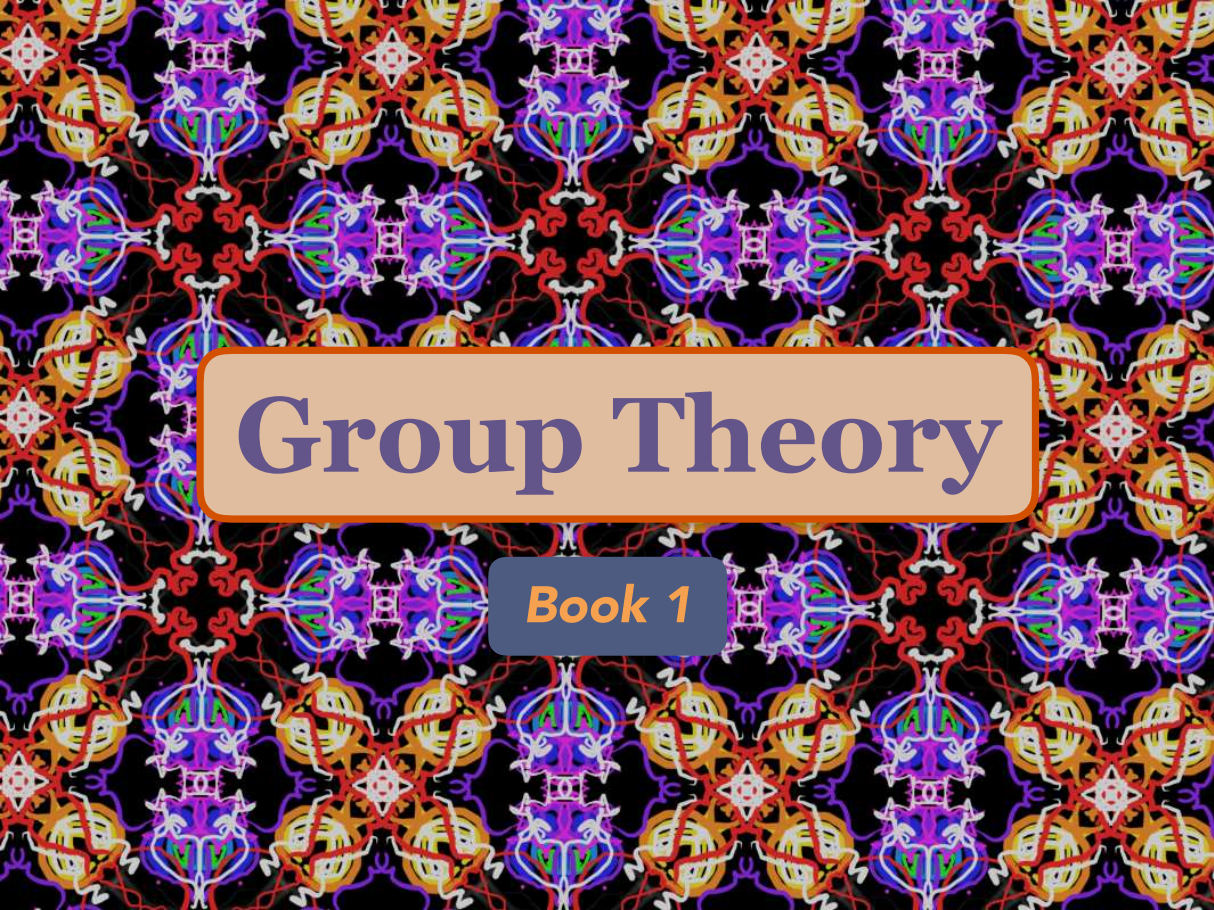

Group Theory
Book 1

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	1	267	1	

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

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

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

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

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

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

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

$G_2 = \langle (12)(34) \rangle$ order 2

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

Composition series with composition factors of prime order: $|G_1/G_0| = 2$, $|G_2/G_1| = 2$,

$|G_3/G_2| = 3$, $|G/G_3| = 2$

$|S_5| = 5! = 120$

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, ...

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 has prime power order $q = p^e$, p prime, $e \geq 1$.

$\mathbb{F}_q$

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

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

·	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

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

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

$GL_1(F)$ is the general linear group of degree n over F.

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

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

$GL_2(2)$

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

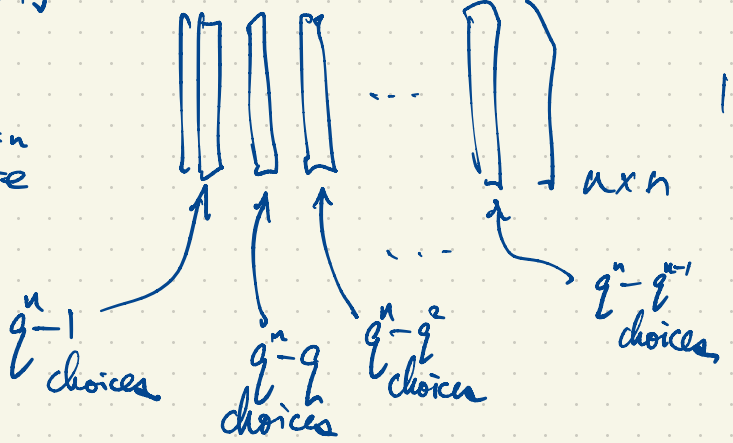
A Sylow 2-subgroup

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

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.



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

$= q^{\frac{n(n-1)}{2}} \prod_{j=1}^{n} (q^j - 1)$

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

$|GL_3(2)| = (2^3-1)(2^3-2)(2^3-2^2)$

$= 7 \cdot 6 \cdot 4 = 168$

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

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

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

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 $GL_n(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^* = \{\text{nonzero field elements}\}$

$A \longmapsto \det A$

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

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

Smaller example: $|A_5| = \frac{1}{2}5! = 60$ smallest nonabelian simple group

$SL_2(\mathbb{F}_4) = \frac{1}{3}\cdot 180 = 60$

$|GL_2(\mathbb{F}_4)| = (4^2-1)(4^2-4) = 15\times 12 = 180$

$\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$

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

·	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

There is only one simple group of order 60;

$SL_2(4) \cong A_5$

What five points is $SL_2(4)$ permuting (all 60 even permutations of the five points)?
We'll answer this soon but first use group presentations:

$A_5 \cong \langle a, b \mid a^5 = b^3 = (ab)^2 = 1\rangle$ = the group generated by a, b subject to these relations $a^5=1,\ b^3=1,\ (ab)^2=1$.

What does this mean?

In A_5, let $a = (1\,2\,3\,4\,5)$, $b = (1\,4\,2)$, so $ab = (1\,2\,3\,4\,5)(1\,4\,2) = (2\,3)(4\,5)$

"left-to-right" composition: see handout

(142): $1 \mapsto 4$, $2 \mapsto 1$, $3 \mapsto 3$, ...

~~$(142)(1) = 4$~~
~~$(142)(2) = 1$~~
~~$(142)(3) = 3$~~
...

$1^{(142)} = 4$

$3^{(142)} = 3$

...

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

$1\,(1\,2\,3\,4\,5)(1\,4\,2)$

$= 2\,(1\,4\,2) = 1$

$SL_2(4)$ is generated by $a = \begin{bmatrix} 1 & 1 \\ \alpha & \beta \end{bmatrix}$, $b = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$

$$ab = \begin{bmatrix} 1 & 1 \\ \alpha & \beta \end{bmatrix}\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \beta & \alpha \end{bmatrix}$$

$$(ab)^2 = \begin{bmatrix} \alpha & \beta \\ \beta & \alpha \end{bmatrix}\begin{bmatrix} \alpha & \beta \\ \beta & \alpha \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$1^{(12345)(142)} = [1^{(12345)}]^{(142)} = 2^{(142)} = 1$

$|SL_2(5)| = |SL_2(\mathbb{F}_5)| = \frac{1}{4}|GL_2(5)| = \frac{1}{4}\cdot 480 = 120$

$|GL_2(5)| = (5^2-1)(5^2-5) = 24\cdot 20 = 480$

$|PSL_2(5)| = |SL_2(5)/\langle -I\rangle| = \frac{120}{2} = 60.$

$-I = \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix} = \begin{bmatrix}4 & 0\\ 0 & 4\end{bmatrix}$

$Z(SL_2(5)) = \langle -I\rangle = \{I, -I\}$ (center)

$Z(GL_2(5)) = \{\lambda I : \lambda \neq 0\}$

$\det(\lambda I) = \begin{vmatrix}\lambda & 0\\ 0 & \lambda\end{vmatrix} = \lambda^2$

$PSL_2(5)$ consists of all 2×2 matrices $\begin{bmatrix}x & y\\ z & w\end{bmatrix}$, $x,y,z,w \in \mathbb{F}_5$ with $xw - yz = 1$, where we identify $\pm\begin{bmatrix}x & y\\ z & w\end{bmatrix}$

$a = \pm\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$, $a^2 = \pm\begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}$, ..., $a^5 = \pm\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} = 1$

$b = \pm\begin{bmatrix}0 & 1\\ 4 & 4\end{bmatrix}$, $b^2 = \pm\begin{bmatrix}4 & 4\\ 1 & 0\end{bmatrix}$, $b^3 = \pm\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$

$ab = \pm\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}0 & 1\\ 4 & 4\end{bmatrix} = \pm\begin{bmatrix}4 & 0\\ 4 & 4\end{bmatrix} = \pm\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}$, $(ab)^2 = \pm\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$

$PSL_2(\mathbb{F}_5)$ can be identified with the 60 fractional linear transformations permuting $\mathbb{F}_5 \cup \{\infty\} = \{0,1,2,3,4,\infty\}$

$A_5 \cong SL_2(4) \cong PSL_2(5)$ of order 60; all are defined by the presentation $\langle a, b \mid a^5 = b^3 = (ab)^2 = 1\rangle$

Composition series for $SL_2(5)$:

$\langle I\rangle \triangleleft \langle -I\rangle \triangleleft SL_2(5)$

order 1 — order 2 — order 120

Why is $SL_2(\mathbb{F}_4) \cong A_5$? One way is to see that $SL_2(\mathbb{F}_4)$ permutes $\mathbb{F}_4 \cup \{\infty\} = \{0, 1, \alpha, \beta, \infty\}$ as fractional linear transformations

$$f_A(z) = \frac{az+b}{cz+d}, \quad A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$B = \begin{bmatrix} e & g \\ h & k \end{bmatrix}$, $f_B(z) = \frac{ez+g}{hz+k}$

$$f_B(f_A(z)) = (f_B \circ f_A)(z) = \frac{e\frac{az+b}{cz+d} + g}{h\frac{az+b}{cz+d} + k} \cdot \frac{cz+d}{cz+d} = \frac{e(az+b)+g(cz+d)}{h(az+b)+k(cz+d)}$$

$$= \frac{(ae+cg)z + (be+dg)}{(ah+ck)z + (bh+dk)} = f_C(z), \quad C = \begin{bmatrix} ae+cg & be+dg \\ ah+ck & bh+dk \end{bmatrix}$$

$f_b = (0, \beta)(\alpha, \infty)$

$$BA = \begin{bmatrix} e & g \\ h & k \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ae+cg & be+dg \\ ah+ck & bh+dk \end{bmatrix}$$

$$f_B \circ f_A = f_{BA}$$

$\{a \cdot 1 + b \cdot \beta : a, b \in \mathbb{F}_2\} = \{0, 1, \beta, \beta+1 = \alpha\}$

$\mathbb{F}_4 \supset \mathbb{F}_2$ is a 2-dim'l vector space with basis $\{1, \alpha\}$.

The map $GL_2(F) \longrightarrow \{\text{fractional linear transformations}\}$

$$A \longmapsto f_A \quad \text{where } f_A(z) = \frac{az+b}{cz+d}, \quad A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is a homomorphism. This homomorphism is onto but in general not one-to-one:

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \longmapsto f_I \qquad f_I(z) = \frac{1z+0}{0z+1} = z$

$\lambda I = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \qquad f_{\lambda I}(z) = \frac{\lambda z + 0}{0z+\lambda} = z$

The kernel of our homomorphism is $Z(GL_2(F)) = \{\lambda I : \lambda \in F, \ \lambda \neq 0\}$.

$$Z(SL_2(\mathbb{F}_4)) = \{\lambda I \in SL_2(\mathbb{F}_4) : \det(\lambda I) = 1\} = \{I\}$$

$\det \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} = \lambda^2 = 1 \iff \lambda = 1.$

Frac. lin. transf. over F are permutations of $F \cup \{\infty\}$

eg. $a = \begin{bmatrix} 1 & 1 \\ \alpha & \beta \end{bmatrix}$, $b = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$, $ab = \begin{bmatrix} \alpha & \beta \\ \beta & \alpha \end{bmatrix}$

$a^5 = b^3 = (ab)^2 = 1$

$f_a(z) = \frac{z+1}{\alpha z + \beta}$, $\quad f_a = (0, \alpha, \infty, \beta, 1)$

$f_b(z) = \frac{\alpha z + 0}{0z + \beta} = \beta z$, $\quad f_b = (1, \beta, \alpha)$

$f_{ab}(z) = \frac{\alpha z + \beta}{\beta z + \alpha}$, $\quad f_{ab} = (0, \alpha)(\beta, \infty) = f_a \circ f_b$

$\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$

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

·	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

$|A_8| = \frac{1}{2}8! = \frac{1}{2} \times 40320 = 20160$

$|GL_4(\mathbb{F}_2)| = (2^4-1)(2^4-2)(2^4-2^2)(2^4-2^3) = 15 \times 14 \times 12 \times 8 = 20160$

$GL_4(2) = SL_4(2) = PGL_4(2) = PSL_4(2)$

$|GL_3(4)| = (4^3-1)(4^3-4)(4^3-4^2) = 63 \cdot 60 \cdot 48 = 181,440$

$|SL_3(4)| = 60,480$

$Z(SL_3(4)) = \{cI : c \neq 0\} = \{I, \alpha I, \beta I\}$

$c\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix} = \begin{bmatrix}c&0&0\\0&c&0\\0&0&c\end{bmatrix}$, $c = 1, \alpha, \beta$ in $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$

$\det(cI) = c^3 = 1$

$PSL_3(4) = SL_3(4)/Z(SL_3(4))$. This group consists of invertible 3×3 matrices over $\mathbb{F}_4 = \{0,1,\alpha,\beta\}$ of determinant 1 in which we identify scalar multiples i.e. $A, \alpha A, \beta A$ give the same group element.

$|PSL_3(4)| = \frac{60,480}{3} = 20,160.$

Easy-ish fact: A_8, $GL_4(2)$ have elements of order 15; $PSL_3(4)$ does not. $PSL_3(4) \not\cong A_8$ or $GL_4(2)$.

A little harder: $A_8 \cong GL_4(2)$.

$(1\,2\,3\,4\,5)(6\,7\,8) \in A_8$ of order 15. Equivalently, $(1\,2\,3\,4\,5) \in A_5$ of order 5; $(6\,7\,8) \in A_8$ of order 3; and they commute.

Why does $GL_4(2)$ have an element of order 15? Consider $\mathbb{F}_{16} \supset \mathbb{F}_2$, an extension of degree 4.

$\mathbb{F}_{16}^\times$ is a multiplicative cyclic group of order 15. $\mathbb{F}_{16}^\times = \{1, \omega, \omega^2, \omega^3, \dots, \omega^{14}\}$, $\omega^{15} = 1$

$\mathbb{F}_{16} = \{0, 1, \omega, \omega^2, \dots, \omega^{14}\}$

$\mathbb{F}_{16} \longrightarrow \mathbb{F}_{16}$

$x \longmapsto \omega x$