Group Theory ——

Finite groups, Classical Lie Groups and Their Representations

By Chin-Lung Wang
王金龍

I. Basic Group Theory

II. Galois Theory of polynomial equations

III. Basic Representation Theory

IV. Representations of SU(2) and SO(3) etc.

V. Semi-simple Lie Algebras

VI. Further Applications

CHAPTER ONE : GROUP THEORY

DEFINITION : A group G is a set equipped with a "product" structure such that

(1) $(x \cdot y) \cdot z = x \cdot (y \cdot z) \quad \forall\, x, y, z \in G$

(2) $\exists\, e \in G$ st $\quad xe = x = ex \quad \forall\, x \in G$

(3) $\forall\, x \in G \quad \exists$ "x^{-1}" st $\quad x x^{-1} = e = x^{-1} x$

The notion of group usually occures as transformations in geometry, or symmetries in physics

Example : Linear transformations on $\mathbb{R}^n$, $\mathbb{C}^n$

the matrix groups

$M_n(\mathbb{R})$: all $n \times n$ real matrixes

product $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} = \begin{bmatrix} 1\cdot5+2\cdot7 & 1\cdot6+2\cdot8 \\ 3\cdot5+4\cdot7 & 3\cdot6+4\cdot8 \end{bmatrix}$

e = identity matrix $= \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} = I_n$

Fact : $A \in M_n(\mathbb{R})$ is invertible $\iff \det A \neq 0$

- $AB \neq BA$
- $(AB)^{-1} = B^{-1} A^{-1}$

$GL_n(\mathbb{R}) = \{ A \in M_n(\mathbb{R}) \mid \det A \neq 0 \}$

$SL_n(\mathbb{R}) = \{ A \in M_n(\mathbb{R}) \mid \det A = 1 \}$

$O(n) \equiv O_n(\mathbb{R}) = \{ A \in M_n(\mathbb{R}) \mid A^t A = I_n \}$

$SO(n) \equiv SO_n(\mathbb{R}) = SL_n(\mathbb{R}) \cap O(n)$

$U(n) = \{ A \in M_n(\mathbb{C}) \mid \bar{A}^t A = I_n \}$

$SU(n) = SL_n(\mathbb{C}) \cap U(n)$; $Sp(n)$, Lorentz group ...

Example : Permutation group of a finite set

Symmetric group S_n

$$\alpha \in S_n \longleftrightarrow \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \cdots & \alpha(n) \end{pmatrix}$$

S_n is a finite group with $|S_n| = n!$

Cyclic Decomposition :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 5 & 4 & 8 & 2 & 7 & 1 \end{pmatrix} = (1358)\cdot(26)\cdot(4)\cdot(7)$$
$$= (1358)\cdot(26)$$

Transposition :

$(i\,j)$ = switch i and j, all others are fixed

S_n is generated by transpositions, eg.

$$(i_1\, i_2\, i_3 \cdots i_r) = (i_1\, i_r)\cdot(i_1\, i_{r-1}) \cdots (i_1\, i_3)(i_1\, i_2)$$

PARITY := even or odd via # of transpositions

Alternating group $A_n := \{\alpha \in S_n \mid \alpha \text{ is even}\}$

FACT: S_n is generated by

$(12), (13), \cdots (1n)$

A_n is generated by 3 cycles $(i\,j\,k)$

FACT: Every finite group is a subgroup of S_N

pf: Let $|G| = N$, then $G < S_N$ via

Any $g \in G$ acts on "the set G" via $g(h) := g \cdot h$

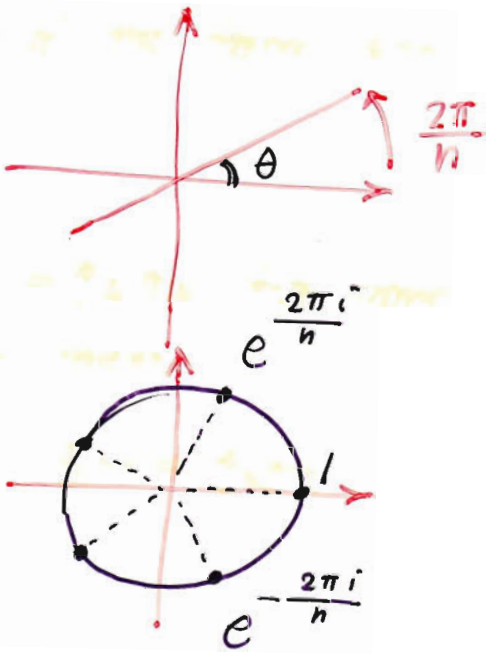
is a permutation since $g(h_1) = g(h_2) \Rightarrow h_1 = h_2$.

REMARK: S_n is not abelian for $n \geq 3$

G is called abelian if $gh = hg \;\; \forall\, g, h \in G$.

Example : Cyclic groups, Dihedral groups

Cyclic group C_n :



- finite subgroup of $SO(2)$ generated by

$$R_{2\pi/n} = \begin{bmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix}$$

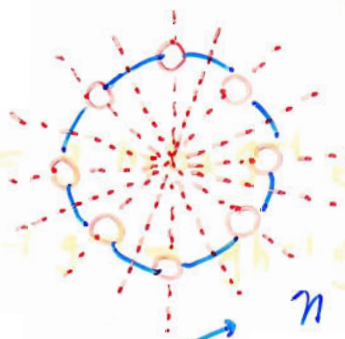
- complex numbers $e^{\frac{2\pi k i}{n}}$
- integers mod n : $\mathbb{Z}/n\mathbb{Z}$
- Abstract group

$$G = \langle x \mid x^n = e \rangle$$

Dihedral group D_n :

- $G \subset O(2)$ gen. by $R_{2\pi/n}$ and $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$

- symmetries of a necklace



- Abstract group

$$G = \langle x, y \mid x^n = 1,\ y^2 = 1,\ yxy = x^{n-1} \rangle$$

- $|D_n| = 2n$, non-abelian group $\longrightarrow$ n rotations, n reflections if $n \geq 3$

C_n as subgroup of S_n

$$C_n = \langle (1\,2\,3 \cdots n) \rangle$$

D_n as subgroup of S_n

$$D_n = \langle (1\,2\,3 \cdots n),\ (1\,n{-}1)(2\,n{-}2)\cdots \rangle$$

SUBGROUPS, COSET SPACES AND QUOTIENTS

Let $H < G$ be a subgroup

a (left) coset of H is a subset of the form gH

FACT: $g_1H \cap g_2H \neq \phi \iff g_2^{-1}g_1 \in H \iff g_1H = g_2H$

If $g_1H \cap g_2H \neq \phi$ then $g_1h_1 = g_2h_2$ for some h_1, h_2

so $g_2^{-1}g_1 = h_2h_1^{-1} \in H$, But then

$$g_2^{-1}g_1H = H \Rightarrow g_1H = g_2H.$$

Corollary: $\exists$ unique decomposition of G

$$G = H \cup aH \cup bH \cup \cdots \cup sH$$

Let G/H denote the coset space $\{g_iH\}_{i\in I}$

then $|G/H| = [G:H] := |G|/|H|$ (Index)

A coset aH is NOT a group unless $a \in H$

FACT: gHg^{-1} is a subgroup of G, called a conjugate group of H

- $(gh_1g^{-1})\cdot(gh_2g^{-1}) = g\,h_1h_2\,g^{-1} \in gHg^{-1}$
- $(ghg^{-1})^{-1} = (g^{-1})^{-1}h^{-1}g^{-1} = gh^{-1}g^{-1}$

In order for G/H has a induced group structure we need that $gHg^{-1} = H \;\forall\, g \in G$

such H is called normal subgroup of G: $H \lhd G$.

We want $[aH]\cdot[bH] = [abH]$

ie. $ah_1 \cdot bh_2 \in abH$

$\Leftrightarrow$ $ah_1b \in abH \iff h_1b \in bH$

$\Leftrightarrow$ $b^{-1}h_1b \in H$

$\Leftrightarrow$ $b^{-1}Hb \subset H$.

Any subgroup of an abelian group is normal

$H \lhd G$

If $H \lhd G$, G/H is the quotient group

has the natural reduction map $G \longrightarrow G/H$

by $g \longmapsto \overline{g} = gH \in G/H$ eg. $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$

GROUP HOMOMORPHISM :

A map $\varphi : G \longrightarrow G'$ is a homomorphism

if $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \quad \forall\ a, b \in G$

- $\varphi(e) = \varphi(e \cdot e) = \varphi(e) \cdot \varphi(e) \Rightarrow \varphi(e) = e'$
- $e' = \varphi(e) = \varphi(a\, a^{-1}) = \varphi(a) \cdot \varphi(a^{-1})$

  $\Rightarrow \varphi(a^{-1}) = \varphi(a)^{-1}$

Image group $\operatorname{Im}\varphi < G' = \{ \varphi(a) \mid a \in G \}$

Kernel subgroup $\ker \varphi < G = \{ g \in G \mid \varphi(g) = e' \}$

- $\ker\varphi$ is a normal subgroup since

  $\varphi(ghg^{-1}) = \varphi(g)\,\varphi(h)\,\varphi(g)^{-1}$ if $\varphi(h) = e'$

  $= \varphi(g)\,\varphi(g^{-1}) = e'$

  ie. $g \ker\varphi\, g^{-1} \subset \ker\varphi$.

THE ISOMORPHISM THEOREM :

$$\overline{\varphi} : G/\ker\varphi \cong \operatorname{Im}\varphi$$

Example : $H < G$, $[G : H] = 2 \Rightarrow H \lhd G$

eg. $C_n \lhd D_n$; $A_n \lhd S_n$

pf : Let $g \notin H$ then $G = H \amalg gH$

also $G = H \amalg Hg$

$\Rightarrow gH = Hg$ ie. $gHg^{-1} = H$.

Warnning : In general, left cosets are quite different with right cosets

EXAMPLES OF NORMAL SUBGROUPS

- Finite abelian group is easy

$$G \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \mathbb{Z}/p_2^{e_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}$$

Here product group $G_1 \times G_2$ is defined by

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 h_1, g_2 h_2)$$

- If $H \triangleleft G$, then G should be some kind of twisted product of G/H and H

Center of G : $Z(G)$

$$Z(G) = \{ h \in G \mid hg = gh \ \forall\, g \in G \}$$

$Z(G)$ is normal $\quad g\,Z(G)\,g^{-1} = Z(G)$ obviously

Commutator group of G : $[G,G] \equiv G'$

$[G,G]$ is the subgroup of G generated by all commutators $\quad [g,h] := ghg^{-1}h^{-1}$

G' is normal since $\quad \alpha\,[g,h]\,\alpha^{-1} = [\alpha g \alpha^{-1}, \alpha h \alpha^{-1}]$

FACT : G' is the smallest normal subgroup K of G such that G/K is abelian

Abelian $\Rightarrow \bar{g}\bar{h}\bar{g}^{-1}\bar{h}^{-1} \in \bar{e} \Rightarrow ghg^{-1}h^{-1} \in K$

We will see later that if G is a p group that is, $|G| = p^n$ for a prime p, then $Z(G) \neq \{e\}$.

GROUPS ACTING ON A SET

Let G be a finite group acting on a finite set X.

For $x \in X$, $\text{Stab}(x) = \{ g \in G \mid gx = x \} \subset G$

$\text{Orbit}(x) = Gx \subset X$

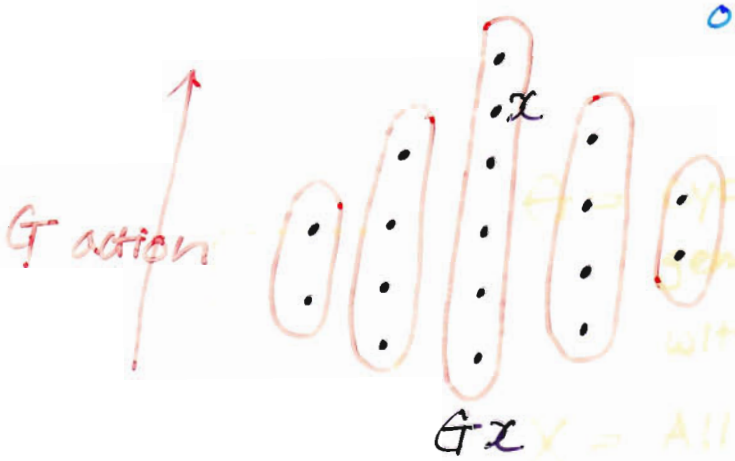
There is an 1 to 1 correspondence :

$$G/\text{Stab}(x) \longleftrightarrow \text{Orbit}(x) = Gx$$

Consequences :

I. Class Formula : $|X| = \sum [G : \text{Stab}(x)]$

sum over orbits



$X = Gx_1 \cup \cdots \cup Gx_N$ disjoint union of orbits

Notice that $\text{Stab}(gx) = g\,\text{Stab}(x)\,g^{-1}$

Application : Any finite group G with order p^2, p a prime, must be abelian

pf: Let G acts on $X \equiv G$ by $g(x) = gxg^{-1}$

then $|G| = |Z(G)| + \sum_x [G : \text{Stab}(x)]$

$|Z(G)| = 1 \Rightarrow p^2 = 1 + kp$ $\longrightarrow\!\!\!\!\!\!\times$

$|Z(G)| = p \Rightarrow$ Let $Z(G) = \langle g \rangle$, $h \notin Z(G)$

then $G \equiv \{ h^i g^j \mid 0 \le i, j \le p \}$ abelian $\longrightarrow\!\!\!\!\!\!\times$

II. Burnside's Formula:

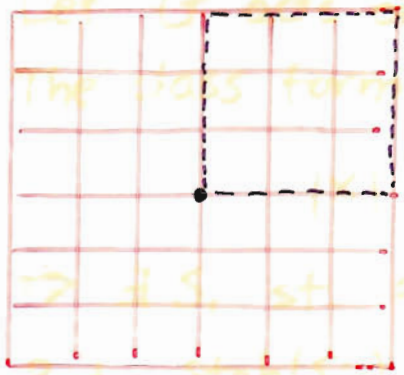
number of orbits $N = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$

$Fix(g) = \{x \in X \mid gx = x\}$

Consider an orbit $\mathcal{O}$; any point $x \in \mathcal{O}$ is counted $|Stab(x)|$ times in $\Sigma_{g \in G} |Fix(g)|$, so the whole orbit is counted

$$[G : Stab(x)] \cdot |Stab(x)| = |G| \text{ times}.$$

Application: How many distinct $n \times n$ colored tablecloths are there if there are q colors avaliable ?



(the case $n=6$)

G = cyclic group of order 4 generated by rotation with angle $90° = R$

X = All q^{n^2} colored table clothes

distinct ones = N

$$N = \frac{1}{|G|}\left(|Fix(e)| + |Fix(R)| + |Fix(R^2)| + |Fix(R^3)|\right)$$

$$= \frac{1}{4}\left(q^{n^2} + q^{(\frac{n}{2})^2} + q^{\frac{n^2}{2}} + q^{(\frac{n}{2})^2}\right)$$

if n is even.

In general:

$$N = \frac{1}{4}\left(q^{n^2} + 2q^{\left[\frac{n^2+3}{4}\right]} + q^{\left[\frac{n^2+1}{2}\right]}\right).$$

Sylow's Theorems

I. Let $|G| = n = p^e m$ with $p \nmid m$, then $\exists H < G$ with $|H| = p^e$ (Sylow p subgroup)

II. Any p subgroup of G is contained in a Sylow p subgroup

III. Any two Sylow p groups are conjugate

IV. Let s be the number of Sylow p-groups then $s \mid m$ and $s \equiv 1 \pmod p$

Proof: I. Let $X = \{ S \subset G \mid |S| = p^e \}$, then

$$|X| = C_{p^e}^{p^e m} = \frac{p^e m (p^e m - 1) \cdots (p^e m - p^e + 1)}{p^e !}$$

$$= m \cdot \frac{(p^e m - 1) \cdots (p^e m - p^e + 1)}{(p^e - 1)!} \quad \text{so } p \nmid |X|$$

Let G acts on X by left multiplications.

The class formula

$$|X| = \sum_i [G : \mathrm{stab}(S_i)]$$

$\Rightarrow \exists S_i$ st. $p^e \mid \mathrm{stab}(S_i) \mid p^e m$

But $\mathrm{Stab}(S_i) \neq G$ (unless $m = 1$)

Now use induction.

Corollary (Cauchy): $p \mid |G| \Rightarrow \exists\, g \in G$ of order p

Let $|G| = p^e m$, $p \nmid m$, H a Sylow p group

pick $h \in H$, $h \neq 1$ then $\mathrm{ord}(h) = p^r$, $r \leq e$

Let $g = h^{p^{r-1}}$ then $\mathrm{ord}(g) = p$.

THE PROOF OF II, III, IV are similar and will be omitted.

THE TECHNIQUE OF GROUP ACTION ON SETS AND SYLOW'S THEOREMS ARE BASIC TOOLS TO STUDY THE STRUCTURES OF FINITE GROUPS

DEFINITION : G is simple if G has no nontrivial normal subgroups

- $|G| = pq$, p, q primes $\Rightarrow$ G is not simple

  Let $p < q$

  $H_1, H_2, \cdots, H_s$ Sylow q subgroups

  $s \mid p$, $s \equiv 1 \ (q) \Rightarrow s = 1$ ~~unless~~

  So the Sylow q group $H \lhd G$

- If $|G| = 15$, then $G \cong C_{15} \cong C_3 \times C_5$

  $15 = 3 \cdot 5$, $3 < 5$

  H = the Sylow 5 group $\lhd G$

  But $s \mid 15$, $s \equiv 1 \pmod 3 \Rightarrow s = 1$, so

  K = the Sylow 3 group $\lhd G$

  clearly that $H \cap K = \{e\}$

  $H \cdot K = G$

  $\Rightarrow G \cong H \times K \cong C_5 \times C_3$.

We list some more applications

- $|G| = p^2 q$, p, q primes $\Rightarrow$ G is not simple
- The only simple groups G with $|G| < 60$ are C_p with p prime < 60.

  We will see later that A_4 is simple

  Notice that $|A_4| = 60$
- All finite simple groups are classified !!

CHAPTER TWO : GALOIS THEORY

SOLVING POLYNOMIAL EQUATIONS BY $\sqrt[n]{\ }$

$x^2+bx+c=0$ (Babylonians B.C ?)

$$X^2+2\cdot\frac{b}{2}x+\left(\frac{b}{2}\right)^2=\left(\frac{b}{2}\right)^2-c$$

$$\left(x+\frac{b}{2}\right)^2=\frac{b^2-4c}{4}$$

Assume know how to solve $X^2=b^2-4c$
then know how to solve $x^2+bx+c=0$

$x^3+bx^2+cx+d=0$ (Ferro, Cardano 1540)

replace x by $x-\frac{b}{3}$, get

$$x^3+px+q=0$$

Let $x=u+v$, get

$$u^3+v^3+3uv(u+v)+p(u+v)+q=0$$

Force $3uv+p=0$, ie. $v=-\frac{p}{3u}$

$$u^3+\left(-\frac{p}{3u}\right)^3+q=0$$

$$\Rightarrow\quad u^6+qu^3-\frac{p^3}{27}=0$$

$$u^3=\frac{-q}{2}\pm\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}$$

Let $\alpha=\sqrt[3]{\frac{-q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}$; $\beta=\sqrt[3]{\frac{-q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}$

Solutions :

$$x=\alpha+\beta\ ;\ \alpha\omega+\beta\omega^2\ ;\ \alpha\omega^2+\beta\omega$$

where $\omega^3=1$, $\omega\neq 1$.

How about $X^4+pX^2+qX+r=0$? (Ferarri 1545)

Let $= (x^2+ax+\lambda)\cdot(x^2-ax+\frac{r}{\lambda})$

$= x^4+\left(\lambda-a^2+\frac{r}{\lambda}\right)x^2+\left(\frac{ar}{\lambda}-\lambda a\right)x+r$

$$\Rightarrow \begin{cases} \lambda-a^2+\frac{r}{\lambda}=p \\ \frac{ar}{\lambda}-\lambda a=q \end{cases} \Rightarrow \begin{cases} \lambda^2-(a^2+p)\lambda+r=0 \\ \lambda^2+\frac{q}{a}\lambda-r=0 \end{cases}$$

Hard to proceed ... But still can be solved !

Ruffini 1813, Abel 1827, Galois 1832~1846 : general polynomial equations of degree ≥ 5 can not be solved by radicals.

Gauss did show the (1800 ?)

FUNDAMENTAL THEOREM OF ALGEBRA

Every $f(x)\in\mathbb{C}[x]$ has a root in $\mathbb{C}$.

Idea of pf:

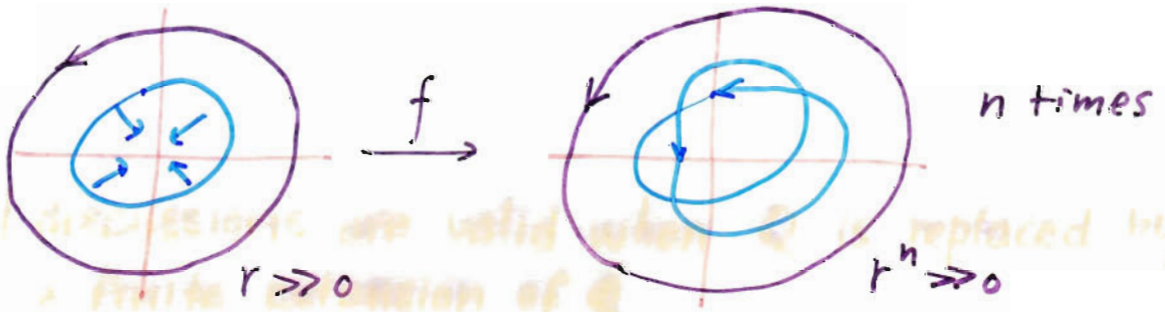
Get a map rotates n times :

$$\mathbb{C} \longrightarrow S^1=\{z\in\mathbb{C} \mid |z|=1\}$$

$$z \longmapsto \frac{f(z)}{|f(z)|}$$

$$f(z)=z^n+a_{n-1}z^{n-1}+\cdots$$

$$=z^n(1+o(z)) \sim z^n=r^n e^{in\theta}$$



GALOIS GROUP OF AN EQUATION

Let $f(x) \in \mathbb{Q}[x]$ be irreducible monic

$$f(x) = (x-\alpha_1)\cdots(x-\alpha_n), \quad \alpha_i \in \mathbb{C}$$

No multiple roots since $(f, f') = 1$

Let $K = \mathbb{Q}(\alpha_1, \cdots, \alpha_n) \subset \mathbb{C}$ be the number system (= field) generated by all rational expressions in $\alpha_1, \cdots, \alpha_n$.

Galois group $G = G(K/\mathbb{Q}) := \mathrm{Aut}_{\mathbb{Q}}(K)$

$$\mathrm{Aut}_{\mathbb{Q}}(K) = \{ \varphi : K \xrightarrow{\sim} K \text{ st } \varphi|_{\mathbb{Q}} = \mathrm{id} \text{ and } \varphi \text{ preserves } (+, \cdot) \}$$

FACT: $G \subset S_n$ as permutation group of $\alpha_1, \cdots, \alpha_n$

pf: Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $a_i \in \mathbb{Q}$

then $\varphi f(x) = f(x)$

$\| \qquad\qquad \| (x-\alpha_1)\cdots(x-\alpha_n)$

$(x-\varphi(\alpha_1))\cdots(x-\varphi(\alpha_n))$

uniqueness of factorization

$\Rightarrow \varphi \in S_n$.

FACT: K is a finite dimensional vector space over $\mathbb{Q}$ and $|G| = \dim_{\mathbb{Q}} K =: [K:\mathbb{Q}]$

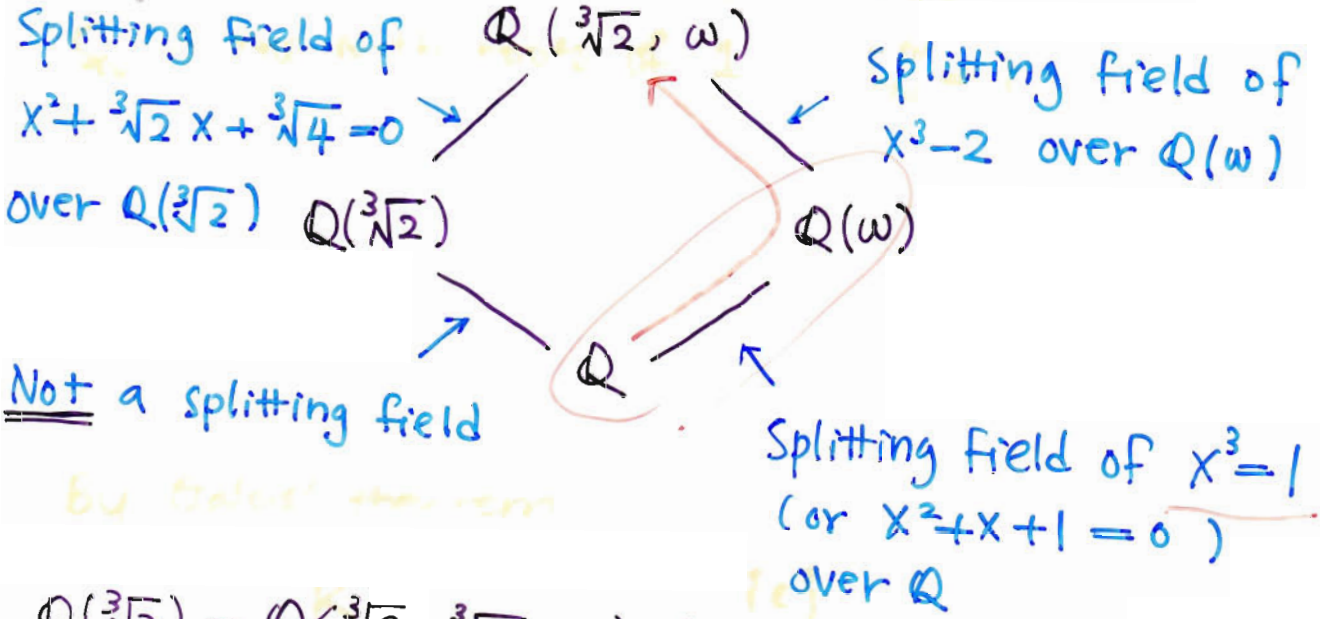
All discussions are valid when $\mathbb{Q}$ is replaced by k, a finite extension of $\mathbb{Q}$.

Method : Jointing roots one by one

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

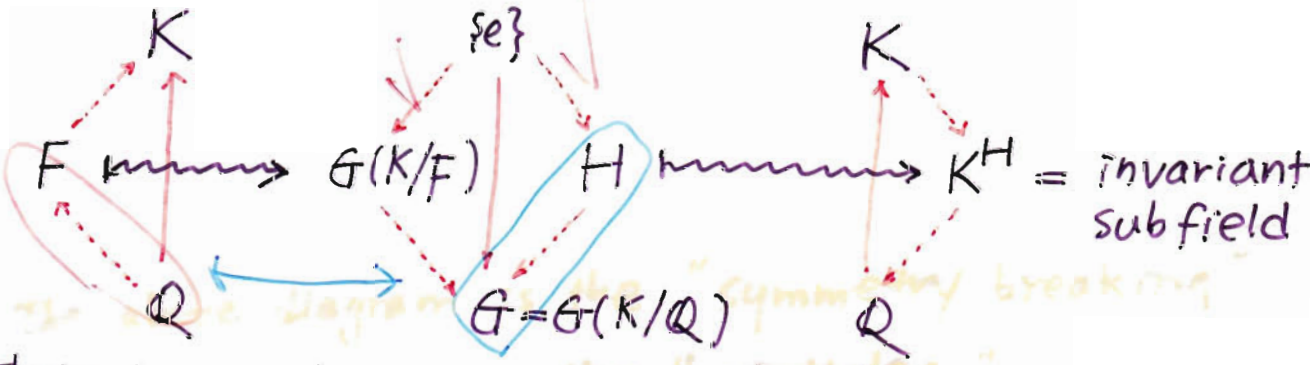
$$K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$$

$$= \mathbb{Q}(\sqrt[3]{2}, \omega)$$



- $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}\langle \sqrt[3]{2}, \sqrt[3]{4}, 1 \rangle \cong \mathbb{Q}[x]/(x^3 - 2)$
  is a 3-dimensional vector space over $\mathbb{Q}$
  And $|Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))| = 3 = \deg(x^3 - 2)$
- $\mathbb{Q}(\omega) = \mathbb{Q}\langle \omega, \omega^2, 1 \rangle \cong \mathbb{Q}[x]/(x^2 + x + 1)$
  is 2-dimensional /$\mathbb{Q}$, $|Aut_{\mathbb{Q}}(\mathbb{Q}(\omega))| = 2 = \deg(x^2 + x + 1)$

FUNDAMENTAL THEOREM OF GALOIS THEORY



There is an 1 to 1 correspondence:

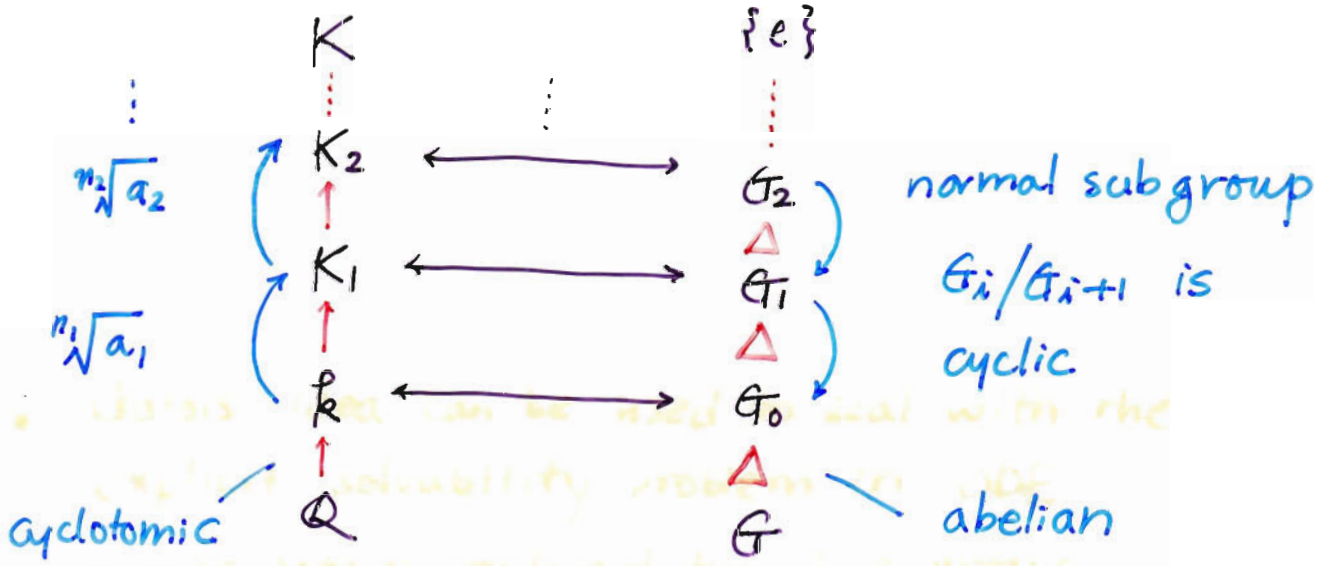
$F/\mathbb{Q}$ splitting field $\leftrightarrow$ $H \lhd G$ and $G(F/\mathbb{Q}) \cong G/H$

SOLVABILITY

Let $f(x) \in \mathbb{Q}[x]$, Want to solve the roots by radicals, may first replace $\mathbb{Q}$ by a cyclotomic extension $k = \mathbb{Q}(\zeta_N)$ where ζ_N is the N-th roots of 1 : $\zeta_N^N = 1$.
Pick N large and divisible enough.

- FACT: The radical extension $X^n - a = 0$ is splitting and the Galois group G is cyclic with $|G|/n$

By Galois' theorem



- FACT: $G(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ is an abelian group, in fact, is a direct sum of cyclic groups

The above diagram is the "symmetry breaking" diagram, roots are the "particles".

Definition : A finite group G is solvable if $\exists$ a sequence of subgroups $G_1, G_2, \cdots$ st. $G \triangleright G_1 \triangleright G_2 \cdots \triangleright \{e\}$ and G_i/G_{i+1} is an abelian group (equivalent to require that G_i/G_{i+1} cyclic)

THEOREM (Galois)
A polynomial is solvable by radicals if and only if its Galois group is solvable.

Task :

I. Show that general polynomial equations of degree ≥ 5 is not solvable

II. Given a polynomial, how to calculate its Galois group ?

Remarks on later development :

- Galois' idea can be used to deal with the explicit solvability problem in ODE, finite group replaced by Lie group
- If we allow some special value of theta functions, then any polynomial can be explicitly solved (geometry of abelian varieties)

THEOREM: A_n is simple if $n \geq 5$

pf: Let $A_n \triangleright K \neq \{e\}$

if K contains a 3 cycle, say (123), then K will contain all 3cycles:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ i & j & k & \ell & m & \cdots \end{pmatrix} (123) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ i & j & k & \ell & m & \cdots \end{pmatrix}^{-1} = (i\ j\ k)$$

γ = may assume to be even, otherwise use $(\ell\ m)\gamma$.

But since A_n is generated by 3 cycles, this will imply $K \equiv A_n$, so A_n is simple.

Claim: Let $1 \neq \alpha \in K$ has maximal number of fixed points, then α is a 3-cycle

If not, then α looks like:

A. $\alpha = (123\cdots)\cdots$ and moves say, 4, 5

or B. $\alpha = (12)(34)\cdots$ since $\alpha \neq (1234)$ odd

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

A. $\alpha_1 = (124\cdots)\cdots$

or B. $\alpha_1 = (12)(45)\cdots$, have $\alpha_1 \neq \alpha$

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

$\forall\ i \geq 6$, $\alpha(i) = i \Rightarrow \alpha_2(i) = i$

Case A. $\alpha_2(2) = 2$, but α moves 1, 2, 3, 4, 5 $\rightarrow\leftarrow$

Case B. $\alpha_2(1) = 1$, $\alpha_2(2) = 2$, but α moves 1, 2, 3, 4 $\rightarrow\leftarrow$

Corollary: S_n is not solvable if $n \geq 5$

$S_n \triangleright A_n \triangleright \{e\}$ stops !

Remark: S_2, S_3, S_4 are solvable

$S_2 \cong C_2$ not interesting

$S_3 \triangleright A_3 \cong C_3$ cyclic, OK.

$S_4 \triangleright A_4 \triangleright K \triangleright \{e\}$

order 12. order 4.

$K = \{(12)(34), (14)(23), (13)(24), e\}$

the Klein's 4 group

is a normal subgroup of A_4, in fact

$A_4/K \cong S_3$ solvable.

THEOREM (Ruffini-Abel-Galois) 1820 ~

The equation $X^n - a_1 X^{n-1} + a_2 X^{n-2} - \cdots + (-1)^n a_n = 0$ for $n \geq 5$ can not be solved by radicals over $\mathbb{Q}(a_1, \cdots, a_n)$.

pf: If $X^n - a_1 X^{n-1} + a_2 X^{n-2} - \cdots + (-1)^n a_n$

$= (X - t_1)(X - t_2) \cdots (X - t_n)$

then a_i = symmetric polynomial in $t_1, \cdots, t_n$ of degree i

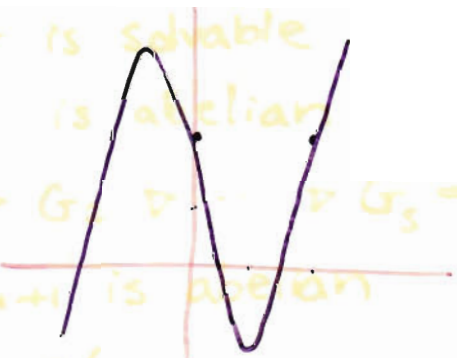
So the Galois group of the splitting field $\mathbb{Q}(t_1, \cdots, t_n)$ over $\mathbb{Q}(a_1, \cdots, a_n)$ is S_n.

To finish the story of Galois theory, we should at least give an concrete example which is not solvable by radicals.

THEOREM: Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial which has exactly 2 non-real roots in $\mathbb{C}$, and $\deg f = p$ is a prime number ≥ 5. Then the Galois group is S_p. Hence $f(x)=0$ can not be solved by radicals.

EXAMPLE: $f(x) = x^5 - 16x + 2$

The graph of $f(x)$ is:



has exactly 3 real roots.

$f(x)$ is irreducible follows from Eisenstein's criterion.

FACT: Let p be a prime, $G < S_p$.
If $(1,2)$ and $(1,2,\cdots,p) \in G$, then $G = S_p$
(true for any $p \in \mathbb{N}$)

Pf of the theorem:

Let $f(x) = (x-\alpha_1)\cdots(x-\alpha_p)$ $\alpha_i \in \mathbb{C}$

since $[\mathbb{Q}(\alpha_1):\mathbb{Q}] = \deg f = p$

so $|G| = [\mathbb{Q}(\alpha_1,\cdots,\alpha_p):\mathbb{Q}]$

$= [\mathbb{Q}(\alpha_1,\cdots,\alpha_p):\mathbb{Q}(\alpha_1)] \cdot [\mathbb{Q}(\alpha_1):\mathbb{Q}]$

so $p \mid |G|$, Sylow $\Rightarrow \exists\, \sigma \in G$ of order p.
(p prime $\Rightarrow \sigma \sim (1\,2\,3\,\cdots\,p)$)

The map $a \mapsto \overline{a}$ fixes all real roots and exchange the 2 cpx roots

$\Rightarrow \exists\, \tau \in G \subset S_p$ st τ looks like $(1,2)$. END

HOW TO DETERMINE THE SOLVABILITY OF A GIVEN FINITE GROUP EFFECTIVELY ?

Recall the derived group $G' = [G, G]$ is the smallest normal subgroup K st. G/K is abelian

Let $G'' = [G', G']$, $G^{(3)} = [G'', G'']$ etc

Derived normal series

$$G = G^0 \triangleright G^1 \triangleright G^{(2)} \triangleright G^{(3)} \triangleright \cdots \triangleright G^{(k)} \triangleright \cdots$$

THEOREM : G is solvable $\iff G^{(k)} = \{e\}$ some k.

pf: $\Leftarrow$: $G^{(k)} = \{e\}$ then G is solvable since $G^{(i)}/G^{(i+1)}$ is abelian

$\Rightarrow$: Let $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_s = \{e\}$ such that G_i/G_{i+1} is abelian

G/G_1 abelian $\Rightarrow G_1 \supset G'$

G_1/G_2 abelian $\Rightarrow G_2 \supset G_1' \supset G''$

G_2/G_3 abelian $\Rightarrow G_3 \supset G_2' \supset G^{(3)}$

$\cdots \Rightarrow G_s \supset G^{(s)}$ $\square$

$G_s = \{e\}$

Example : $|G| = p^n \Rightarrow G$ is solvable

$= p.q$ p, q primes $\Rightarrow$ solvable

pf: Had seen that $Z(G)$ is nontrivial

$G/Z(G)$ is also a p-group

By induction $G/Z(G)$ is solvable

$G/Z(G) \triangleright G_1/Z(G) \triangleright \cdots \triangleright G_s/Z(G) = \{e\}$

$\Rightarrow G \triangleright G_1 \triangleright \cdots \triangleright G_s = Z(G)$ abelian.

REFERENCES

Basic Group Theory and Galois Theory

- M. Artin : ALGEBRA
- N. Jacobson : BASIC ALGEBRA I

Representation Theory

- J. P. Serre : LINEAR REPRESENTATIONS OF FINITE GROUPS
- T. Bröcker / T. Dieck : REPRESENTATIONS OF COMPACT LIE GROUPS

Group Theory in Physics

- B. L. Vander Waerden : GROUP THEORY AND QUANTUM MECHANICS
- S. Sternberg : GROUPS AND PHYSICS

Theory