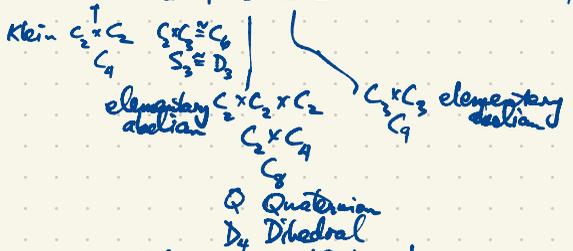


# Group Theory

*Book 1*

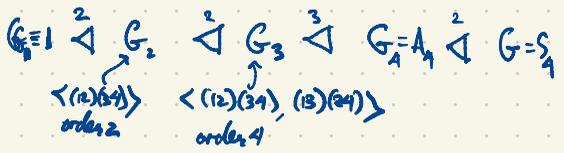
Finite groups (up to isomorphism)

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



$S_n$  = 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  $n \geq 5$ .

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

Simple groups:
 

- cyclic of prime order
- nonabelian simple groups of order

60, 168, 360, 504, 660, 1092, 2498, 2520, 3120, 1050, ...  
 $SL_3(2) \cong PSL_2(7)$   
 $SL_2(4) \cong PSL_2(5) \cong A_5$

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	$\alpha$	$\beta$
+	0	1	$\alpha$	$\beta$
0	0	1	$\alpha$	$\beta$
1	0	0	$\beta$	$\alpha$
$\alpha$	$\alpha$	$\beta$	0	1
$\beta$	$\beta$	$\alpha$	1	0

	0	1	$\alpha$	$\beta$
.	0	1	$\alpha$	$\beta$
0	0	0	0	0
1	0	1	$\alpha$	$\beta$
$\alpha$	0	$\alpha$	$\beta$	1
$\beta$	0	$\beta$	1	$\alpha$

$GL_n(F)$  = 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

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

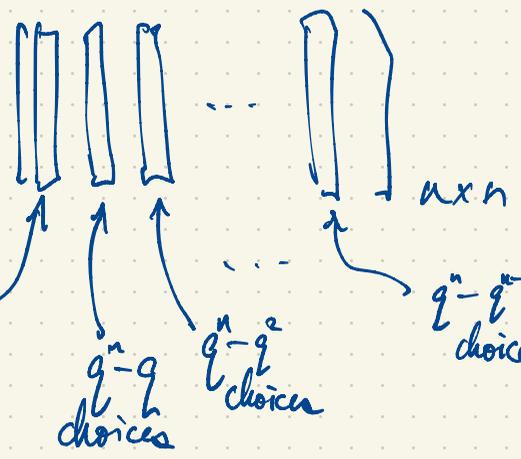
$GL_2(2)$

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

A Sylow  $p$ -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.



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

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

$GL_3(2)$  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  $F$   
 $= \{ A \in GL_n(F) : \det A = 1 \}$

$$|SL_n(F)| = \frac{|GL_n(F)|}{|F^\times|}$$

there is a surjective homomorphism  $GL_n(\mathbb{F}_q) \rightarrow \mathbb{F}_q^\times = \{ \text{nonzero field elements} \}$   
 $A \mapsto \det A$

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

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

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	$\alpha$	$\beta$
0	0	1	$\alpha$	$\beta$
1	1	0	$\beta$	$\alpha$
$\alpha$	$\alpha$	$\beta$	0	1
$\beta$	$\beta$	$\alpha$	1	0

·	0	1	$\alpha$	$\beta$
0	0	0	0	0
1	0	1	$\alpha$	$\beta$
$\alpha$	0	$\alpha$	$\beta$	1
$\beta$	0	$\beta$	1	$\alpha$

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:

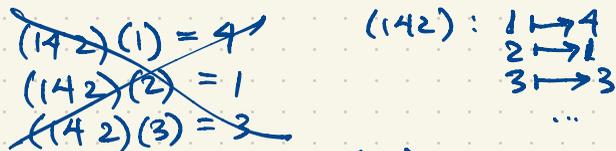
$$A_5 \cong \langle a, b \mid a^5 = b^3 = (ab)^2 = 1 \rangle = \text{the group generated by } a, b \text{ subject to three relations}$$

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

What does this mean?

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

"left-to-right" composition: see handout



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

$$1 (12345)(142)$$

$$= 2(142) = 1$$

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

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

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

$$1 (12345)(142)$$

$$\begin{aligned} &= \begin{bmatrix} 1 & (12345) \end{bmatrix} (142) \\ &= 2(142) = 1 \end{aligned}$$



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

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

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

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

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

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

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

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

$\mathbb{F}_q \supset \mathbb{F}_2$  is a 2-dimensional vector space with basis  $\{1, \alpha\}$ .

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

+	0	1	$\alpha$	$\beta$
0	0	1	$\alpha$	$\beta$
1	1	0	$\beta$	$\alpha$
$\alpha$	$\alpha$	$\beta$	0	1
$\beta$	$\beta$	$\alpha$	1	0

·	0	1	$\alpha$	$\beta$
0	0	0	0	0
1	0	0	$\alpha$	$\beta$
$\alpha$	0	$\alpha$	$\beta$	1
$\beta$	0	$\beta$	1	$\alpha$

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  $F \cup \{\infty\}$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$PSL_3(4) = SL_3(4)/Z(SL_3(4))$ . This group consists of invertible  $3 \times 3$  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 harder:  $A_8 \cong GL_4(2)$ .

$(12345)(678) \in A_8$  of order 15. Equivalently,  $(12345) \in A_5$  of order 5;  $(678) \in A_3$  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.  $\mathbb{F}_{16}^\times = \{1, \omega, \omega^2, \omega^3, \dots, \omega^{14}\}$ ,  $\omega^{15} = 1$ .  $\mathbb{F}_{16} = \{0, 1, \omega, \omega^2, \dots, \omega^{14}\}$

$$\begin{aligned} \mathbb{F}_{16} &\rightarrow \mathbb{F}_{16} \\ x &\mapsto \omega x \end{aligned}$$

$$f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$$

$$\mathbb{F}_{16} = \mathbb{F}_2[\omega] \text{ where } \omega \text{ is a root of } f(x)$$

$$= \{a + b\omega + c\omega^2 + d\omega^3 : a, b, c, d \in \mathbb{F}_2\}$$

$$\omega^4 = \omega + 1$$

Equivalently, take  $A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$  (companion matrix for  $f(x)$ )

$$\text{so } A^4 = A + I$$

$$\mathbb{F}_2[A] = \{aI + bA + cA^2 + dA^3 : a, b, c, d \in \mathbb{F}_2\}$$

$\subset$   $\{4 \times 4 \text{ matrices over } \mathbb{F}_2\}$ .

$$\{0, I, A, A^2, \dots, A^{14}\}, \quad A^{15} = I.$$

$A \in GL_4(2)$  has order 15.

Claim:  $PSL_3(4)$  has no element of order 15. (So it cannot be isomorphic to  $A_5$  or  $GL_2(5)$ .)

Proof: Suppose  $A \in PSL_3(4)$  has order 15, so  $A^3$  has order 5 and  $A^5$  has order 3; here  $A^3$  and  $A^5$  commute.

By Sylow theory, any two subgroups of order 5 are conjugate in  $G = PSL_3(4)$ .  $\langle A^3 \rangle$  is a Sylow 5-subgroup  
WLOG,  $A^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \beta \end{bmatrix}$ . Next use a general fact from linear algebra

If  $A, B$  are  $n \times n$  matrices which commute ( $AB=BA$ ) then every eigenspace for  $A$  is an invariant subspace for  $B$   
i.e. if  $Av = \lambda v$  then  $A(Bv) = \lambda(Bv)$ . Proof:  $A(Bv) = B(Av) = B(\lambda v) = \lambda(Bv)$ .

$A^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \beta \end{bmatrix}$  has  $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$  as an eigenvector with eigenvalue 1, and  $A^5$  commutes with  $A^3$  so  $\langle \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \rangle$  is invariant under  $A^5$ .  
( $\begin{bmatrix} \alpha \\ 0 \\ 0 \end{bmatrix}$  doesn't have eigenvalue 1, so the 1-eigenspace of  $A^3$  is  $\langle \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \rangle$ .)

so  $A^5 = \begin{bmatrix} c & * & * \\ 0 & * & * \\ 0 & * & * \end{bmatrix}$   $c \neq 0 \Rightarrow c \in \{1, \alpha, \beta\}$ , WLOG  $c=1$  so  $A^5 = \begin{bmatrix} 1 & * & * \\ 0 & * & * \\ 0 & * & * \end{bmatrix}$  has order 3 in  $G$

$A^5 = \begin{bmatrix} 1 & * & * \\ 0 & C & * \\ 0 & 0 & C \end{bmatrix}$  where  $C \in SL_2(4)$ ,  $C^3 = I$ .  $|SL_2(4)| = 60 = 2^2 \cdot 3 \cdot 5$ .  $C^3$  is conjugate (in  $SL_2(4)$ ) to  $\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$   
and  $C^3$  commutes with  $\begin{bmatrix} \alpha \\ 0 \\ 0 \end{bmatrix}$ . However,  $\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$  has two <sup>distinct</sup> eigenspaces  $\langle \begin{bmatrix} 1 \\ 0 \end{bmatrix} \rangle$ ,  $\langle \begin{bmatrix} 0 \\ 1 \end{bmatrix} \rangle$  and so  
 $C^3$  has two distinct eigenspaces and these are not invariant under  $\begin{bmatrix} \alpha \\ 0 \\ 0 \end{bmatrix}$  which has no eigenvectors;  
its char. poly. is irreducible over  $\mathbb{F}_4$ . Contradiction!

More examples of group presentations:

The dihedral group of order  $2n$  has presentation  $\langle a, b : a^n = b^2 = 1, bab^{-1} = a^{-1} \rangle$

The cyclic group of order  $n$  is  $\langle a : a^n = 1 \rangle$

The symmetric group  $S_n$  of degree  $n \geq 3$  is generated by  $(1, 2), (1, 2, 3, \dots, n)$ , but not in a convenient way since their relations are very complicated.

We might instead use all  $\binom{n}{2}$  transpositions  $(i, j), 1 \leq i < j \leq n$  or simply the  $n-1$  transpositions  $(i, i+1), 1 \leq i \leq n-1$

$S_n$  has presentation  $\langle r_1, \dots, r_{n-1} : r_i^2 = r_{i+1}^2 = \dots = r_{n-1}^2 = 1, (r_i r_{i+1})^3 = 1 \text{ for } i=1, 2, \dots, n-2, (r_i r_j)^2 = 1 \text{ for } 1 \leq i < j \leq n-1, |i-j| \geq 2 \rangle$

$= \langle r_1, \dots, r_{n-1} : (r_i r_j)^2 = 1 \text{ if } i=j \text{ or } |i-j| \geq 2; (r_i r_j)^3 = 1 \text{ if } |i-j|=1 \rangle$

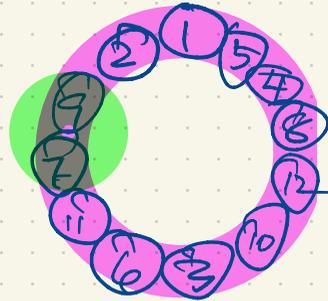
$S_n$  is an example of a Coxeter group  $\langle r_1, \dots, r_{n-1} : r_i r_j = 1 \text{ if } i=j \rangle$

i.e. a group given by a presentation  $\langle r_1, \dots, r_{n-1} : (r_i r_j)^{m_{ij}} = 1 \rangle$ ,

$A_n < S_n, |A_n| = \frac{1}{2} n!$ ,  $A_n$  is generated by

$$\begin{aligned} g_1 &= (12)(23) = (1, 3, 2) \\ g_2 &= (12)(34) \\ g_3 &= (12)(45) \\ &\vdots \\ g_{n-2} &= (12)(n-1, n) \end{aligned}$$

$$\frac{bab^{-1} = a^{-1}}{\text{relation}} \leftrightarrow \frac{abab^{-1} = 1}{\text{relation}}$$



$(3, 4)(7, 8)$  has order 2

$(3, 4)(4, 5) = (3, 5, 4)$  has order 3

$(3, 4)(3, 4) = 1 \dots$

$$m_{ii} = 1, m_{ij} = m_{ji} \geq 1$$

$$g_i^2 = 1, g_i^2 = g_3^2 = \dots = g_{n-2}^2 = 1$$

$$(g_i g_j)^2 = 1 \text{ if } |i-j| \geq 2$$

$$(g_i g_j)^3 = 1 \text{ if } |i-j|=1$$

$$\mathcal{A}_8 \cong GL_4(2)$$

**2.5 Satz.** Sei  $V = V(4, 2)$  der Vektorraum der Dimension 4 über dem Körper  $GF(2)$  und  $GL(4, 2)$  die Gruppe aller linearen Abbildungen von  $V$  auf sich. Dann gilt  $GL(4, 2) \cong \mathcal{A}_8$ .

**Beweis.** Die Matrizen

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \quad G_2 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

$$G_3 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad G_4 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$G_5 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad G_6 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

liegen in  $GL(4, 2)$ . Triviale, aber etwas langwierige Rechnungen zeigen, daß sie die in I, 19.8 (S. 138) angegebenen definierenden Relationen

$$G_i^3 = G_i^2 = E \quad (2 \leq i \leq 6), \quad (G_i G_{i+1})^3 = E \quad (1 \leq i \leq 5),$$

$$(G_i G_j)^2 = E \quad (i + 1 < j)$$

von  $\mathcal{A}_8$  erfüllen. Also ist  $\mathfrak{G} = \langle G_1, \dots, G_6 \rangle$  ein epimorphes Bild von  $\mathcal{A}_8$ . Da  $\mathcal{A}_8$  nach 2.4 einfach ist, folgt  $\mathfrak{G} \cong \mathcal{A}_8$ . Eine einfache Rechnung zeigt (siehe auch II, 6.2)  $|GL(4, 2)| = |\mathcal{A}_8|$ . Wegen  $\mathfrak{G} \leq GL(4, 2)$  folgt jetzt  $\mathfrak{G} = GL(4, 2) \cong \mathcal{A}_8$ . **q.e.d.**

B. Huppert,  
Endliche Gruppen I  
1967.

With no relations in a group presentations, we have a free group.

$$F_n = \langle r_1, \dots, r_n \rangle = \text{free group on } n \text{ generators} = \{ \text{all (finite) products of } r_1, \dots, r_n, r_1^{-1}, r_2^{-1}, \dots, r_n^{-1} \}$$

↑ no relations

$$r_i^k r_i^l = r_i^{k+l}, \quad r_i^0 = 1.$$

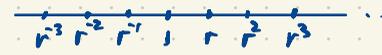
$$F_1 = \langle r \rangle = \{ \dots, r^3, r^2, r, 1, r, r^2, r^3, \dots \} = \text{infinite cyclic group} \cong \mathbb{Z}$$

Informally,  $F_1 = \mathbb{Z}$ .

$$\mathbb{Z} \xrightarrow{\cong} F_1$$

$$k \mapsto r^k$$

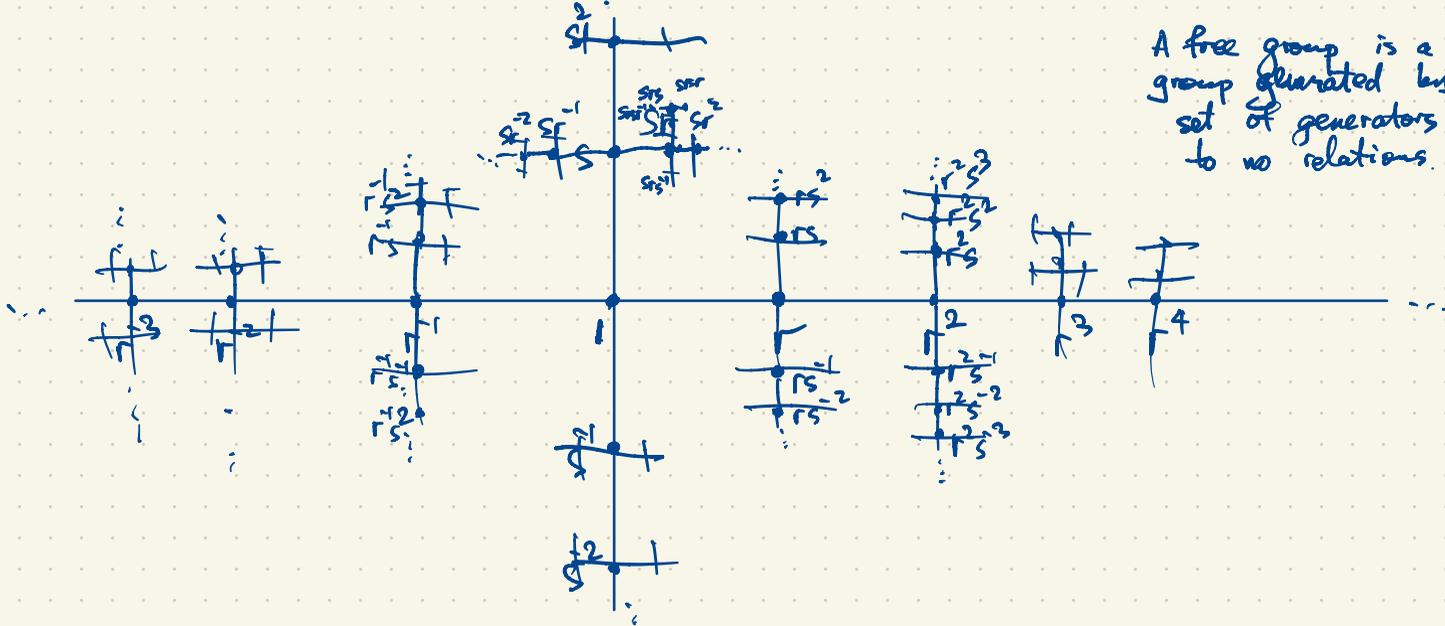
$$d(r^i, r^j) = |i-j|$$



$F_0 = \{1\}$  trivial group

$$F_2 = \langle r, s \rangle = \{ \text{all products of powers of } r \text{'s and } s \text{'s} \} = \{ 1, r, r^{-1}, s, s^{-1}, rs, rs^{-1}, \dots, r^3 s^{-1} r^2 s^3 r, \dots \}$$

A free group is a group generated by a set of generators subject to no relations.



A group presentation expresses a group  $G$  as  $G \cong \langle X | R \rangle$

$\uparrow$  set of generators i.e. literal symbols  
 $\uparrow$  relations: words on the symbols

Words: strings of letters  
 Every relation can be rewritten as  $w=1$  where the relator  $w$  is a word i.e.  $w \in \langle X \rangle$

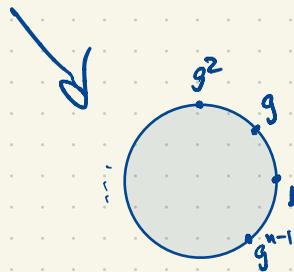
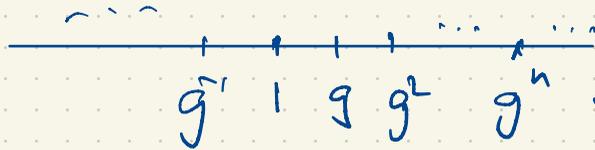
$G = \langle X | R \rangle$  is a homomorphic image of the free group  $\langle X \rangle$ ;

$$\langle X \rangle \longrightarrow \langle X | R \rangle = \langle X \rangle / K \quad \text{where } K \trianglelefteq \langle X \rangle \text{ is the normal subgroup generated by elements of } R \text{ and their conjugates in } \langle X \rangle.$$

eg.  $C_n = \langle g | g^n = 1 \rangle = \langle g | g^n \rangle = \langle g \rangle / \langle g^n \rangle = \{ \dots, g^3, g^2, g^1, 1, g, g^2, g^3, \dots \} / \{ \dots, g^{2n}, g^n, 1, g, g^{2n}, \dots \}$

$\uparrow$  one generator       $\uparrow$  one relator

$$= \{ 1, g, g^2, \dots, g^{n-1} \}$$



$$\langle r, s \mid rs = sr \rangle = \langle r, s \mid r^i s^j r s = 1 \rangle = \langle r, s \mid r^i s^j r s \rangle = \{ r^i s^j \mid i, j \in \mathbb{Z} \} \cong \mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$$

free abelian group on two generators

$$S_3 = \langle r, s \mid r^2 = s^2 = (rs)^3 = 1 \rangle = \langle r, s \mid r^2, s^2, (rs)^3 \rangle$$

If we have a group  $G$  generated by two elements  $r, s$  satisfying  $r^2 = s^2 = (rs)^3 = 1$ , then we show  $|G| = 1, 2$  or  $6$  and  $G$  is  $1, C_2$  or  $S_3$  respectively.

Elements of  $G$  are products of powers of  $r$  and  $s$ . Since  $r^{-1} = r$  and  $s^{-1} = s$ , elements of  $G$  must have the form  $1, r, s, rs, sr, rsr, srs, rsrs, srsr, \dots$

$$\text{But } rsrsrs = 1 \Rightarrow rsrsrs \cdot srs = 1 \cdot srs \Rightarrow rsr = srs \Rightarrow rsrs = srsr = sr$$

so  $G = \{ 1, r, s, rs, sr, rsr \}$  (at most six distinct elements)

If these six elements are distinct then  $G \cong S_3$ ; an isomorphism  $G \rightarrow S_3$  is given by  $r \mapsto (12), s \mapsto (23), (rs = (132) \text{ etc.})$

These three possibilities for  $G$  are all realizable and no other possibilities occur.

All possibilities arise as  $S_3/K$  where  $K \triangleleft S_3$ . ( $K = 1, A_3 = \langle rs \rangle = \langle (123) \rangle$ , or  $S_3$ ).

---

Next consider

$$G = \langle r, s \mid r^3, s^3, (rs)^2 \rangle$$

A group  $G$  generated by two elements  $r, s$  satisfying  $r^3 = s^3 = (rs)^2 = 1$  has

$$|G| = 1, 3 \text{ or } 12 \quad (I, C_3, \text{ or } A_4)$$

Coxeter, Todd (1936) described an algorithm for determining  $G$  from its presentation.

We will deduce  $|G| \leq 12$  by showing  $G$  has a subgroup  $H$  with  $|H| \leq 3$  and  $[G:H] \leq 4$ .

(So  $|G| = [G:H]|H| \leq 4 \cdot 3 = 12$ .)

(Lagrange's theorem)

Recall: Right cosets of  $H \leq G$  have the form  $Hg = \{hg : h \in H\}$ ,  $g \in G$ ;  $|Hg| = |H|$   
 $G$  permutes the right cosets of  $H$  by  $Hx \mapsto Hxg$ .

Let's take  $H = \langle r \rangle$  so  $|H| = 1$  or  $3$ . Right cosets of  $H$  in  $G$ :

(1) •  $H = H1 = Hr$

(2) •  $Hs$

(3) •  $Hs^2 = Hsr$

(4) •  $Hs^2r = Hsr^2$

$$rsrs = 1 \implies rsrs \cdot s^2r^2 = 1 \cdot s^2r^2 \implies rs = s^2r^2$$

$$sr = r^2s^2$$

$$Hsr = Hr^2s^2 = Hs^2$$

$$(Hs^2r)s = Hs^2 \cdot s^2r^2 = Hsr^2 = Hs^2r$$

$$Hsr^2 = Hsr \cdot r = Hr^2s^2 \cdot r = Hs^2r$$

$A_4$  has normal subgroups  $I$ ,  $\langle (12)(34), (13)(24) \rangle$ ,  $A_4$

These must be the only right cosets of  $H$  (not necessarily distinct)

Right multiplication by  $s$  permutes the right cosets of  $H$  as  $(123)(4) = (123)$

$$(1)(234)$$

Assuming we actually have 4 distinct right cosets of  $H$  in  $G$  then  $[G:H] = 4$ ,  $|H| = 3$  and  $|G| = 12$ .  
 And we have an isomorphism  $G \rightarrow A_4$ ,  $r \mapsto (234)$ ,  $s \mapsto (123)$ . So  $rs \mapsto (234)(123) = (12)(34)$

$$G = \langle r, s \mid r^3, s^3, (rs)^2 \rangle, \quad H = \langle r \rangle$$

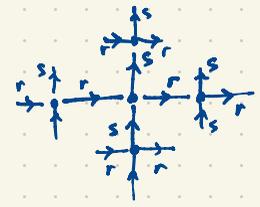
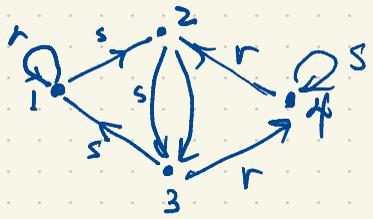
$$Hr = H$$

	r	r	r	s	s	s	r	s	r	s
1	1	1	1	2	3	1	1	2	3	1
2	3	4	2	3	1	2	3	1	1	2
3	4	2	3	1	2	3	4	4	2	3
4	2	3	4	4	4	4	2	3	4	4

This is the Coxeter-Todd coset enumeration algorithm.  
 The largest (i.e. most general) group generated by two elements  $r, s$  satisfying  $r^3 = s^3 = (rs)^2 = 1$  has  $[G:H] = 4, |H| = 3, |G| = 12$ .

Such a group is represented as a permutation group  $\langle (234), (123) \rangle = A_4$ .  
 $\langle r, s \mid r^3, s^3, (rs)^2 \rangle \cong A_4 = F_2 / \text{normal subgp. gen. by } r^3, s^3, (rs)^2 \text{ and their conjugates}$

The Schreier graph of  $G = \langle r, s \mid r^3, s^3, (rs)^2 \rangle$  on the cosets of  $H = \langle r \rangle$



- vertex 1 represents  $H = H1$
- 2 - -  $Hs$
- 3 - -  $Hs^2$

This tree is the Cayley graph of  $F_2 = \langle r, s \rangle$  (free group on two generators)

$S_3 \cong \langle r, s \mid r^2, s^2, (rs)^3 \rangle$  on cosets of  $H = \langle r \rangle$

Coxeter diagram

When generators of  $G$  have order 2, write  $\text{---}$  in place of  $\text{---}$  instead of  $\text{---}$

Schreier graph



$rsrsrs = 1$

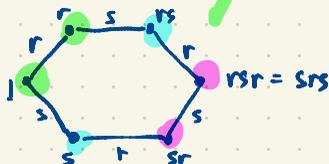
$rsrsrs \cdot srs = 1 \cdot srs$

$rsr = srs$

$(Hsr)s = Hsr = Hsr$

branched cover

$S_3$  on cosets of  $H = \{1\}$ : Schreier graph reduces to a Cayley graph: vertices of graph are elements of  $G$  (same as cosets of  $\{1\}$ )



Cayley graph of  $S_3$ : homeomorphic to  $S^1 = \text{circle}$

(12) (23) (31)

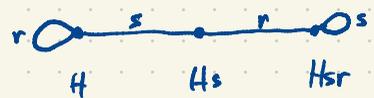
$(rt)^2 = rtot = 1$   
 $rt \cdot t \cdot r = 1 \cdot tr$

A Coxeter group is a group having a presentation using generators and relators  $(rs)^2, (rt)^2, (st)^2, \dots$  (all exponents are positive integers)

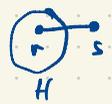
$\langle r, s \mid r^2, s^2, (rs)^2 \rangle$  has Coxeter diagram  $\text{---}$

This Coxeter group is a Klein 4-group  $C_2 \times C_2$

$S_3$  has Schreier graph on subgroup  $H = \langle r \rangle$ .



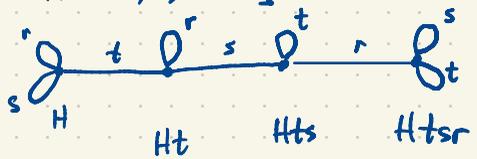
Coxeter diagram



$$S_4 = \langle r, s, t : r^2, s^2, t^2, (rs)^2, (rt)^2, (st)^2 \rangle$$

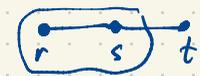
Find Schreier graph on

$$H = \langle r, s \rangle \cong S_3$$



Coxeter diagram

$$rt = tr$$



$$sts = tst$$

$$Hr = H$$

$$Hs = H$$

$$(Ht)r = Htr = Ht$$

$$(Hts)t = Hsts = Hts$$

$$(Htsr)t = Htstr = Htsr = Htsr$$

$$|S_4| = 4 \times 6 = 24$$

$S_n$  has Coxeter diagram  $A_{n-1} = 1 - 2 - 3 - \dots - n-1$

$S_n = W(A_{n-1}) =$  Weyl group (Coxeter group) of type  $A_{n-1}$

$$|S_n| = n! = n |S_{n-1}|$$

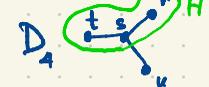
Next few lectures:

- more examples of Coxeter groups
- buildings
- Burnside problems
- presentations in algebraic topology

### Coxeter Diagrams

$A_n$   (n nodes)  $W(A_n) \cong S_{n+1}$

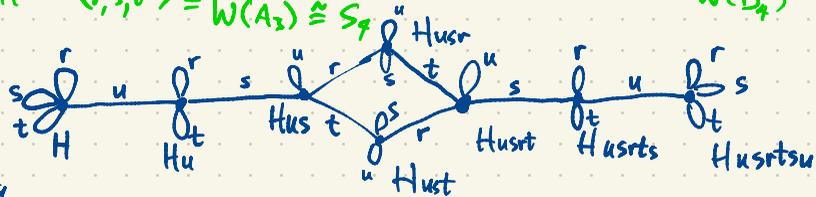
$D_n$   (n nodes)



$|W(D_4)| = 192$

$W(D_4) = \langle r, s, t, u : r^2, s^2, t^2, u^2, (rt)^2, (ru)^2, (tu)^2, (rs)^3, (st)^3, (su)^3 \rangle$   
 $H = \langle r, s, t \rangle \cong W(A_3) \cong S_4$  Enumerate cosets of H in  $G = W(D_4)$ .  
 $rt = tr, ru = ur, ut = tu, rsr = srs, sts = tst, sus = uss$

### Schreier diagram:



$[G:H] = 8$   
 $|G| = 8 \times 24 = 192$

$Hur = Hru = Hu$

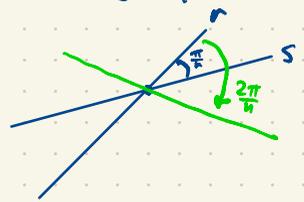
$(Hus)_u = Hsus = Hus$

$(Husr)_u = Husur = Hsusr = Husr$

$(Husr)_s = Hursr = Hrusr = Husr$

$Husr_t = Hustr$

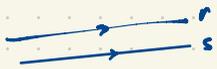
Coxeter groups are groups generated by reflections  
 Consider a group generated by two reflections  $r, s$  of a Euclidean plane whose axes are angle  $\frac{\pi}{n}$  apart



$r^2 = s^2 = 1, (rs)^n = 1$

$rs$  (left-to-right composition) is a rotation by angle  $\frac{2\pi}{n}$  about the intersection point of the two axes.

$\langle r, s \mid r^2, s^2, (rs)^n \rangle$  is dihedral of order  $2n$ .



$\langle r, s | r^2, s^2 \rangle$  is an infinite dihedral group  
with infinite cyclic subgroup  $\langle rs \rangle$

When studying Coxeter groups, we often focus on the subgroup of index 2 generated by products of an even number of generating reflections (just like the alternating subgroup of  $S_n$ ).