Group Theory

Book 1

Finite groups (up to isomorphism)

n	1	2	3	4	5	6	7	8	9	10	11	…	59	60	61	62	63	64	65	…
no. of groups of order n	1	1	1	2	1	2	1	5	2	2	1		1	13	1	2	4	267	1	

$n=4$: Klein $C_2 \times C_2$, C_4

$n=6$: $C_2 \times C_3 \cong C_6$, $S_3 \cong D_3$

$n=8$: elementary abelian $C_2 \times C_2 \times C_2$, $C_2 \times C_4$, C_8, Q Quaternion, D_4 Dihedral

$n=9$: $C_3 \times C_3$ elementary abelian, C_9

$n=60$: $C_2 \times C_2 \times C_3 \times C_5$, $C_4 \times C_3 \times C_5 \cong C_{60}$

$|S_5| = 5! = 120$

S_5 has composition series

$$1 \overset{60}{\triangleleft} A_5 \overset{2}{\triangleleft} S_5$$

Simple groups
- cyclic of prime order
- nonabelian simple groups of order

60, 168, 360, 504, 660, 1092, 2448, 2520, 3420, 4080, …

S_n = symmetric group of degree n, $|S_n| = n!$

A_n = alternating group of degree n, order, $|A_n| = \frac{1}{2} n!$ $(n \geq 2)$

A_n is simple for $n \geq 5$

$|S_4| = 24$ solvable

$$G_1 = 1 \overset{2}{\triangleleft} G_2 \overset{2}{\triangleleft} G_3 \overset{3}{\triangleleft} G_4 = A_4 \overset{2}{\triangleleft} G = S_4$$

$G_2 = \langle (12)(34) \rangle$ order 2, $G_3 = \langle (12)(34), (13)(24) \rangle$ order 4

Composition series with composition factors of prime order: $|G_2/G_1| = 2$, $|G_3/G_2| = 2$, $|G_4/G_3| = 3$, $|G/G_4| = 2$

G is solvable if all its composition factors are cyclic of prime order.

Jordan-Hölder Theorem: Every finite group has a composition series with its factors being simple groups.

G $(G \neq 1)$ is simple if its only composition series is $1 \triangleleft G$ (the only normal subgroups are 1 and G).

eg. cyclic groups of prime order are simple.

A_n is simple for $n \geq 5$.

Classical groups of Lie type are analogous to Lie groups

We use finite fields: Every finite field $\hat{\ }$ has prime power order $q = p^e$, p prime, $e \geq 1$.

$\mathbb{F}_q$

including $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$; $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

$GL_n(F)$ = group of all invertible $n \times n$ matrices over F.

$\alpha^2 = 1 + \alpha = \beta$

$GL_n(F)$ is the general linear group of degree n over F.

$GL_2(\mathbb{R})$ is a Lie group

$$GL_2(\mathbb{F}_2) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \underbrace{\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{\text{order } 2}, \underbrace{\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}}_{\text{order } 6} \right\} \cong S_3$$

$\parallel$

$GL_2(2)$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

A Sylow p-subgroup

$$\begin{bmatrix} 1 & * & * & \cdots & * \\ & 1 & & & \vdots \\ & & \ddots & & \\ & 0 & & \ddots & * \\ & & & & 1 \end{bmatrix}$$

of order $q^{\frac{n(n-1)}{2}}$

$$|GL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$$

There are q^{n^2} matrices of size $n \times n$ over $\mathbb{F}_q$ but most of them are not invertible.

$n \times n$

$q^n - 1$ choices

$q^n - q$ choices

$q^n - q^2$ choices

$\dots$

$q^n - q^{n-1}$ choices

$|GL_2(2)| = (2^2 - 1)(2^2 - 2) = 6$

$|GL_3(2)| = (2^3 - 1)(2^3 - 2)(2^3 - 2^2)$
$= 7 \cdot 6 \cdot 4 = 168$

$GL_3(2)$ is the second-smallest nonabelian simple group

$$|GL_n(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}} (q^n - 1)(q^{n-1} - 1) \cdots (q - 1)$$
$$= q^{\frac{n(n-1)}{2}} \prod_{j=1}^{n} (q^j - 1)$$

$|GL_4(2)| = (2^4-1)(2^4-2)(2^4-2^2)(2^4-2^3) = 15 \cdot 14 \cdot 12 \cdot 8 = 20160$

$|A_8| = \frac{8!}{2} = \frac{40320}{2} = 20160$

There are two simple groups of order 20160 : $A_8 \cong GL_4(2)$, $PSL_3(4)$

$|GL_3(4)| = (4^3-1)(4^3-4)(4^3-4^2) = 63 \cdot 60 \cdot 48 = 181440 = 9 \cdot 20160$

$GL_3(4)$ is not simple.

$GL_n(F)$ has a normal subgroup $SL_n(F)$ = special linear group of degree n over F

$= \{ A \in GL_n(F) : \det A = 1 \}$.

$|SL_n(\mathbb{F}_q)| = \frac{|GL_n(\mathbb{F}_q)|}{q-1}$

there is a surjective homomorphism $GL_n(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^\times = \{$nonzero field elements$\}$

$A \longmapsto \det A$

First isomorphism theorem: $GL_n(\mathbb{F}_q) / SL_n(\mathbb{F}_q) \cong \mathbb{F}_q^\times$

If $q=2$ then $SL_n(q) = GL_n(q)$.