

on  $\mathbb{R}$ ,  $f'$  has two roots $\Rightarrow f$  has exactly 3 roots in  $\mathbb{R}$ .

$$f / (x - r_1)(x - r_2)(x - r_3) = \text{quadratic}$$

2 further complex roots  $\leadsto \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \rightarrow \bar{z}, \bar{\bar{z}}$ .Consider  $G = \text{Gal}(S_Q(f) / Q)$ any  $\sigma \in G$  permutes  $r_1, \dots, r_5$  $\sigma$  is determined by this permutation

$$S_Q(f) = Q(r_1, \dots, r_5)$$

 $\Rightarrow G < S_5$  ( $G$  can be regarded as subgroup of  $S_5$ )

$$U \xrightarrow{r_1 \rightarrow r_2} U$$

$$r_2 \rightarrow r_3$$

$$r_3 \rightarrow r_4$$

$$r_4 \rightarrow r_5$$

 $\Rightarrow G$  contains a 2-cycle. $f$  is irreducible by EisensteinConsider  $Q(r_i) \cong Q[x] / \langle f \rangle$ 

$$\text{so } [Q(r_i) : Q] = 5$$

$$E = Q(r_1, \dots, r_5)$$

$$5 \mid [E : Q]$$

$$1 \mid ?$$

$$Q(r_i)$$

$$1 \mid 5$$

$$Q$$

 $\Rightarrow$ 

$$\Rightarrow 5 \mid |\text{Gal}(E/Q)| = |G|$$

Sylow's theorem

 $p$ , prime,  $p \mid |G| \Rightarrow G$  has a subgroup of order  $p$ . $\Rightarrow G$  has a subgroup of order 5

$$\Rightarrow G > \mathbb{Z}/5$$

 $\Rightarrow G$  has a 5-cycle. $\Rightarrow G$  has 2-cycle,  $G$  has 5-cycle

$$\Rightarrow G = S_5$$



Theorem: Let  $E/F$ ,  $f \in F[x]$ .

If  $f$  is irreducible over  $F[x]$ , then it has no multiple roots even in  $E$ .

( $a$  is a root iff  $(x-a) \mid f$ )  
( $a$  is a multiple iff  $(x-a)^2 \mid f$ )

Definition: If  $f \in F[x]$ , i.e.  $f = \sum_{k=0}^{\deg f} a_k x^k$ , define  
 $f' = \sum_{k=1}^{\deg f} k a_k x^{k-1}$

Claim: 1.  $a' = 0$  2.  $(af+bg)' = af' + bg'$   
3.  $(fg)' = f'g + g'f$

Proposition:  $f$  has multiple roots (in some extension  $E/F$ )  
iff  $f$  &  $f'$  have a common factor of  $\deg > 0$  in  $F[x]$ .

Proposition implies Theorem: If  $f$  is irreducible, then  
 $f$  &  $f'$  have no common factors, QED.

Proof of proposition

$\Rightarrow$  Assume  $f$  has a multiple root  $a \in E$

$(x-a)^2 \mid f \Rightarrow f = (x-a)^2 g$  for some  $g$

$f' = 2(x-a)g + g'(x-a)^2 = (x-a)(2g + (x-a)g')$

$\Rightarrow x-a \mid f'$  but  $a \in E$  but not proven for base field  $F$ .

Assume  $f$  &  $f'$  have no common factor in  $F[x]$  if  $\deg > 0$

$\langle f, f' \rangle = \langle p \rangle$  for  $p \in F[x]$

$\Rightarrow p \mid f$ ,  $p \mid f' \Rightarrow p = 1 \Rightarrow \deg p = 0$

$\Rightarrow \langle f, f' \rangle = \langle 1 \rangle \Rightarrow \exists \alpha, \beta \in F[x]$  s.t.

$\alpha f + \beta f' = 1 \Rightarrow$  since  $x-a \mid f$  &  $x-a \mid f'$   
 $\Rightarrow x-a \mid 1$

$\therefore f$  and  $f'$  do have common factor of  $\deg > 0$  in  $F[x]$ .

$\Leftarrow$  Suppose  $p \mid f$  &  $p \mid f' \Rightarrow p$  is irreducible.

Let  $E$  be an extension of  $F$  in which  $p$  has a root  
call this root  $a$ .  
( $E = F[x]/\langle p \rangle$ )

Apr 2

$$\Rightarrow f(a) = 0, f'(a) = 0$$

$$\Rightarrow (x-a) \mid f, \quad (x-a) \mid f' \text{ in } \mathbb{C}[x]$$

$$f = (x-a) \cdot g$$

$$f' = g + (x-a)g'$$

$$\Rightarrow g = \underbrace{f'}_{(x-a) \mid f'} - \underbrace{(x-a)g'}_{(x-a) \mid (x-a)g'}$$

$$\Rightarrow (x-a) \mid g$$

$$\Rightarrow g = (x-a)h$$

$$\Rightarrow f = (x-a)g = (x-a)(x-a)h = (x-a)^2 h$$

□