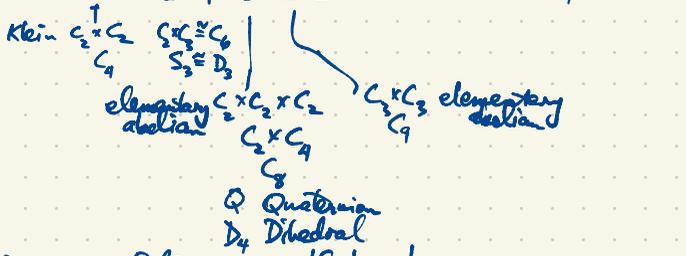


Group Theory

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	↑	267	1

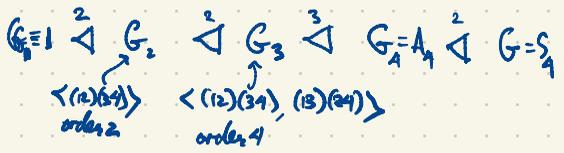


$|S_5| = 5! = 120$
 S_5 has composition series
 $1 \triangleleft A_5 \triangleleft S_5$

Simple groups $\left\{ \begin{array}{l} \text{cyclic of prime order} \\ \text{nonabelian simple groups of order} \end{array} \right.$
 60, 168, 360, 504, 660, 1092, 2498, 2520, 3120, 1050, ...

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



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 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, $e \geq 1$.

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

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

	0	1	α	β	
.	0	1	α	β	
0	0	0	0	0	0
1	0	1	α	β	1
α	0	α	β	1	α
β	0	β	1	α	β

$GL_n(F)$ = 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

$GL_2(\mathbb{F}_2) = \{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \} \cong S_3$

$GL_2(2)$

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

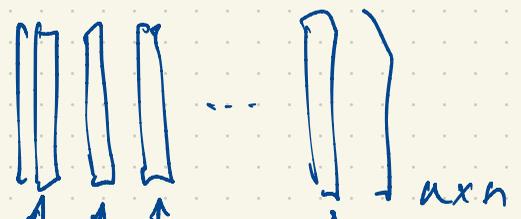
A Sylow p -subgroup

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

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

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

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



$q^n - 1$ choices

$q^n - q$ choices

$q^n - q^2$ choices

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

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

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

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

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

$$|SL_n(F_q)| = \frac{|GL_n(F_q)|}{q-1}$$

there is a surjective homomorphism $GL_n(F_q) \rightarrow F_q^* = \{ \text{nonzero field elements} \}$
 $A \mapsto \det A$

First isomorphism theorem: $GL_n(F_q) / SL_n(F_q) \cong F_q^*$

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

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

$$SL_2(\mathbb{F}_3) = \frac{1}{2} \cdot 180 = 60$$

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

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

+	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:

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

$a^5 = 1, \quad b^3 = 1, \quad (ab)^2 = 1.$

What does this mean?

In A_5 , let $a = (12345)$, $b = (142)$, so $ab = (12345)(142) = (23)(45)$

"left-to-right" composition: see handout

~~$$\begin{aligned} (142)(1) &= 4 \\ (142)(2) &= 1 \\ (142)(3) &= 3 \end{aligned}$$~~

$$(142): \begin{array}{l} 1 \mapsto 4 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \\ \dots \end{array}$$

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

$$1 (12345)(142)$$

$$= 2(142) = 1$$

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

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

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

$$1 (12345)(142)$$

$$\begin{aligned} &= \left[1 (12345) \right] (142) \\ &= 2(142) = 1 \end{aligned}$$

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

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

$$B = \begin{bmatrix} e & g \\ h & k \end{bmatrix}, \quad f_B(z) = \frac{ez+g}{gz+k}, \quad f_B \circ f_A(z) = (f_B \circ f_A)(z) = \frac{e \frac{az+b}{cz+d} + g}{h \frac{az+b}{cz+d} + k} \cdot \frac{cz+d}{cz+d} = \frac{e(az+b) + g(cz+d)}{h(az+b) + k(cz+d)}$$

$$= \frac{(ae+cg)z + (be+dg)}{(ah+ck)z + (bh+dk)} = f_C(z), \quad C = \begin{bmatrix} ae+cg & be+dg \\ ah+ck & bh+dk \end{bmatrix} \quad f_b = (0, \beta)(\alpha, \infty)$$

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

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

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

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

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

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mapsto f_I$$

$$f_I(z) = \frac{1z+0}{0z+1} = z$$

$$\lambda I = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$$

$$f_{\lambda I}(z) = \frac{\lambda z + 0}{0z + \lambda} = z$$

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

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

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

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

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

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

$$\mathbb{F}_7 = \{0, 1, \alpha, \beta\}$$

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

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

$$f_a(z) = \frac{z+1}{\alpha z + \beta}$$

$$f_a = (0, \alpha)(\beta, 1)$$

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

$$f_b = (1, \beta)(\alpha)$$

$$f_{ab}(z) = \frac{\alpha z + \beta}{\beta z + \alpha}$$

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