

# Group Theory

**Written by: Hayder Abbas Janabi**

PhD student at Budapest University of Technology and Economics, Budapest, Hungary.

Lecturer at University of Kufa, Najaf, Iraq.

E-mail: `haydera.janabi@uokufa.edu.iq`

**October, 2020**

Based on the lecture given by Dr. Erzsébet Horváth in the spring semester 2018.

**For MSc (Mathematics, Physics, etc) students, to the subject Group Theory.**

This lecture notes is refereed by:

Dr.Kiss Sándor

Department of Algebra

Budapest University of Technology and Economics.

**This work was supported by the NKFI-Grant No. 115288 and by the Stipendium Hungaricum PhD fellowship at the Budapest University of Technology and Economics.**

## List of Symbols

$[H, K]$  commutator subgroup

$[x, y]$  commutator element of  $x$  and  $y$

$\Gamma(G, X)$  Cayley graph of  $G$  with generators  $X$

$\omega^G$   $G$ -orbit of  $\omega$

$\Phi(G)$  Frattini subgroup of  $G$

$A \leq B$  subgroup

$A \triangleleft B$  normal subgroup

$A \rtimes B$  semidirect product

$A \wr B$  wreath product

$a \sim b$   $a$  is conjugate to  $b$

$Aut_c(\Gamma(G, X))$  colour preserving automorphisms of the Cayley graph

$C_G(x)$  centralizer of the element  $x$  in  $G$

$cl(G)$  nilpotency class of  $G$

$Core_G(H)$  maximal normal subgroup of  $G$  contained in  $H$

$d.l.(G)$  derived length of  $G$

$F(G)$  Fitting subgroup of  $G$

$F(X)$  free group with free generating set  $X$

$F_n$  free group of rank  $n$

$Fix(\pi)$  the set of fixed point of permutation  $\pi$

$G = \langle x_1, \dots, x_n \mid r_1, \dots, r_k \rangle$  group given by generators and relations

$g^x = x^{-1}gx$  conjugate of an element  $g$  by  $x$

$G'$  derived subgroup

$G^{(i)}$   $i^{\text{th}}$  member of the derived series

$G_\omega$  point stabilizer of  $\omega$

$G_{\alpha_1, \dots, \alpha_n}$  pointwise stabilizer of set  $\{\alpha_1, \dots, \alpha_n\}$

$H^x = x^{-1}Hx$  conjugate of a subset  $H$  by  $x$

$\text{Hall}_\pi(G)$  the set of Hall  $\pi$ -subgroups of  $G$

$I(\pi)$  the set of inversions of permutation  $\pi$

$K_G(x)$   $G$ -conjugacy class of the element  $x$

$K_i(G)$  the  $i^{\text{th}}$  member of the lower central series of  $G$

$o(x)$  order of an element  $x$

$\text{Syl}_p(G)$  the set of Sylow  $p$ -subgroups of  $G$

$V : G \rightarrow Q/Q'$  transfer map

$Z(G)$  centre of  $G$

$Z^i(G)$  the  $i^{\text{th}}$  member of the upper central series of  $G$

# Contents

<b>1</b>	<b>Permutation groups, the automorphism group of <math>S_n</math></b>	<b>6</b>
<b>2</b>	<b>Application of the Sylow theorems, small groups</b>	<b>16</b>
<b>3</b>	<b><math>k</math>-transitive and primitive groups</b>	<b>18</b>
<b>4</b>	<b>Group extensions, semidirect product, wreath product</b>	<b>22</b>
4.1	The Sylow $p$ -subgroups of symmetric groups . . . . .	24
<b>5</b>	<b>Solvable groups and nilpotent groups</b>	<b>25</b>
<b>6</b>	<b>Hall theorems, and the Schur-Zassenhaus theorem</b>	<b>35</b>
<b>7</b>	<b>Normal <math>p</math>-complement theorems and the transfer</b>	<b>40</b>
<b>8</b>	<b>Free groups, the Nielsen-Schreier theorem</b>	<b>45</b>
<b>9</b>	<b>Problem sheets</b>	<b>53</b>
	<b>Index</b>	<b>66</b>

# 1 Permutation groups, the automorphism group of $S_n$

**Definition 1.1.**  $G$  is a **group** if there exists a binary operation  $\cdot : G \times G \rightarrow G$  (denoted by  $\cdot$  or by just writing letters beside each other) such that the following axioms are satisfied:

1.  $(ab)c = a(bc)$  for all  $a, b, c \in G$ . (associativity)
2. There exists an element  $e \in G$  such that  $ea = ae = a$  for all  $a \in G$ . (there exists a unit element)
3. For all  $x \in G$  there exists an element  $y \in G$  such that  $xy = e = yx$  (all element has an inverse, let us denote this  $y$  by  $x^{-1}$ ).

**Remark 1.1.**  $e$  and  $x^{-1}$  are unique. (see Algebra 1)

**Definition 1.2.** Let  $\Omega := \{1, 2, \dots, n\}$ . A **permutation** of  $\Omega$  is a bijective map  $\pi : \Omega \rightarrow \Omega$ . These form a group under composition. It is called the **symmetric group** of degree  $n$ , denoted by  $S_n$  (or  $S_\Omega$ ) and its order is  $|S_n| = n!$ .

**Definition 1.3.**  $G$  is a **permutation group** of degree  $n$  if  $G \leq S_n$ . (or it is isomorphic to a subgroup of  $S_n$ ).

**Definition 1.4.** A **group action** on  $\Omega$  (or **permutation representation**) is a homomorphism  $\varphi : G \rightarrow S_\Omega$  such that  $g \mapsto \varphi(g)$ . and the group  $G$  acts in the following way on  $\Omega : \omega^g := \omega^{\varphi(g)}$ . Then  $\omega^{(gh)} = \omega^{\varphi(gh)} = \omega^{\varphi(g)\varphi(h)} = (\omega^g)^h$ .

**Definition 1.5.** The group action  $\varphi$  is **faithful** if  $\ker \varphi = \{1\}$ , then  $G \cong \varphi(G) \leq S_n$  and we get a permutation group.

**Definition 1.6.** The group action is **transitive** on  $\Omega$  if for all  $\alpha, \beta \in \Omega$ , there exists an element  $g \in G$  such that  $\alpha^g = \beta$ .

**Remark 1.2.** In this note permutation will always act from the right, and multiply from the left.

**Remark 1.3.** We know from (Algebra 1) that every permutation can be written as a product of disjoint cycles uniquely (up to the order of the cycles). We note that disjoint cycles always commute.

**Example 1.1.**  $(123)(1453) = (12)(345)$   
 $(123)^{-1} = (321), (123)^2 = (132), (123)^3 = () = id.$

**Theorem 1.7.** If  $\pi \in S_n$ ,  $\pi = \pi_1 \cdots \pi_k$  is a product of disjoint cycles with lengths  $n_1, \dots, n_k$ , then  $o(\pi) = \text{lcm}(n_1, \dots, n_k)$ , where  $\text{lcm}$  is the least common multiple. (here  $o(\pi)$  is the order of the element  $\pi$ )

*Proof.*  $o(\pi) = \min\{k \geq 1 \mid \pi^k = id\}$ . Let  $\text{lcm}(n_1, \dots, n_k) = l$  and  $l = n_i \beta_i$

then  $\pi^l = (\pi_1 \cdots \pi_k)^l = \pi_1^l \cdots \pi_k^l = (\pi_1^{n_1})^{\beta_1} \cdots (\pi_k^{n_k})^{\beta_k} = 1$

(We know if  $x^N = 1$  then  $o(x) \mid N$ ) (see problem sheet 1/5)

thus:

if  $\pi^l = 1$  then  $o(\pi) \mid l$ .

On the other hand:

$1 = \pi^{o(\pi)} = (\pi_1 \cdots \pi_k)^{o(\pi)} = \pi_1^{o(\pi)} \cdots \pi_k^{o(\pi)}$ . Since  $\pi_1, \dots, \pi_k$  act on disjoint sets, if the product is 1 then  $\pi_i^{o(\pi)} = 1$  for all  $i$ , hence  $o(\pi_i) \mid o(\pi) \forall i$ . Hence  $\text{lcm}(o(\pi_1), \dots, o(\pi_k)) \mid o(\pi)$  and so  $l = o(\pi)$ . □

**Definition 1.8.** If  $\pi \in S_n$ , then  $I(\pi) := \{(i, j) \mid i < j \text{ and } \pi(i) > \pi(j)\}$  is the set of **inversions** of  $\pi$ . The permutation  $\pi$  is **even** if it has even number of inversions.  $\pi$  is **odd** if it has odd number of inversions.

**Remark 1.4.** Let  $p(x_1, \dots, x_n) := \prod_{1 \leq i < j \leq n} (x_i - x_j)$ . and let  $\pi$  act by permuting the indices  $p^\pi = \prod_{1 \leq i < j \leq n} (x_{\pi(i)} - x_{\pi(j)})$  and  $\pi$  is odd if and only if  $p^\pi = -p$ ,  $\pi$  is even if and only if  $p^\pi = p$ .

**Definition 1.9.**  $A_n := \{\pi \in S_n \mid \pi \text{ is an even permutation}\}$ .

**Remark 1.5.** Let  $\varphi : S_n \rightarrow \{\pm 1\} = C_2$  where  $\pi \mapsto (-1)^{|I(\pi)|}$ . This is a group homomorphism.  $\ker \varphi = A_n$  thus  $A_n \triangleleft S_n$  and  $\text{Im } \varphi = C_2$ . By the homomorphism theorem we have

that  $S_n/\ker \varphi \cong \text{Im } \varphi = C_2$ . So  $\frac{|S_n|}{|\ker \varphi|} = 2$  and  $[S_n : A_n] = 2$ . Thus  $A_n$  is an index 2 normal subgroup in  $S_n$ . The name of  $A_n$  is **alternating group of degree  $n$** .

**Theorem 1.10.** *If  $n \geq 5$  then  $A_n$  is simple. (see problem sheet 1/4)*

**Definition 1.11.** A 2-cycle  $(\alpha, \beta)$  is called **transposition**.

**Remark 1.6.** Every permutation is a product of transpositions. It is enough to prove for cycles:  $(1, 2, \dots, n) = (1, n)(2, n) \cdots (n-1, n)$ , so transpositions generate  $S_n$

**Remark 1.7.** The transposition  $(\alpha, \alpha+1)$  is an odd permutation,  $(\alpha, \beta) = (\alpha, \alpha+1)(\alpha+1, \alpha+2) \cdots (\alpha+k-2, \alpha+k-1)(\alpha+k-1, \beta)(\alpha+k-1, \alpha+k-2) \cdots (\alpha+1, \alpha)$  if  $\beta = \alpha+k$ . Hence  $(\alpha, \beta)$  is also odd. The cycle  $(1, 2, \dots, n)$  is odd if  $n$  is even and even if  $n$  is odd.

**Theorem 1.12. (Cauchy)**

*If  $p$  divides  $|G|$  then there exists an element  $x \in G$  such that  $o(x) = p$ .*

*Proof.* Let  $\Omega := \{(g_1, \dots, g_p) \mid g_i \in G, \prod_{i=1}^p g_i = 1\} \subseteq G \times \dots \times G$  ( $p$ -times).

Let  $\pi$  be the cyclic shift on  $(g_1, \dots, g_p) : (g_1, \dots, g_p)^\pi = (g_2, g_3, \dots, g_p, g_1)$ .

If  $g_1 \cdots g_p = 1$  then  $g_2 \cdots g_p = g_1^{-1}$ , hence  $g_2 \cdots g_p g_1 = 1$ . So  $\pi$  acts on  $\Omega$ .

An element  $(g_1, \dots, g_p)$  of  $\Omega$  is fixed by  $\pi$  if and only if  $(g_1 = g_2 = \dots = g_p = g)$  and  $g^p = 1$ , e.g.  $(1, \dots, 1)$ . The number of elements in  $\Omega$ ,  $|\Omega| = |G|^{p-1}$ , since  $g_1, \dots, g_{p-1}$  can be arbitrary and  $g_p$  is already determined.

Since  $p$  divides  $|G|$  then  $p$  divides  $|\Omega|$ . As  $o(\pi) = p$ ,  $\pi$  is the product of cycles of length  $p$  and cycles of length 1, which belong to the fixed points of  $\pi$ , which we denote by  $\text{Fix}(\pi)$ . Hence,  $|\Omega| = |\text{Fix}(\pi)| + p \cdot |(\text{number of length } p \text{ cycles in } \pi)|$ . So  $p$  divides  $|\text{Fix}(\pi)|$ . Thus there exists a fixed point  $(g, \dots, g) \in \Omega$ , where  $g \neq 1$ . Since  $g^p = 1$ , we have that  $o(g) = p$ . □

**Definition 1.13.** Let  $G \leq S_\Omega$  or  $(\varphi : G \rightarrow S_\Omega)$  is a permutation representation) and  $\omega \in \Omega$  then:

$G_\omega := \{g \in G \mid \omega^g = \omega\}$  is called the **point stabilizer of  $\omega$**  in  $G$ . We remark that  $G_\omega$  is a subgroup of  $G$ .

$\omega^G = \{\alpha \in \Omega \mid \exists g \in G, \omega^g = \alpha\}$  is called the  **$G$ -orbit of  $\omega$** .



**Theorem 1.14.** *If  $G$  is a group action on  $\Omega$  then  $\Omega = \cup^* \Omega_i$  is a disjoint union of  $G$ -orbits. Moreover,  $|\omega^G| = |G : G_\omega|$ . (the length of the orbit of  $\omega$  = the index of the point stabilizer of  $\omega$ )*

*Proof.* Let  $\alpha, \beta \in \Omega$ , we say that  $\alpha, \beta$  are equivalent if there exists an element  $g \in G$  such that  $\alpha^g = \beta$ . This is an equivalence relation. The equivalence classes are the orbits of  $G$ . Hence  $\Omega = \cup^* \Omega_i$ .

Observe that  $\omega^g = \omega^h \Leftrightarrow \omega^{gh^{-1}} = \omega \Leftrightarrow gh^{-1} \in G_\omega \Leftrightarrow G_\omega g = G_\omega h$ .

$$|\omega^G| = |\{\text{different images of } \omega \text{ under } G\}| = |\{\text{different cosets of } G_\omega\}| = |G : G_\omega| \quad \square$$

**Corollary 1.1.**  $|G| = |G_\omega| \cdot |\omega^G|$ .

**Definition 1.15.**  $G_{\alpha_1, \dots, \alpha_n} := \{g \in G \mid \alpha_i^g = \alpha_i, i = 1, \dots, n\} = (G_{\alpha_1, \dots, \alpha_{n-1}})_{\alpha_n}$ .

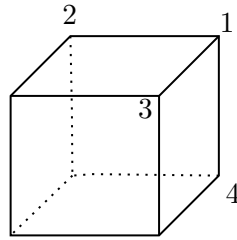
**Example 1.2.** How many elements does the group of symmetries of the cube have?

$$|1^G| = 8,$$

$$|G| = |1^G| \cdot |G_1| = 48$$

$$|G_1| = |2^{G_1}| \cdot |(G_1)_2| = 6$$

$$|G_{1,2}| = |3^{G_{1,2}}| \cdot |(G_{1,2})_3| = 2$$



**Theorem 1.16. (Cayley)**

- a) Every group of order  $n$  is isomorphic to a transitive permutation group of degree  $n$ .
- b) If there exists a subgroup  $H \leq G$  of index  $[G : H] = t$  then  $G$  has a transitive permutation representation of degree  $t$  with kernel  $= \cap_{x \in G} x^{-1} H x \leq H$ . (this is the maximal normal subgroup of  $G$  contained in  $H$  denoted by  $\text{Core}_G(H)$ ).

*Proof.* a) •  $G$  acts on  $G$  with right multiplication, there exists a map

$$\Phi : G \rightarrow S_{|G|}, \text{ such that } g \mapsto \pi_g = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1g & g_2g & \cdots & g_ng \end{pmatrix}$$

- $\Phi(gh) = \pi_{gh} = \pi_g\pi_h = \Phi(g)\Phi(h)$  since:

$$\begin{array}{ccc} g_i & & g_i \\ \downarrow g & & \downarrow gh \\ g_i g & & \\ \downarrow h & & \downarrow \\ g_i gh & & g_i(gh) \end{array}$$

So  $\Phi$  is a homomorphism.

- $\ker \Phi = \{g : \pi_g = id\} = \{1\}$ . So  $\Phi$  is a faithful permutation representation.
  - $G \cong \Phi(G) \leq S_{|G|}$
  - $\Phi$  is a transitive action, since  $g_i g = g_i$  if  $g = g_i^{-1}g_i$ .
- b) •  $G$  acts on the cosets of  $H$   $\{Hx : x \in G\}$  by right multiplication, so there exists a map

$$\Phi : G \rightarrow S_{[G:H]}, \text{ such that } g \mapsto \pi_g = \begin{pmatrix} Hg_1 & Hg_2 & \cdots & Hg_t \\ Hg_1g & Hg_2g & \cdots & Hg_tg \end{pmatrix}.$$

- Since  $\Phi(gh) = \pi_{gh} = \pi_g\pi_h = \Phi(g)\Phi(h)$ , so  $\Phi$  is a group homomorphism.
- $\ker \phi = \{g \in G \mid Hg_i g = Hg_i, \forall i = 1, \dots, t\} = \{g \in G \mid Hg_i g g_i^{-1} = H \forall i\}$   
 $= \{g \in G \mid g_i g g_i^{-1} \in H \forall i\} = \{g \in G \mid g \in g_i^{-1} H g_i \forall i\}$   
 $= \bigcap_{i=1}^t g_i^{-1} H g_i = \bigcap_{x \in G} x^{-1} H x = Core_G(H)$ , since every element  $x \in G$  can be written as  $x = h g_i$  for some  $h \in H$  and  $i$ .
- $\Phi$  is a transitive action since  $Hg_i g = Hg_i$  e.g. for  $g = g_i^{-1}g_i$ .

□

**Theorem 1.17.** *If  $\varphi : G \rightarrow S_\Omega$  is a transitive action on  $\Omega$  then the point stabilizers are conjugate.*

*Proof.* Let  $\alpha, \beta \in \Omega$ . Since  $G$  is transitive on  $\Omega$ , there exists an element  $g \in G$  such that  $\alpha^g = \beta$ . We prove that  $g^{-1}G_\alpha g = G_\beta$ , using short form of  $x^{-1}Hx =: H^x$ , this means that  $G_\alpha^g = G_\beta$ .

1. If  $\beta^{g^{-1}G_\alpha g} = \beta$ , then  $g^{-1}G_\alpha g \subseteq G_\beta$ , hence  $G_\alpha \subseteq gG_\beta g^{-1}$ ,
2. If  $\alpha^{gG_\beta g^{-1}} = \alpha$ , then  $gG_\beta g^{-1} \subseteq G_\alpha$ .

From (1) and (2) we have that  $G_\alpha = gG_\beta g^{-1}$ , hence  $G_\alpha^g = G_\beta$ . □

**Remark 1.8.** There are also other actions that are frequently used, e.g.: **conjugation action on elements of a group, conjugation action on subgroups.**

	1. Right multiplication on elements	2. right multiplication on right cosets of $H \leq G$	3. conjugation on elements	4. conjugation on subgroups
$\Omega$	$G$	$\{Hx \mid x \in G\}$	$G$	$\{H \mid H \leq G\}$
Action of $x$	$\pi_x = \begin{pmatrix} g_1 & \cdots & g_n \\ g_1x & \cdots & g_nx \end{pmatrix}$	$\pi_x = \begin{pmatrix} Hg_1 & \cdots & Hg_t \\ Hg_1x & \cdots & Hg_tx \end{pmatrix}$	$\pi_x = \begin{pmatrix} g_1 & \cdots & g_n \\ g_1^x & \cdots & g_n^x \end{pmatrix}$	$\pi_x = \begin{pmatrix} H_1 & \cdots & H_t \\ H_1^x & \cdots & H_t^x \end{pmatrix}$
Orbits $\omega^G$	$gG = G$ $\forall g \in G$	$Hg_iG = \{Hg_1, \dots, Hg_t\}$	$K_G(g)$	$\{H^g \mid g \in G\}$
Is transitive?	Yes	Yes	Not	Not
1 element orbits	No	No	elements of $Z(G)$	Normal subgroups
$G_\omega$ point stabilizer	1	$Hxg = Hx \Leftrightarrow$ $xgx^{-1} \in H \Leftrightarrow$ $g \in H^x$	$x^g = x \Leftrightarrow$ $g \in C_G(x)$	$H^g = H \Leftrightarrow$ $g \in N_G(H)$
Length of the orbit	$ G $	$[G : H]$	$ K_G(g) $	$ G : N_G(H) $
kernel of the action	1	$Core_G(H) = \bigcap_{x \in G} x^{-1}Hx$	$Z(G)$	$\bigcap_{H \leq G} N_G(H)$

Now we apply Theorem 1.14. We have the following:

**Corollary 1.2.** 1.  $|K_G(x)| = [G : C_G(x)]$  we used the 3rd action.

2.  $|Syl_p(G)| = [G : N_G(P)]$ , since the orbit of  $P \in Syl_p(G)$  is  $Syl_p(G)$  in the 4<sup>th</sup> action.

**Definition 1.18.** We say that two actions of  $G$ ,  $\varphi_1 : G \rightarrow S_{\Omega_1}$ , and  $\varphi_2 : G \rightarrow S_{\Omega_2}$  are **equivalent** if there exists a bijection  $b_1 : \Omega_1 \rightarrow \Omega_2$  such that for all  $g \in G$ , and for all  $\omega_1 \in \Omega_1$ ,  $b_1(\omega_1^{\varphi_1(g)}) = (b_1(\omega_1))^{\varphi_2(g)}$

$$\begin{array}{ccc}
 \omega_1 & \xrightarrow{b} & b(\omega_1) \\
 \downarrow g & & \downarrow g \\
 \omega_1^{\varphi_1(g)} & \xrightarrow{b} & (b(\omega_1))^{\varphi_2(g)}
 \end{array}$$

**Theorem 1.19.** All transitive actions of  $G$  are equivalent to a group action on the right cosets of a subgroup  $H$  with right multiplication.

*Proof.* Let  $\varphi : G \rightarrow S_{\Omega}$  be a transitive action on  $\Omega$ . Let  $H := G_{\omega}$ , let  $\Omega' := \{G_{\omega}g \mid g \in G\}$ . Observe that  $\omega^h = \omega^x \Leftrightarrow hx^{-1} \in G_{\omega} \Leftrightarrow G_{\omega}x = G_{\omega}h \Leftrightarrow h \in G_{\omega}x$ . So  $G_{\omega}x = \{h \in G \mid \omega^h = \omega^x\}$ . Let  $b : G_{\omega}x \mapsto \omega^x$ . Then this is a bijection between right cosets of  $G_{\omega}$  and the elements of  $\Omega$ , which is compatible with the action of elements of  $G$ , so this is an equivalence,

$$\begin{array}{ccc}
 G_{\omega}x & \xrightarrow{b} & \omega^x \\
 \downarrow g & & \downarrow g \\
 G_{\omega}xg & \xrightarrow{b} & \omega^{xg} = (\omega^x)^g
 \end{array}$$

□

**Definition 1.20.** Let  $G$  be a group.  $Aut(G) = \{\varphi : G \rightarrow G \mid \varphi \text{ bijective homomorphism (automorphism)}\}$ .  $Aut(G)$  is a group under composition of maps. This is the **automorphism group of  $G$** .

**Definition 1.21.** The group of inner automorphisms of the group  $G$  is defined as  $Inn(G) := G/Z(G)$ .

**Remark 1.9.** The elements of  $Inn(G)$  correspond to conjugations with elements of  $G$ , since  $g^{x_1} = g^{x_2}$  for all  $g \in G \Leftrightarrow g^{x_1 x_2^{-1}} = g$ , for all  $g \in G \Leftrightarrow x_1 x_2^{-1} \in Z(G) \Leftrightarrow Z(G)x_1 = Z(G)x_2$ .

**Example 1.3.** If  $n > 2$  then  $Z(S_n) = 1$ , so  $Inn(S_n) \cong S_n$ . (see problem sheet 1/2)

**Theorem 1.22.** If  $n > 2$ , and  $n \neq 6$  then  $Aut(S_n) \cong S_n$ .

*Proof.* • Let  $n = 3$ . We know that  $S_3 = \langle (1, 2, 3), (1, 2) \rangle$ . If  $\varphi \in Aut(G)$  then  $\varphi$  preserves elements orders. Thus  $(1, 2)$  can be mapped to  $(1, 2), (1, 3)$  or  $(2, 3)$ , and  $(1, 2, 3)$  can be mapped to  $(1, 2, 3)$  or  $(1, 3, 2)$ . Hence  $|Aut(S_3)| \leq 6$ . However,  $|Inn(S_3)| = 6$  and  $Inn(S_3) \leq Aut(S_3)$  so  $Aut(S_3) \cong S_3$ .

- Let  $n = 4$ . We know that  $S_4 = \langle \underbrace{(1, 2, 3, 4)}_a, \underbrace{(1, 2, 4, 3)}_b \rangle$ . (one can check with GAP)

Since  $|S_4| = 24$  and the number of elements of order 4 in  $S_4$  is  $\frac{4 \cdot 3 \cdot 2 \cdot 1}{4} = 6$ , so  $\varphi(a)$  can be chosen in at most 6 ways,  $\varphi(b) \neq \varphi(a)$  and  $\varphi(b) \neq \varphi(a)^{-1}$  thus  $\varphi(b)$  can be chosen in at most 4 ways.

Hence  $|Aut(S_4)| \leq 24$ . As  $Inn(S_4) \leq Aut(S_4)$  we have that  $Aut(S_4) \cong S_4$ .

- Let  $n \geq 5$ . Observe that an automorphism preserves conjugacy classes: suppose that  $a$  is conjugate to  $b$  in  $S_n$ . We denote this by  $a \sim b$ . If  $x^{-1}ax = b$  then  $\varphi(x)^{-1}\varphi(a)\varphi(x) = \varphi(b)$ , hence  $\varphi(a) \sim \varphi(b)$ .

Let  $K_{S_n}((1, 2))$  be the conjugacy class of transpositions in  $S_n$ . If  $\varphi \in Aut(S_n)$  then it takes  $(1, 2)$  into an element of order 2, which is a product of disjoint transpositions.

Then  $K_{S_n}((1, 2)) \xrightarrow{\varphi} K_{S_n}((1, 2)(3, 4) \cdots (2k-1, 2k))$ , for some  $k$ .

Let us check if it is possible or not.

We know that  $|K_{S_n}((1, 2))| = \binom{n}{2} = \frac{n(n-1)}{2}$  and

$|K_{S_n}((1, 2)(3, 4) \cdots (2k-1, 2k))| = \frac{\binom{n}{2} \binom{n-2}{2} \cdots \binom{n-2k+2}{2}}{k!}$ . We investigate when there numbers are equal, namely

$\frac{n(n-1)}{2} = \frac{n(n-1)(n-2)\cdots(n-2k+2)(n-2k+1)}{2^k k!}$ . This is equivalent to  $2^{k-1}k! = (n-2)(n-3)\cdots(n-2k+1)$ .

If  $k = 2$  then this gives us  $2 \cdot 2 = (n-2)(n-3)$ , which has no solution.

If  $k = 3$ , then we have that  $4 \cdot 6 = (n-2)(n-3)(n-4)(n-5)$ . Here  $n$  is a solution if and only if  $n = 6$ .

Let  $k \geq 4$ . We show that there is no solution, since the left hand side is smaller than the right hand side. The right hand side is the smallest if  $n = 2k$ ,

(the left side is independent of  $n$ ). So it is enough to prove the inequality for  $n = 2k$ .

Observe that  $2^{k-1}k! < (2k-2)(2k-3)\cdots 1 \Leftrightarrow 2 \cdot 4 \cdots (2k-2)k < (2k-2)(2k-3)\cdots 1$   
 $\Leftrightarrow k < (2k-3)(2k-5)\cdots 3 \cdot 1$ . This is true since  $k < 2k-3 \Leftrightarrow k > 3$ .

Hence if  $\varphi \in \text{Aut}(S_n)$  and  $n > 6$ , then  $\varphi(K_{S_n}(1, 2)) = (K_{S_n}(1, 2))$ .

We define a graph  $\Gamma = (V, E)$ . The vertices  $V$  of  $\Gamma$  are the transpositions of  $S_n$ .

Two transpositions  $(a, b)$  and  $(c, d)$  are connected with an edge if and only if

$|\{a, b\} \cap \{c, d\}| = 1$ . This is equivalent to  $o((a, b)(c, d)) = 3$ .

(Note that  $(a, x)(x, b) = (abx)$  and  $(a, x)(a, x) = id$  if  $|\{a, b\} \cap \{c, d\}| = 2$ , moreover  $o((a, b)(c, d)) = 2$  if  $\{a, b\} \cap \{c, d\} = \emptyset$ ).

Let  $\sigma \in \text{Aut}(S_n)$  then, as we have seen,  $\sigma(K_{S_n}((1, 2))) = K_{S_n}((1, 2))$ , so

$\sigma$  permutes the vertices of  $\Gamma$  and  $\sigma$  preserves the orders of elements. We show that  $\sigma$  also preserves edges. The transposition  $(a, b)$  and  $(c, d)$  are connected with an edge if

and only if  $o((a, b)(c, d)) = 3$ . Then  $o(\sigma((a, b))\sigma((c, d))) = o(\sigma((a, b)(c, d))) = o((a, b)(c, d)) = 3$ ,

hence  $\sigma(a, b)$  and  $\sigma(c, d)$  are also connected with an edge, so  $\sigma$  preserves edges and we have that  $\sigma \in \text{Aut}(\Gamma)$ . We define the following subgraph.

$G_a := \{(a, x) | x \in \{1, 2, \dots, n\} \setminus \{a\}\}$  then  $|G_a| = n - 1$  and

$G_a$  is a complete graph on  $n - 1$  points for every  $a \in \{1, \dots, n\}$ .

$\Gamma$  has no other complete subgraphs on  $n - 1$  points, see problem sheet 2/2.

Since  $\sigma$  is a graph automorphism, hence complete  $n - 1$  point subgraphs are mapped to complete  $n - 1$  point subgraphs and so  $\sigma(G_a) = G_{a'}$ . Since  $S_n$  is transitive on

$\{1, 2, \dots, n\}$ , there exists an element  $g \in S_n$  such that  $a^g = a'$ , for  $a \in \{1, 2, \dots, n\}$ .

Then  $g = \begin{pmatrix} a_1 & \cdots & a_m \\ a'_1 & \cdots & a'_m \end{pmatrix}$ , in a particular  $a^g = a', b^g = b'$ .

If  $a \neq b$ , then  $\{(a, b)\} = G_a \cap G_b$ , and  $\{(a, b)^\sigma\} = G_{a'} \cap G_{b'} = \{(a', b')\} = \{(a^g, b^g)\} = \{(a, b)^g\}$ . Hence  $(a, b)^\sigma = (a, b)^g$  on transpositions. Since the transpositions generate  $S_n$ , on the whole  $S_n$   $\sigma$  is the conjugation by  $g$ .

Hence every  $\sigma \in \text{Aut}(S_n)$  is a conjugation by some  $g \in G$ . Thus  $\text{Aut}(S_n) \cong \text{Inn}(S_n) \cong S_n$ .

□

## 2 Application of the Sylow theorems, small groups

We know by Lagrange's theorem that if  $G$  is a finite group and  $H$  is a subgroup in  $G$ , then  $|H|$  divides  $|G|$ .

However, the converse is not true. For example  $|A_5| = 60$  and 15 divides 60, but there is no subgroup of  $A_5$  of order 15. (see problem sheet 3/1)

However, for each maximal  $p$ -power divisor of  $|G|$ , there exists a subgroup of that order.

**Definition 2.1.** Let  $G$  be a finite group and let  $p$  be a prime. Suppose that  $|G| = p^a m$ , where  $(p, m) = 1$ . If  $P$  is a subgroup of  $G$  and  $|P| = p^a$ , then  $P$  is called a **Sylow  $p$ -subgroup** of  $G$ .

**Theorem 2.2. (Sylow)**

Let  $G$  be a finite group, let  $p$  be a prime and let  $|G| = p^a m$ , where  $(p, m) = 1$ . Then

1. (Ep) There exists a subgroup  $P \leq G$ , such that  $|P| = p^a$ . (existence of Sylow  $p$ -subgroups)
2. Let  $\text{Syl}_p(G) := \{P \leq G \mid |P| = p^a\}$ . Then  $|\text{Syl}_p(G)| = [G : N_G(P)] \equiv 1 \pmod{p}$ .
3. (Cp) For all  $P_1, P_2 \in \text{Syl}_p(G)$  there exists an element  $g \in G$  such that  $P_1^g = P_2$ . (Sylow  $p$ -subgroups are conjugate)
4. (Dp) If  $H \leq G$  is a  $p$ -subgroup, then there exists a subgroup  $P \in \text{Syl}_p(G)$  such that  $H \leq P$ , ( $P$  is a maximal  $p$ -subgroup under containment as well).



**Corollary 2.1.** Let  $|G| = pq$  where  $p < q$  primes.

If  $Q \in \text{Syl}_q(G)$ , then  $Q \triangleleft G$ .

If  $q \not\equiv 1(p)$ , then  $P \triangleleft G$  and  $G \cong C_{pq}$ .

If  $q \equiv 1(p)$ , then there exist elements  $a, b \in G$  such that

$G = \langle a, b \mid a^q = 1, b^p = 1, b^{-1}ab = a^m, m \equiv 1(q), m \not\equiv 1(q) \rangle$ . In particular, if  $|G| = 2q$  and  $G$  is non-abelian then  $G \cong D_{2q}$ .

*Proof.* Let  $|G| = pq$ , then if  $P \in \text{Syl}_p(G)$  then  $|P| = p$  and If  $Q \in \text{Syl}_q(G)$  then  $|Q| = q$ , so  $P$  and  $Q$  are cyclic,  $P \cong C_p, Q \cong C_q$ . (problem sheet 2/8/c )

The number of Sylow  $q$ -subgroups in  $G$  is  $\underbrace{[G : N_G(Q)]}_{\equiv 1(q)} \mid [G : Q] = p$ . Hence

$[G : N_G(Q)] = kq + 1 \mid p$ , and  $q > p$  so  $k = 0$  hence  $Q \triangleleft G$ .

The number of Sylow  $p$ -subgroups is  $[G : N_G(P)] \mid [G : P] = q$  and  $[G : N_G(P)] \equiv 1(p)$ .

If  $q \not\equiv 1(p)$  then  $[G : N_G(P)] = 1$  hence  $P \triangleleft G$ . Since  $P \cap Q = 1$  and

$PQ = G$  then  $G \cong P \times Q \cong C_p \times C_q \cong C_{pq}$ . (see problem sheet 2/8/e )

If  $q \equiv 1(p)$  then there can be a non-abelian group of order  $pq$ . Let

$Q = \langle a \rangle$  where  $o(a) = q$ , let  $P = \langle b \rangle$ , where  $o(b) = p$ . Then  $\langle a \rangle = Q \triangleleft G$  and hence

$b^{-1}ab \in \langle a \rangle$ , so  $b^{-1}ab = a^m$  for some  $m$ , and  $\underbrace{b^{-1} \cdots b^{-1}}_{k\text{-times}} a \underbrace{b \cdots b}_{k\text{-times}} = a^{m^k}$ .

Let  $k = p$ . Then  $b^p = 1$  and we have that  $a = a^{m^p}$  hence  $a^{m^p-1} = 1$ . Thus  $o(a) \mid m^p - 1$  and so  $m^p \equiv 1(q)$ . Observe that  $m \not\equiv 1(q)$ , otherwise  $b^{-1}ab = a$  and  $G$  is commutative.

Hence if  $G$  is nonabelian,  $G$  satisfies relations of the group

$X = \langle a, b \mid a^q = 1, b^p = 1, b^{-1}ab = a^m, m^p \equiv 1(q), m \not\equiv 1(q) \rangle$ .

By Dyck's theorem, see Algebra 1, or Theorem 8.6,  $G$  is a factor group of  $X$ . Since  $|X| \leq pq$  we have that  $X \cong G$ .

In particular, if  $|G| = 2q$ ,  $q$  is prime and  $G$  is non-abelian then

$G = \langle a, b \mid a^q = 1, b^2 = 1, b^{-1}ab = a^{-1} \rangle$ , Hence  $G \cong D_{2q}$ . □

**Corollary 2.2. Small groups**

1	1
2	$C_2$
3	$C_3$
4	$C_4, C_2 \times C_2$
5	$C_5$
6	$C_6, D_6$
7	$C_7$
8	(abelian $C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$ )(non-abelian $Q_8, D_8$ )
9	$C_9, C_3 \times C_3$
10	(abelian $C_{10} = C_2 \times C_5$ )(non-abelian $D_{10}$ )
11	$C_{11}$
12	(abelian $C_{12}, (C_2 \times C_2) \times C_3$ )(non-abelian $D_{12}, A_4, C_3 \rtimes C_4$ )
13	$C_{13}$
14	(abelian $C_{14}$ )(non-abelian $D_{14}$ )
15	$C_{15}$

For the non-abelian groups of order 8, see problem sheet 2/9.

For the non-abelian groups of order 12, see problem sheet 3/4.

### 3 $k$ -transitive and primitive groups

**Definition 3.1.** Let  $G$  act on  $\Omega$ . We say that this action is  $k$ -**transitive** on  $\Omega$  if for all  $\alpha_1, \alpha_2, \dots, \alpha_k \in \Omega$  distinct and for all  $\beta_1, \beta_2, \dots, \beta_k \in \Omega$  distinct, there exists an element  $g \in G$  such that  $\alpha_i^g = \beta_i$ , for  $i = 1, 2, \dots, k$ .

**Remark 3.1.**  $G$  is 1-transitive if and only if  $G$  is transitive on  $\Omega$ .

**Remark 3.2.** If  $G$  is  $k$ -transitive on  $\Omega$  and  $k > 1$  then  $G$  is  $(k - 1)$ -transitive on  $\Omega$ .

**Theorem 3.2.** Let  $k \geq 2$ . The following are equivalent for an action of  $G$  on  $\Omega$

1.  $G$  is  $k$ -transitive on  $\Omega$ .
2.  $G$  is transitive on  $\Omega$  and there exists an  $\alpha \in \Omega$  such that  $G_\alpha$  is  $(k - 1)$ -transitive on  $\Omega \setminus \{\alpha\}$ .
3.  $G$  is transitive on  $\Omega$  and for all  $\alpha \in \Omega$ ,  $G_\alpha$  is  $(k - 1)$ -transitive on  $\Omega \setminus \{\alpha\}$ .

*Proof.* (1)  $\Rightarrow$  (2)

Let  $\alpha \in \Omega$ . We have to prove that  $G_\alpha$  is  $k - 1$  transitive on  $\Omega \setminus \{\alpha\}$ .

Let  $\beta_1, \dots, \beta_{k-1} \in \Omega \setminus \{\alpha\}$  distinct, and let  $\gamma_1, \dots, \gamma_{k-1} \in \Omega \setminus \{\alpha\}$  distinct.

We have to find an element  $g_\alpha \in G_\alpha$  such that  $\beta_i^{g_\alpha} = \gamma_i$ , for  $i = 1, \dots, k - 1$ .

Now  $\alpha, \beta_1, \dots, \beta_{k-1} \in \Omega$  are distinct and  $\alpha, \gamma_1, \dots, \gamma_{k-1} \in \Omega$  are distinct. From (1) we have that there exists an element  $g \in G$  such that  $\alpha^g = \alpha$  and  $\beta_i^g = \gamma_i$ , for  $i = 1, \dots, k - 1$ , hence  $g \in G_\alpha$  and  $G_\alpha$  is  $(k - 1)$ -transitive on  $\Omega \setminus \{\alpha\}$ .

(2)  $\Rightarrow$  (3)

Let  $\beta \in \Omega$ . We have to prove that  $G_\beta$  is  $(k - 1)$ -transitive on  $\Omega \setminus \{\beta\}$ , in other words for  $\beta_1, \dots, \beta_{k-1} \in \Omega \setminus \{\beta\}$  distinct, and for  $\beta'_1, \dots, \beta'_{k-1} \in \Omega \setminus \{\beta\}$  distinct, there exists an element  $g \in G_\beta$  such that  $\beta_i^g = \beta'_i$ ,  $i = 1, \dots, k - 1$ .

From (2) we have that  $G$  is transitive on  $\Omega$ . So there exists an element  $g \in G$  such that  $\alpha^g = \beta$ . Let  $\alpha_i := \beta_i^{g^{-1}}$  and  $\alpha'_i := (\beta'_i)^{g^{-1}}$ . Then  $\alpha_1, \dots, \alpha_{k-1} \in \Omega \setminus \{\alpha\}$  are distinct, and  $\alpha'_1, \dots, \alpha'_{k-1} \in \Omega \setminus \{\alpha\}$  are distinct.

By (2), there exists an element  $g_\alpha \in G_\alpha$  such that  $\alpha_i^{g_\alpha} = \alpha'_i$ , for  $i = 1, \dots, k - 1$ .

Then  $\beta_i^{g_\alpha^{-1}g_\alpha g} = \beta'_i$ , for  $i = 1, \dots, k - 1$ , so  $G_\beta$  is  $(k - 1)$ -transitive on  $\Omega \setminus \{\beta\}$ .

(3)  $\Rightarrow$  (1)

We have to prove that for every  $\alpha_1, \dots, \alpha_k \in \Omega$  distinct, and for every  $\beta_1, \dots, \beta_k \in \Omega$  distinct, there exists an element  $g \in G$  such that  $\alpha_i^g = \beta_i$ , for  $i = 1, \dots, k$ . Since  $G$  is transitive on  $\Omega$ , we have that there exists an element  $g \in G$  such that  $\alpha_1^g = \beta_1$ .

From (3) we have that  $G_{\beta_1}$  is  $(k - 1)$ -transitive on  $\Omega \setminus \{\beta_1\}$ . Now  $\alpha_2^g, \alpha_3^g, \dots, \alpha_k^g \in \Omega \setminus \{\beta_1\}$ . Since  $\alpha_2^g, \dots, \alpha_k^g$  are distinct and  $\beta_2, \dots, \beta_k \in \Omega \setminus \{\beta_1\}$ , we have that there exists an element  $h \in G_{\beta_1}$  such that  $(\alpha_i^g)^h = \beta_i$ , for  $i = 2, \dots, k$ . Since  $\alpha_1^g = \beta_1$ ,  $((\alpha_1^g)^h) = \beta_1$  and so  $\alpha_i^{gh} = \beta_i$ , for  $i = 1, 2, \dots, k$ .  $\square$

**Definition 3.3.** Let  $G \leq S_\Omega$  (or  $G$  acts on  $\Omega$ ). We say that  $\Omega = \cup_{i=1}^k \Omega_i$  is a  **$G$ -invariant partition** of  $\Omega$  if  $\Omega_i \cap \Omega_j = \emptyset$  for all  $i \neq j$ , and for all  $g \in G$ , for all  $i = 1, \dots, k$ , there exists  $j$  such that  $\Omega_i^g = \Omega_j$ . This partition is **proper** if there exists an index  $i$  such that  $|\Omega_i| \neq 1$  and  $\Omega_i \neq \Omega$ .

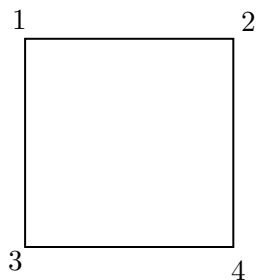
**Definition 3.4.** We say that  $G \leq S_\Omega$  (or action of  $G$  on  $\Omega$ ) is **primitive**, if it is transitive and there is no proper  $G$ -invariant partition on  $\Omega$ .

We say that  $G$  is **imprimitive** on  $\Omega$  if  $G$  is transitive on  $\Omega$  but not primitive.

**Remark 3.3.** If  $G$  is transitive and not primitive, then since there exists an element  $g \in G$  such that  $\Omega_i^g = \Omega_j$ , we have that  $|\Omega_i| = |\Omega_j|$ .

**Definition 3.5.** If  $G$  acts on  $\Omega$ , then a subset  $B \subseteq \Omega$  is called a **block** (or **domain of imprimitivity**) for  $G$  if for all elements  $g \in G$  ( $B^g \cap B \neq \emptyset \Rightarrow B = B^g$ ).  $B$  is a **proper block** if  $B \neq \Omega$ ,  $|B| \neq 1$ .

**Example 3.1.**  $D_8$  acts on  $\{1, 2, 3, 4\}$  transitively,  $\{1, 4\}, \{2, 3\}$  are blocks,



**Theorem 3.6.** If  $G$  is transitive on  $\Omega$ , then  $G$  is primitive if and only if  $\Omega$  has no proper blocks for  $G$ .

*Proof.* It is enough to prove that the action is imprimitive if and only if there exists a proper block.

$\implies$ ) Suppose that  $\Omega = \cup^* \Omega_i$ , is a proper  $G$ -invariant partition on  $\Omega$ .

Then  $\Omega_i$  is a proper block for every  $i$ .

$\impliedby$ )

If  $B \subsetneq \Omega$  is a proper block for  $G$  then we will prove that  $\Omega = \cup B^g$  is a proper  $G$ -invariant partition of  $\Omega$ . By transitivity of  $G$ , we have that  $\Omega = \cup_{g \in G} B^g$ .

We want to prove that if  $B^g \cap B^h \neq \emptyset$  then  $B^g = B^h$ . Since  $(B^g)^{h^{-1}} \cap B \neq \emptyset$  we have that  $B^{gh^{-1}} = B$ , hence  $B^g = B^h$ . So  $\Omega = \cup_{g \in G} B^g$  is a  $G$ -invariant partition. Since  $|B| \neq 1, B \neq \Omega$ , it is a proper partition of  $\Omega$  and so  $G$  is imprimitive.  $\square$

**Example 3.2.**  $G := \{1, (123)(abc), (132)(acb), (1b)(2a)(3c), (1a)(2c)(3b), (1c)(2b)(3a)\}$   
 $\Omega = \{1, 2, 3\} \cup \{a, b, c\} = \{1, a\} \cup \{2, b\} \cup \{3, c\}$  are two  $G$ -invariant partitions on  $\Omega$ .

**Theorem 3.7.** *If the group  $G$  acts on  $\Omega$  transitively, then the following are equivalent:*

1.  $G$  acts on  $\Omega$  primitively.
2. There exists  $\alpha \in \Omega$  such that  $G_\alpha$  is maximal in  $G$ .
3. For all  $\alpha \in \Omega$ ,  $G_\alpha$  is maximal in  $G$ .

*Proof.* (3)  $\Rightarrow$  (2) This is obvious.

(2)  $\Rightarrow$  (3) Since  $G$  is transitive on  $\Omega$ , by Theorem 1.17 we have that  $G_\alpha$  is conjugate to  $G_\beta$ . Thus they are maximal at the same time, so  $G_\beta$  is also maximal.

(1)  $\Leftrightarrow$  (2) It is enough to prove that  $G$  is imprimitive on  $\Omega$  iff there is an  $\alpha \in \Omega$  such that  $G_\alpha$  is not maximal.

$\Rightarrow$ )

If the action of  $G$  is imprimitive then there exists a block  $B \subsetneq \Omega$  such that  $|B| \neq 1$ .

Let  $M := \{g \in G \mid B^g = B\}$ . Then  $M = \{g \in G \mid B^g \cap B \neq \emptyset\}$  and  $M$  is a subgroup of  $G$ . Observe that if  $\alpha \in B$ , then  $G_\alpha \leq M$ . We will prove  $G_\alpha \subsetneq M$ . Since  $|B| > 1$ , and  $\alpha \in B$  then there exists  $\beta \in B$  such that  $\alpha \neq \beta$ . As  $G$  is transitive on  $\Omega$ , there exists an element  $g \in G$  such that  $\alpha^g = \beta$ . Thus,

$\alpha^g \in B^g \cap B \neq \emptyset$ , and hence  $B^g = B$  and  $g \in M$ . However  $g \in M \setminus G_\alpha$  and so

$G_\alpha \subsetneq M$ . Since  $B \neq \Omega$ , there exists an element  $g \in G$  such that  $B^g \neq B$ , thus  $g \in G \setminus M$  and so  $M \neq G$  and we have that  $G_\alpha \subsetneq M \subsetneq G$ , so  $G_\alpha$  is not maximal.

$\Leftarrow$ )

If  $G_\alpha$  is not maximal, then we want to prove that the action is imprimitive. Let us choose a maximal subgroup  $M$  such that  $G_\alpha \subsetneq M \subsetneq G$ . We want to find a proper block of  $G$  on  $\Omega$ . Let  $B := \{\alpha^m \mid m \in M\}$ , then  $|B| > 1$  because  $G_\alpha \leq M$ , and there exists an element  $m \in M \setminus G_\alpha$ , so for that  $\alpha^m \neq \alpha$ . Moreover  $B \neq \Omega$ , since if  $B = \Omega$  then  $M$  were transitive on  $\Omega$  then for every  $g \in G$  there would exist an element  $m \in M$  such that  $\alpha^g = \alpha^m$ . Hence  $\alpha^{gm^{-1}} = \alpha$ . and so  $gm^{-1} \in G_\alpha \subsetneq M$ . Let  $m_1 := gm^{-1}$ . Then  $g = m_1m \in M$ , hence every

$g \in G$  is in  $M$ , so this is a contradiction, and thus  $B \neq \Omega$ .

Now, want to prove that  $B$  is a block. If  $B^g \cap B \neq \emptyset$ , then there exist elements  $m, m' \in M$  such that  $\alpha^{mg} = \alpha^{m'}$ . Hence  $\alpha^{mg(m')^{-1}} = \alpha$  and we have that  $mg(m')^{-1} \in G_\alpha \not\subseteq M$ . Hence there is an element  $m'' \in M$  such that  $mg(m')^{-1} = m''$  and we have that  $g = m^{-1}m''m' \in M$ . By the definition of  $B$ , we have that  $B^g = B$  and so  $B$  is a block. Hence  $G$  acts imprimitively.  $\square$

**Definition 3.8.** A group  $G$  is **sharply  $k$ -transitive** on  $\Omega$  if for all distinct  $\alpha_1, \dots, \alpha_k \in \Omega$  and for all distinct  $\beta_1, \dots, \beta_k \in \Omega$ , there is a unique element  $g \in G$  such that  $\alpha_i^g = \beta_i$ , for  $i = 1, 2, \dots, k$ .

**Theorem 3.9. (Jordan)**

Let  $G \leq S_n$  be a sharply  $k$ -transitive group. If  $G \neq S_n$  or  $A_n$ , then  $k = 4$  and  $n = 11$  or  $k = 5$  and  $n = 12$ . (The Mathieu-groups  $M_{11}$  and  $M_{12}$  are such groups.)

## 4 Group extensions, semidirect product, wreath product

**Definition 4.1.**

$$1 \xrightarrow{i} A \xrightarrow{\psi} B \xrightarrow{\varphi} C \xrightarrow{\pi} 1 \quad (*)$$

Let  $A, B, C$  be groups,  $\psi, \varphi$  group homomorphisms,  $i$  is the embedding of 1 and  $\pi$  is the surjection on 1. We say that the sequence (\*) is **exact** if  $\text{Im } i = \ker \psi$  (if and only if  $\psi$  is injective) and  $\text{Im } \varphi = \ker \pi$  (if and only if  $\varphi$  is surjective) and  $A \cong \text{Im } \psi = \ker \varphi$  (in this case  $B/\ker \varphi \cong \text{Im } \varphi = C$ ) hence  $B/\psi(A) \cong B/A$ . In this case we tell that  $B$  is an **extension** of  $A$  by  $C$ .

( $A \triangleleft B$  and  $B/A \cong C$ ) (shortly)

**Definition 4.2.** The extension  $A$  by  $C$  is **split** (or **inner semidirect product**), if there exists a subgroup  $C_1 \leq B$  such that  $C_1 \cong C$ ,  $A \cap C_1 = \{1\}$  and  $AC_1 = B$ .

(in this case  $B/A = (AC_1)/A \cong C_1/(C_1 \cap A) \cong C_1 \cong C$ )

**Lemma 4.1.** Let  $G = KQ$ ,  $K \triangleleft G$ ,  $K \cap Q = 1$  (split extension of  $K$  by  $Q$ ), then there exists a map  $\Theta : Q \rightarrow \text{Aut}(K)$  such that  $x \mapsto \Theta_x = \begin{pmatrix} K \\ xKx^{-1} \end{pmatrix}$  is a homomorphism ( $Q$  acts on  $K$  with conjugation by  $x^{-1}$  for  $x \in Q$ ).

*Proof.*  $\Theta : Q \rightarrow \text{Aut}(K)$  is a homomorphism since  $\Theta_{xy}(K) = xyky^{-1}x^{-1} = \Theta_x(\Theta_y(K))$ , hence  $\Theta_{xy} = \Theta_x\Theta_y$ .  $\square$

**Definition 4.3. (Outer semidirect product)**

Let  $Q$  and  $K$  be groups and  $\Theta : Q \rightarrow \text{Aut}(K)$  be a group homomorphism.

$G := K \rtimes_{\Theta} Q = \{(a, x) \mid a \in K, x \in Q\}$  with multiplication rule  $(a, x)(b, y) = (a\Theta_x(b), xy)$  with this multiplication  $G$  is a group. (see problem sheet 5/2)

The unit element is  $(1, 1)$ ,  $(k, q)^{-1} = (\Theta_{q^{-1}}(k))^{-1}, q^{-1}$  and  $(1, q)(k, 1)(1, q)^{-1} = (\Theta_q(k), 1)$ . The elements  $K^* = \{(k, 1) \mid k \in K\}$  form a normal subgroup isomorphic to  $K$ , the elements  $Q^* = \{(1, q) \mid q \in Q\}$  form a subgroup isomorphic to  $Q$ ,  $G = K^*Q^*$  and  $K^* \cap Q^* = \{(1, 1)\}$ .

**Definition 4.4. (Wreath product)**

Let  $D \leq S_{\Lambda}$ ,  $Q \leq S_{\Omega}$  be permutation groups, let  $D_{\omega} \cong D$  for all  $\omega \in \Omega$ , then  $K = \prod_{\omega \in \Omega} D_{\omega}$ ,

is the base group of the wreath product. Let:  $D \sim Q := \left( \prod_{\omega \in \Omega} D_{\omega} \right) \rtimes Q$ , where  $Q$  acts on

$\prod_{\omega \in \Omega} D_{\omega}$  by permuting components:  $(d_{\omega_1}, d_{\omega_2}, \dots)^q = (d_{\omega_1 q}, d_{\omega_2 q}, \dots)$ .

**Remark 4.1.** If  $|D| < \infty$ , then  $|K| = |D|^{|\Omega|}$ . If  $Q$  is also finite, then  $|D \sim Q| = |D|^{|\Omega|}|Q|$ .

**Theorem 4.5.** Let us suppose that  $D \leq S_{\Lambda}$  ( $D$  acts on  $\Lambda$ ) and  $Q \leq S_{\Omega}$  ( $Q$  acts on  $\Omega$ ).

Then  $D \sim Q$  acts on  $\Lambda \times \Omega$ , and  $D \sim Q \leq S_{(\Lambda \times \Omega)}$ , where the action is defined by

$$(\lambda, \omega)^{(d_{\omega_1}, \dots, d_{\omega_n}, q)} = (\lambda^{d_{\omega}}, \omega^q). \quad (*)$$

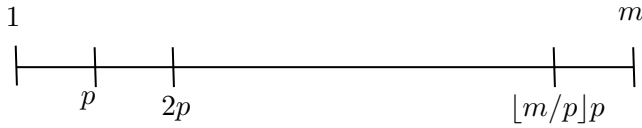
This define an action  $\varphi : D \sim Q \rightarrow S_{(\Lambda \times \Omega)}$ , in other words

$\varphi((d_{\omega_1}, \dots, d_{\omega_n}, q)(d'_{\omega_1}, \dots, d'_{\omega_n}, q')) = \varphi(d_{\omega_1}, \dots, d_{\omega_n}, q)\varphi(d'_{\omega_1}, \dots, d'_{\omega_n}, q')$ , as  $(\lambda^{d_{\omega}}, \omega^q)^{(d'_{\omega_1}, \dots, d'_{\omega_n}, q')} = (\lambda^{d_{\omega}d'_{\omega q}}, (\omega^q)^{q'})$  is the image of  $(\lambda, \omega)$  when we apply the left hand side. On the other hand,  $(d_{\omega_1}, \dots, d_{\omega_n}, q)(d'_{\omega_1}, \dots, d'_{\omega_n}, q') = ((d_{\omega_1}, \dots, d_{\omega_n})(d'_{\omega_1 q}, \dots, d'_{\omega_n q}), qq')$   $= (d_{\omega_1}d'_{\omega_1 q}, \dots, d_{\omega_n}d'_{\omega_n q}, qq')$ . Thus  $(\lambda, \omega)^{(d_{\omega_1}d'_{\omega_1 q}, \dots, d_{\omega_n}d'_{\omega_n q}, qq')} = (\lambda^{(d_{\omega}d'_{\omega q})}, \omega^{qq'})$  is the image

of  $(\lambda, \omega)$ , when we apply the right hand side, This action is faithful, since if  $(\lambda^{d_\omega}, \omega^q) = (\lambda, \omega)$  for all  $\lambda$  and for all  $\omega$ , then  $\lambda^{d_\omega} = 1$  for all  $\omega$ , and  $q = 1$  and so  $(d_{\omega_1}, \dots, d_{\omega_n}, q) = (1, \dots, 1)$ . Hence  $G \sim Q \leq S_{\Lambda \times \Omega}$ .

#### 4.1 The Sylow $p$ -subgroups of symmetric groups

What is the order of the Sylow  $p$ -subgroup of  $S_m$ . The order of  $S_m$  is  $m!$ . We need  $p^M \mid m!$  but  $p^{M+1} \nmid m!$



$M = \lfloor \frac{m}{p} \rfloor + \lfloor \frac{m}{p^2} \rfloor + \lfloor \frac{m}{p^3} \rfloor + \dots$ , since

$\lfloor \frac{m}{p} \rfloor$  numbers between 1 and  $m$  are divisible by  $p$

$\lfloor \frac{m}{p^2} \rfloor$  numbers between 1 and  $m$  are divisible by  $p^2$

$\vdots$

etc.

**Remark 4.2.**  $C_p \sim C_p = \underbrace{C_p \times \dots \times C_p}_{p\text{-times}} \rtimes C_p$  and  $C_p \leq S_{|C_p|}$ , since  $C_p$  acts on  $C_p$  by right multiplication.

By the previous theorem, we have that  $C_p \sim C_p \leq S_{p^2}$ . Hence  $(C_p \sim C_p) \sim \dots \sim C_p \leq S_{p^n}$ .

**Theorem 4.6.** (Kaloujnine 1984)

Let  $p$  be a prime. The Sylow  $p$ -subgroup of  $S_{p^n}$  is the iterated wreath product

$$W_n = \underbrace{(C_p \sim C_p) \sim \dots \sim C_p}_{n\text{-times}}$$

*Proof.* The proof is by induction on  $n$ .

If  $n = 1$ , then  $|S_p| = p!$ , and if  $P \in \text{Syl}_p(S_p)$ , then  $|P| = p$  hence  $P \cong C_p$ .

By induction we suppose that the  $n$ -fold iterated wreath product  $P = (C_p \sim \dots \sim C_p) \in \text{Syl}_p(S_{p^n})$ .

Since  $P \leq S_{p^n}, C_p \leq S_p$ , then  $P \sim C_p$  acts on the direct product set of order  $p^{n+1}$ , hence

$P \sim C_p \leq S_{p^{n+1}}$ .



If  $P_1 \in Syl_{p^{n+1}}$ , then  $|P_1| = p^{\mu^{(n+1)}}$ , where  $\mu^{(n+1)} = \lfloor \frac{p^{n+1}}{p} \rfloor + \lfloor \frac{p^{n+1}}{p^2} \rfloor + \cdots + \lfloor \frac{p^{n+1}}{p^{n+1}} \rfloor = p^n + p^{n-1} + \cdots + 1$ .

We know by induction that  $|P| = p^{1+\cdots+p^{n-1}}$ . Hence  $|P \sim C_p| = |P|^p \cdot p = p^{p+\cdots+p^n} \cdot p = p^{1+\cdots+p^n}$ .

This is exactly the size of the Sylow  $p$ -subgroups of  $S_{p^{n+1}}$ . Hence we are done.

□

**Remark 4.3.** We can also determine the Sylow  $p$ -subgroup of  $S_m$ , where  $m$  is not necessarily a  $p$ -power. Let us write  $m$  in  $p$ -adic number system:  $m = a_0 + a_1p + \cdots + a_t p^t$ , where  $0 \leq a_i < p - 1$ . Let  $\Omega := \{1, 2, \dots, m\}$ . Then  $P \in Syl_p(S_m)$  has size  $p^\mu$ , where

$$\begin{aligned} \mu &= \lfloor \frac{m}{p} \rfloor + \lfloor \frac{m}{p^2} \rfloor + \cdots + \lfloor \frac{m}{p^t} \rfloor = \\ &= (a_1 + a_2p + \cdots + a_t p^{t-1}) + (a_2 + a_3p + \cdots + a_t p^{t-2}) + \cdots + (a_{t-1} + a_t p) + (a_t) \\ &= a_1 + a_2(p+1) + a_3(p^2+p+1) + a_4(p^3+p^2+p+1) + \cdots + a_t(p^{t-1} + p^{t-2} + \cdots + 1). \end{aligned}$$

Thus,  $|P| = p^{a_1} p^{a_2(p+1)} p^{a_3(p^2+p+1)} \cdots p^{a_t(p^{t-1}+\cdots+1)} = |X_1^{a_1}| |X_2^{a_2}| \cdots |X_t^{a_t}|$ , where  $X_i \in Syl_p(S_{p^i})$ .

We partition  $\Omega$  into  $a_0$  1-element sets,  $a_1$   $p$ -element sets,  $a_2$   $p^2$ -element sets  $\cdots$  etc.

Hence the group  $1^{a_0} \times X_1^{a_1} \times X_1^{a_1} \times \cdots \times X_t^{a_t} \leq S_1^{a_0} \times S_p^{a_1} \times \cdots \times S_{p^t}^{a_t} \leq S_\Omega \cong S_m$ .

This group has the order of  $p$ , thus it is a Sylow  $p$ -subgroup of  $S_m$ .

## 5 Solvable groups and nilpotent groups

**Definition 5.1.** A finite group  $G$  is **solvable** if there exists a subnormal series

$G = N_0 \triangleright N_1 \triangleright \cdots \triangleright N_n = \{e\}$  ( $\forall N_i \triangleleft N_{i-1}$  but not necessarily  $N_i \triangleleft G$ ) such that  $N_i/N_{i+1}$  is abelian for all  $i$ .

**Definition 5.2.** A **composition series** of  $G$  is a subnormal series without repetitions, such that it cannot be refined properly (hence every  $N_i/N_{i+1}$  is simple).

**Remark 5.1.** A finite group  $G$  is solvable if and only if it has a composition series such that all  $N_i/N_{i+1}$  are of prime order.

**Definition 5.3.**  $[x, y] = x^{-1}y^{-1}xy$  is the **commutator element** of  $x$  and  $y$ .

**Remark 5.2.**  $[x, y] = 1$  if and only if  $xy = yx$ .

**Definition 5.4.**  $G' = \langle [x, y] \mid x, y \in G \rangle$  is called the **derived subgroup** of  $G$ .

**Definition 5.5.** A subgroup  $H \leq G$  is called a **characteristic subgroup** of  $G$  (denoted by  $H \text{ char } G$ ), if for every automorphism  $\varphi \in \text{Aut}(G)$ , we have that  $\varphi(H) = H$ .

**Remark 5.3.** If  $H \text{ char } G$  then  $H \triangleleft G$ .

*Proof.* If  $\varphi_g : G \rightarrow G$ , such that  $x \mapsto g^{-1}xg$ , then  $\varphi_g \in \text{Aut}(G)$ . Since  $H \text{ char } G$  we have that  $\varphi_g(H) = H$ , so  $g^{-1}Hg = H$ . Thus  $H \triangleleft G$ . □

**Remark 5.4.** If  $A \triangleleft B \triangleleft C$  then it is not necessarily true that  $A \triangleleft C$ .

**Example 5.1.** Let  $K_4 := \{(), (12)(34), (13)(24), (14)(23)\}$ ,  $C_2 = \{(), (12)(34)\} \triangleleft K_4 \triangleleft S_4$  but  $\{(), (12)(34)\}$  not normal in  $S_4$  because  $\pi = (23) \in S_4$  but  $\pi^{-1}(12)(34)\pi \notin C_2$ , hence  $C_2$  is not closed under conjugation.

**Remark 5.5.**

(i) If  $A \text{ char } B \triangleleft C$  then  $A \triangleleft C$ .

(ii) If  $A \text{ char } B \text{ char } C$ , then  $A \text{ char } C$ .

*Proof.* (i) Obviously  $A \leq C$ . Let  $g \in G$ . We will show that  $g^{-1}Ag = A$ .

Let  $\varphi_g : G \rightarrow G$  such that  $x \mapsto g^{-1}xg$ . Then  $\varphi_g(B) = B$ . We show that

$\varphi_g \in \text{Aut}(B)$ . This is because  $\varphi_g$  is bijective and  $\varphi_g(x)\varphi_g(y) = g^{-1}xgg^{-1}yg = g^{-1}xyg = \varphi_g(xy)$ .

Since  $A \text{ char } B$ ,  $\varphi_g(A) = A$  for every  $g \in G$ , hence  $A \triangleleft C$ .

(ii) See problem sheet 6/1. □

**Corollary 5.1.** If  $N$  is a normal subgroup of  $G$  then not necessarily  $N \text{ char } G$ .

*Proof.* In Example 5.1  $C_2 \triangleleft K_4$ , but  $C_2$  not characteristic in  $K_4$ .

Suppose  $C_2 \text{ char } K_4 \triangleleft S_4$ . Then  $C_2 \triangleleft S_4$ , and this is a contradiction. □

**Proposition 5.1.**  $G'$  is a characteristic subgroup of  $G$ .

*Proof.* We have to prove that for every  $\varphi \in \text{Aut}(G)$ ,  $\varphi(G') = G'$ .

It is enough to prove that for every  $x, y \in G$   $\varphi([x, y]) \in G'$ . Now,  $\varphi([x, y]) = \varphi(x^{-1}y^{-1}xy) = \varphi(x^{-1})\varphi(y^{-1})\varphi(x)\varphi(y) = \varphi(x)^{-1}\varphi(y)^{-1}\varphi(x)\varphi(y) = [\varphi(x), \varphi(y)] \in G'$ .

Since  $\varphi^{-1}(G') \leq G'$ , hence  $\varphi(G') = G'$  and we have that  $G'$  char  $G$ . □

**Definition 5.6.**  $G'' = (G')'$ ,  $G^{(i)} = (G^{(i-1)})'$

**Definition 5.7.** **Derived series** of  $G$  :  $G \geq G' \geq G'' \geq \dots \geq G^{(i)} \geq \dots$

**Remark 5.6.**  $G^{(i)}$  char  $G$ , in particular  $G^{(i)}$  is normal subgroup of  $G$ .

*Proof.*  $G'$  char  $G$ ,  $G'' = (G')'$  char  $G'$ , so by Remark 5.5 (ii) we have that  $G''$  char  $G$ .

Suppose by induction that  $G^{(i)}$  char  $G$ .

$G^{(i+1)} = (G^{(i)})'$  char  $G^{(i)}$  char  $G$ . By Remark 5.5 (ii) we have that  $G^{(i+1)}$  char  $G$ . □

**Remark 5.7.**  $G$  is abelian if and only if  $G' = \{1\}$ .

**Definition 5.8.**  $G$  is called **metabelian** if there exists a normal subgroup  $N \triangleleft G$  such that  $N$  is abelian and  $G/N$  is abelian.

**Remark 5.8.**  $G$  is metabelian if and only if  $G'' = 1$

**Remark 5.9.**  $G'$  is the minimal normal subgroup  $N$  such that  $G/N$  is abelian.

*Proof.*  $G/N$  is abelian  $\Leftrightarrow [xN, yN] = \bar{1} = N \Leftrightarrow [xN, yN] = [x, y]N = N \Leftrightarrow [x, y] \in N \Leftrightarrow G' \leq N$ .

□

**Corollary 5.2.**  $G$  is solvable if and only if there exists a natural number  $k$  such that  $G^{(k)} = \{1\}$ . The minimal such  $k$  is called the **derived length** of  $G$  denoted by  $d.l.(G)$ .

*Proof.*  $\Leftarrow$  :)

Suppose that  $G \geq G' \geq \dots \geq G^{(k)} = \{1\}$ . This chain is a normal series, and the factors  $G^{(i)}/G^{(i+1)} = G^{(i)}/(G^{(i)})'$  are abelian. Then  $G$  is solvable.

$\Rightarrow$  :)

Suppose that  $G$  is solvable. Then there exists a series  $G = N_0 \triangleright N_1 \triangleright N_2 \triangleright \dots \triangleright N_k = \{1\}$ ,

such that  $N_i/N_{i+1}$  is abelian for  $i = 0, 1, \dots, k-1$ . Since  $G/N_1$  is abelian, so  $G' \leq N_1$ . Since  $N_1/N_2$  is abelian, then  $N_1' \leq N_2$ , hence  $G'' \leq N_2$ . We want to prove that  $G^{(k)} \leq N_k = \{1\}$ . By induction suppose that  $G^{(i)} \leq N_i$ ,  $G^{(i+1)} \leq N_i'$  and  $N_i/N_{i+1}$  is abelian we have that  $N_i' \leq N^{i+1}$  hence  $G^{(i+1)} \leq N_{i+1}$ . Thus  $G^{(k)} = \{1\}$ .  $\square$

**Proposition 5.2.**

1. If  $G$  is solvable and  $H$  is a subgroup of  $G$ , then  $H$  is solvable and  $d.l.(H) \leq d.l.(G)$ .
2. If  $G$  is solvable then  $G/N$  is solvable and  $d.l.(G/N) \leq d.l.(G)$ .
3. If  $N$  is solvable normal subgroup of  $G$  and  $G/N$  is solvable then  $G$  is solvable and  $d.l.(G) \leq d.l.(N) + d.l.(G/N)$ .
4. If  $H, K$  are solvable then  $H \times K$  is solvable.

*Proof.* 1. This is because  $H^i \leq G^i$  for every  $i$ .

2. This is because  $H^i \leq (G/N)^i = G^i N / N$ .

3. Easy to see.

4. Easy to see.

$\square$

**Definition 5.9.** A nontrivial normal subgroup  $H$  of  $G$  is called a **minimal normal subgroup** of  $G$  if there exists no normal subgroup  $N$  such that  $1 \leq N \leq H$ .

**Definition 5.10.** A group  $G$  is called **characteristically simple** if there is no characteristic subgroup  $N$  of  $G$  such that  $\{1\} \leq N \leq G$ .

**Proposition 5.3.** *If  $\{1\} < N$  is a minimal normal subgroup of a group  $G$ , then  $N$  is characteristically simple.*

*Proof.* Suppose  $\{1\} \neq H \text{ char } N \triangleleft G, H \neq N$ . Then by Remark 5.3  $H \triangleleft G$  and this is a contradiction since  $N$  was minimal.  $\square$

**Theorem 5.11.** *If  $G$  is a finite solvable group, and  $N$  is a minimal normal subgroup of  $G$  then there exists a prime  $p$  such that  $N \cong C_p \times \cdots \times C_p$  ( $N$  is a so called elementary abelian  $p$ -group).*

*Proof.*  $N$  is characteristically simple (by Prop 5.3). Since  $N' \text{ char } N$ ,  $N' = N$  or  $N' = \{1\}$ . However,  $N' = N$  impossible, as  $N$  is solvable. Hence  $N$  is abelian. Now, by the fundamental theorem of abelian groups we have that  $N \cong N_{p_1} \times N_{p_2} \times \cdots \times N_{p_k}$ , where  $N_{p_i} \in \text{Syl}_{p_i}(N)$ . Then  $N_{p_i} \text{ char } N$ . Hence  $N_{p_i} = N$  or  $\{1\}$  since  $N$  is characteristically simple. Thus  $N$  is abelian  $p$ -group.

Let  $\Omega_n(N) := \langle x \in N \mid x^{p^n} = 1 \rangle$ . We prove that  $\Omega_n(N) \text{ char } N$ . Let  $\varphi \in \text{Aut}(N)$ . It is enough to prove that if  $x^{p^n} = 1$  then  $\varphi(x)^{p^n} = 1$ . But  $\varphi(x^{p^n}) = \varphi(x)^{p^n} = 1$ . In particular,  $\Omega_1(N) \text{ char } N$ . Hence  $\Omega_1(N) = \{1\}$  or  $\Omega_1(N) = N$ .

However,  $\Omega_1(N) = \langle x \mid x^p = 1 \rangle \neq \langle \{1\} \rangle$ , since there exists an element of order  $p$  in  $N$ .

Thus  $\Omega_1(N) = N$ . Since  $N$  is abelian, so  $N \cong C_p \times \cdots \times C_p$  elementary abelian.  $\square$

**Remark 5.10.** Every finite group of  $p$ -power order is solvable.

*Proof.* We know from (Algebra 1) that if  $|G| = p^k > 1$  then  $Z(G) \neq 1$ .

Let  $Z^2(G)$  be the inverse image of  $Z(G/Z(G))$  in  $G$ , and in general let  $Z^{i+1}(G)$  be the inverse image of  $Z(G/Z^i(G))$ . Then  $1 < Z(G) < Z^2(G) < \cdots$  and  $Z^{i+1}(G)/Z^i(G) = Z(G/Z^i(G))$  abelian. Hence  $G$  is solvable.  $\square$

**Theorem 5.12. (Burnside)**

*If  $G$  is a finite group and  $|G| = p^\alpha q^\beta$ ,  $p \neq q$  primes, then  $G$  is solvable.*

**Theorem 5.13. (Feit-Thompson 1963)**

*If  $G$  is a finite group and  $|G|$  is odd, then  $G$  is solvable.*

**Theorem 5.14. (Further properties of solvability)**

1. *If  $N, M$  are normal subgroups of  $G$  and  $G/N, G/M$  are solvable, then  $G/(N \cap M)$  is also solvable.*

2. If  $M, N$  are normal subgroups of  $G$  and  $M, N$  are solvable, then  $MN$  is also solvable.

*Proof.* 1. Let  $g \in G$ , let  $\varphi : G \rightarrow G/N \times G/M$  be a map such that  $g \mapsto (gN, gM)$ . Then this is a homomorphism and  $\ker \varphi = \{g \in G \mid g \in N \cap M\} = N \cap M$ . So by the homomorphism theorem  $G/(N \cap M) \cong \text{Im } \varphi \leq G/N \times G/M$ . Now we use Prop 5.2 (4) and (1) to get that  $G/(N \cap M)$  is solvable.

2. Since  $M$  is solvable and  $(MN)/N \cong M/(M \cap N)$  is solvable, moreover  $N$  is solvable, so by Prop 5.2 (3)  $MN$  is also solvable.

□

**Definition 5.15.** In a finite group  $G$  there is a biggest solvable normal subgroup (product of all solvable normal subgroups) is called the **solvable radical** of  $G$ .

**Remark 5.11.** If  $p, q$  are primes then every group of order  $pq$  is solvable.

*Proof.* If  $q > p$  and  $Q \in \text{Syl}_q(G)$  then  $Q \triangleleft G$ . Hence we have the normal series  $G \triangleright Q \triangleright \{1\}$ . Then  $G/Q \cong C_p$ , and  $Q/\{1\} \cong C_q$ . Hence  $G$  is solvable. □

**Remark 5.12.** If  $|G| = pqr$ , where  $p, q, r$  are different primes then  $G$  is solvable.

**Remark 5.13.** Groups of orders  $(1 - 59)$  are solvable.

**Remark 5.14.** If  $G$  is non-abelian simple group then  $G$  is not solvable since  $G' = G$ .

**Definition 5.16.** Let  $G$  be a group and let  $H, K$  be subgroups of  $G$ . Then the subgroup  $[H, K] := \langle [h, k] \mid h \in H, k \in K \rangle$  is called the **commutator subgroup** of  $H$  and  $K$ .

**Remark 5.15.**

1. Let  $H, K \leq G$ .  $K$  is a subgroup of  $N_G(H)$  if and only if  $[H, K] \leq H$ .
2. Suppose  $H$  is a subgroup of  $G$ ,  $K$  is normal subgroup of  $G$ , and  $K$  is a subgroup  $H$ . Then  $[H, G]$  is a subgroup of  $K$  if and only if  $H/K$  is a subgroup of  $Z(G/K)$ .

*Proof.* 1.  $\implies$ ) :

Let  $K \leq N_G(H)$ . It is enough to prove that for every  $h \in H$ , and for every  $k \in K$ ,  $[h, k] = h^{-1} \underbrace{k^{-1}hk}_{\in H} \in H$ . But since  $\underbrace{k^{-1}hk}_{\in H} \in H$  we have that  $[h, k] \in H$ .

$\impliedby$ ) :

Suppose that  $h^{-1}k^{-1}hk \in H$ , for every  $h \in H$ , and for every  $k \in K$   $k^{-1}hk \in H$  so  $K \leq N_G(H)$ .

2.  $[H, K] \leq K \Leftrightarrow H$  is commuting with  $G \bmod K$ . In other words  $H/K \leq Z(G/K)$ . □

**Definition 5.17.** (Lower central series of  $G$ )

$K_0(G) := G, K_1(G) := [G, G] = G', K_2(G) = [G', G] = [K_1(G), G], \dots$ . In general  $K_{i+1}(G) = [K_i(G), G]$ . Then  $K_0(G) \geq K_1(G) \geq \dots$  is the **lower central series** of  $G$ .

**Definition 5.18.** (Upper central series)

$Z^0(G) = \{1\}, Z^1(G) = Z(G), Z^2(G) = \text{inverse image of } Z(G/Z(G)) \text{ in } G$ . In general  $Z^{i+1}(G)/Z^i(G) = Z(G/Z^i(G))$ . Then  $Z^0(G) \leq Z^1(G) \leq Z^2(G) \leq \dots$  is the **upper central series** of  $G$ .

Written the following theorem we also introduce the notion of **nilpotent groups**.

**Theorem 5.19.** For a group  $G$  the following are equivalent:

1. The lower central series of  $G$  in finitely many steps reaches  $\{1\}$ .
2. The upper central series of  $G$  in finitely many steps reaches  $G$ .

The number of steps in (1) and (2) are equal. If this number is  $c$ , then  $G$  is called a **nilpotent group of class  $c$** , or shortly by  $c = cl(G)$ .

*Proof.* (2)  $\Rightarrow$  (1)

Suppose  $Z^c(G) = G$ , for some  $c$ . We will prove by induction on  $i$  that  $K_i(G) \leq Z^{c-i}(G)$  (\*). For  $i = 0, G = K_0(G) = Z^c(G) = G$ . Suppose that (\*) holds for  $i$ . Then by induction we have that  $K_{i+1}(G) = [K_i(G), G] \leq [Z^{c-i}(G), G] \leq Z^{c-i-1}$ , since

$Z^{c-i}(G)/Z^{c-i-1}(G) = Z\left(G/Z^{c-i-1}(G)\right)$ . Then (\*) holds for every  $i$  and hence  $K_c(G) \leq Z^0(G) = \{1\}$ .  
(1)  $\Rightarrow$  (2)

Suppose that  $K_c(G) = \{1\}$ . We want to prove that  $K_{c-j}(G) \leq Z^j(G)$ (\*\*). We prove by induction on  $j$ .

If  $j = 0$ , then  $\{1\} = K_c(G) = Z^0(G) = \{1\}$ . Suppose by induction that (\*\*) holds for  $j$ .

Then  $K_{c-j}(G) = [K_{c-(j+1)}, G]$ , thus  $K_{c-(j+1)}$  and  $G$  are interchangeable mod  $K_{c-j}(G)$ .

In other words  $K_{c-(j+1)}(G)/K_{c-j}(G) \leq Z\left(G/K_{c-j}(G)\right)$ .

By induction we know that  $K_{c-j}(G) \leq Z^j(G)$ . So we have that

$K_{c-(j+1)}(G)Z^j(G)/Z^j(G) \leq Z\left(G/Z^j(G)\right)$ . Hence  $K_{c-(j+1)}(G) \leq Z^{j+1}(G)$  holds.

Hence (\*\*) holds for every  $j$  and for  $j = c$  we have that  $G = K_0(G) \leq Z^c(G)$ . Thus  $Z^c(G) = G$ . □

**Definition 5.20.** A group  $G$  is called **supersolvable** if it has a normal series, where factors are of prime order.

**Remark 5.16.** Abelian groups  $\subsetneq$  nilpotent groups  $\subsetneq$  supersolvable groups  $\subsetneq$  solvable groups  $\subsetneq$  all finite groups.

**Example 5.2.** 1.  $S_3 \triangleright A_3 \triangleright \{e\}$  is supersolvable but not nilpotent, since  $Z(S_3) = \{1\}$ .

2. Every finite  $p$ -group is nilpotent  $1 < Z(G) < Z^2(G) < \dots < Z^c(G) = G$ .

3. We know that e.g.  $D_8$  and  $Q_8$  are nilpotent but not abelian  $p$ -groups.

4.  $A_5$  is not solvable, since  $A'_5 = A_5$ .

5.  $S_4$  is solvable but not supersolvable, since the only normal subgroups in  $S_4$  are  $S_4, A_4, K_4$  and  $\{1\}$ . There is no normal subgroup of order 2 in it. In the series  $S_4 \triangleright A_4 \triangleright K_4 \triangleright \{1\}$ , the factors are abelian.

**Theorem 5.21. (Properties of nilpotency)**

1. If  $G$  is nilpotent and  $H$  is a subgroup of  $G$ , then  $H$  is also nilpotent and  $cl(H) \leq cl(G)$ .



2. If  $G$  is nilpotent and  $N$  is normal subgroup of  $G$ , then  $G/N$  is also nilpotent and  $cl(G/N) \leq cl(G)$ .

3. If  $G_1$  and  $G_2$  are nilpotent, then  $G_1 \times G_2$  is nilpotent and  $cl(G_1 \times G_2) = \max(cl(G_1), cl(G_2))$ .

*Proof.* 1. This is because  $K_i(H)$  is a subgroup of  $K_i(G)$  hence  $cl(H) \leq cl(G)$ .

2. This is because  $K_i(G)N/N = K_i(G/N)$ , and so  $cl(G/N) \leq cl(G)$ .

3. Easy to see. □

**Remark 5.17.** If  $N$  is a nilpotent normal subgroup of  $G$  and  $G/N$  is nilpotent, then  $G$  is not necessarily nilpotent. (See Example 5.3.)

**Example 5.3.**  $S_3 \triangleright A_3, S_3/A_3 \cong C_2$  is nilpotent and  $A_3 \cong C_3$  is nilpotent( $p$ -group). But  $S_3$  is not nilpotent since  $Z(S_3) = \{1\}$ .

**Theorem 5.22. (Frattini-argument)**

Let  $G$  be a finite group and let  $H$  be a normal subgroup of  $G$ ,  $P \in Syl_p(H)$ . Then  $G = HN_G(P)$ .

*Proof.* It is enough to prove that  $G \leq HN_G(P)$ . Let  $g \in G$ , since  $H \triangleleft G$ , we have that  $P^g \leq H$ , and  $P^g \in Syl_p(H)$ . By Sylow's theorem, there exists an element  $h \in H$  such that  $P^g = P^h$ , so  $P^{gh^{-1}} = P$  and hence  $gh^{-1} \in N_G(P)$ . Then  $gh^{-1} = n \in N_G(P)$ . Thus  $g = nh = h_1n \in HN_G(P)$  for some  $h_1 \in H$ . □

**Theorem 5.23.** If  $G$  is a finite group then the following are equivalent:

1.  $G$  is nilpotent.
2. For every proper subgroup  $H \subsetneq G$ ,  $H \subsetneq N_G(H)$  holds.
3. Every maximal subgroup of  $G$  is of prime index and normal.
4. Every Sylow subgroup of  $G$  is normal.

5.  $G$  is the direct product of its Sylow subgroups.

6. If  $x, y \in G$  and  $(o(x), o(y)) = 1$  then  $[x, y] = 1$ .

*Proof.* (1)  $\Rightarrow$  (2)

Suppose that  $G$  is nilpotent of class  $c$ . We have to prove that  $N_G(H) > H$ .

Since  $K_c(G) = \{1\}$ , there exists an index  $i$  such that  $K_i(G) \not\leq H$  but  $K_{i+1}(G) \leq H$ . Since  $[K_i(G), H] \leq K_{i+1}(G) \leq H$ , we have that  $K_i(G) \leq N_G(H)$  by Remark 5.15 (1), and so  $N_G(H) > H$ .

(2)  $\Rightarrow$  (3)

Let  $M$  be maximal subgroup in  $G$ . Then  $M \neq G$  and by (1)  $M < N_G(M) = G$ . Hence  $M \triangleleft G$ . We have to prove that  $[G : M]$  is prime. Since  $M \triangleleft G$  and  $M$  is maximal in  $G$ , hence  $G/M$  has no nontrivial proper subgroups, so  $G/M \cong C_p$ , for some prime  $p$ .

(3)  $\Rightarrow$  (4)

Suppose by contradiction that there exists a Sylow subgroup  $P \in \text{Syl}_p(G)$ , such that  $P \not\triangleleft G$ . Then since  $N_G(P) \not\leq G$  we can find a maximal subgroup  $H$  such that  $N_G(P) \leq H < G$ .

From (3) we know that  $H \triangleleft G$ .

Now, by the Frattini-argument we have that  $G = HN_G(P) \leq H$ , which is a contradiction.

Hence  $P \triangleleft G$ .

(4)  $\Rightarrow$  (5)

Let  $|G| = \prod_{i=1}^t p_i^{\alpha_i}$  and let  $P_i \in \text{Syl}_{p_i}(G)$ . From (4) we have that  $P_i \triangleleft G, i = 1, \dots, t$ , hence

$\prod_{i=1}^t P_i \triangleleft G$ . For all  $i$ , we have that  $P_i \leq \prod_{j=1}^t P_j$ , hence  $|P_i|$  divides  $|\prod_{j=1}^t P_j|$  and hence

$$\prod_{j=1}^t |P_j| \left| \prod_{j=1}^t P_j \right| \leq |G|. \text{ But } \prod_{j=1}^t |P_j| = |G|, \text{ so } \prod_{j=1}^t |P_j| = \left| \prod_{j=1}^t P_j \right| = |G|.$$

Now,  $P_i \triangleleft G$ , for  $i = 1, \dots, t$ , so  $\prod_{j=1}^t P_j = G$ . We have to prove that  $P_i \cap \prod_{j \neq i} P_j = \{1\}$ .

Then we will have  $G = \times_{i=1}^t P_i$ . Now,  $|P_1 P_2| = \frac{|P_1| |P_2|}{|P_1 \cap P_2|}$  divides  $|P_1| |P_2|$ ,

$$|P_1 P_2 P_3| = \frac{|P_1 P_2| |P_3|}{|P_1 P_2 \cap P_3|} \left| P_1 P_2 P_3 \right| \left| P_1 P_2 P_3 \right| \text{ and by induction we have that}$$

$|\prod_{j \neq i} P_j| \mid \prod_{j \neq i} |P_j|$ . Hence  $P_i \cap \prod_{j \neq i} P_j = \{1\}$ .  
(5)  $\Rightarrow$  (6)

We have to prove that if  $x, y \in G$ , and  $(o(x), o(y)) = 1$ , then  $[x, y] = 1$ . Since  $G = \times_{i=1}^t P_i$ ,  $x = (x_1, x_2, \dots, x_t)$ , where  $x_i \in P_i$  and  $y = (y_1, y_2, \dots, y_t)$ , where  $y_i \in P_i$ . If  $x_i \neq 1$ , then  $y_i = 1$  and if  $y_j \neq 1$  then  $x_j = 1$ . So  $xy = yx$  hence  $[x, y] = 1$ .

(5)  $\Rightarrow$  (1)

We know that  $G = \times_{i=1}^t P_i$ , when  $P_i \in Syl_{p_i}(G)$ . We also know that every finite  $p$ -group is nilpotent. As  $G$  is the direct product of nilpotent groups it is also  $G$  is nilpotent by Theorem 5.21 (3).

(6)  $\Rightarrow$  (4)

From (6) we have that  $[P_i, P_j] = 1$  for every  $i \neq j$ , hence  $P_i \leq N_G(P_j)$  and  $P_j \leq N_G(P_i)$ . So  $\prod P_i \leq G$ . However,  $\prod |P_i| \mid |G|$ , but  $\prod |P_i| = |G|$ , so  $\prod P_i = G$ . If  $g \in G$  then  $g = p_1 p_2 \dots p_t$ , where  $p_i \in P_i$ . Hence  $P_i^{p_1 \dots p_t} = P_i$ . Thus  $g \in N_G(P_i)$  and so  $P_i \triangleleft G$   $\square$

## 6 Hall theorems, and the Schur-Zassenhaus theorem

**Definition 6.1.** If  $G$  is a finite group and  $|G| = \prod_{i=1}^t p_i^{\alpha_i}$ ,  $\pi(G) = \{p_1, p_2, \dots, p_k\}$ , **set of prime divisors** of  $G$ . For a subset  $\pi \subset \pi(G)$  we define  $\pi' = \pi(G) \setminus \pi$ . In particular  $p' = \pi(G) \setminus \{p\}$ . We say that  $n$  is a  $\pi$ -number if the prime divisors of  $n$  are in the set  $\pi$ ,  $n$  is a  $\pi'$ -number if the prime divisors of  $n$  are in the set  $\pi'$ .

**Definition 6.2.** Let  $\pi$  be a subset of  $\pi(G)$ . Let  $H$  be a subgroup of  $G$  and let  $\pi(H) = \pi$  and suppose that  $([G : H], |H|) = 1$  then we call  $H$  a **Hall  $\pi$ -subgroup** of  $G$ .

**Definition 6.3.** A subgroup  $H$  of  $G$  is a  **$\pi$ -subgroup** of  $G$  if  $\pi(H) \subseteq \pi$ .

**Definition 6.4.**  $Hall_{\pi}(G) = \{H \leq G \mid H \text{ is a Hall } \pi\text{-subgroup of } G\}$ .

**Theorem 6.5. (Ph. Hall 1939)**

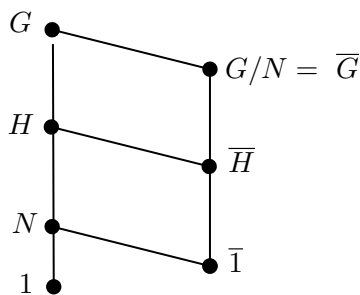
(Analogues of Sylow's theorems for solvable groups)

1.  $E_\pi$ , for every subset  $\pi$  of  $\pi(G)$  there exists a Hall  $\pi$ -subgroup  $H \in Hall_\pi(G)$ .
2.  $C_\pi$ , every Hall  $\pi$ -subgroup of  $G$  is conjugate in  $G$ .
3.  $D_\pi$ , every  $\pi$ -subgroup of  $G$  can be embedded into a Hall  $\pi$ -subgroup of  $G$ .

*Proof.* (of  $E_\pi$ )

The proof is by induction on  $|G|$ . If  $G$  is a  $p$ -group then  $H = G$ . Let  $G$  be an arbitrary finite solvable group. Let  $1 \neq N \triangleleft G$  be a minimal normal subgroup. We have seen that  $N$  is an elementary abelian  $p$ -group. In  $G/N$  by induction  $E_\pi$  holds. Let  $\bar{H} = H/N \in Hall_\pi(G/N)$ . There are two cases:

1. If  $p \in \pi$  then the inverse image  $H$  of  $\bar{H}$  is also a  $\pi$ -group.



$[G : H] = [G/N : H/N]$  and it is a  $\pi$ ! number. So  $H \in Hall_\pi(G)$ .

2. If  $p \notin \pi$ , ( $\underbrace{|N|}_{\pi' \text{-number}}$ ,  $\underbrace{|H/N|}_{\pi \text{-number}}$ ) = 1. By the Schur-Zassenhaus theorem (see Theorem 6.7), there exists a subgroup  $H_1 \leq H$  such that  $H = N \cdot H_1$  and  $N \cap H_1 = \{1\}$  (complement to  $N$  in  $H$ ).

Then  $H/N \cong H_1$ , so  $|H_1|$  is a  $\pi$ -number and  $[G : H_1] = [G : H][H : H_1] = [G : H]|N|$ , which is a  $\pi'$ -number. So  $H_1 \in Hall_\pi(G)$ .

□

**Remark 6.1.** 1. If  $\pi = \{p\}$  we get Sylow's theorems for solvable groups.

2. Solvability is important

- $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$ , there is no subgroup  $H \leq A_5$  such that  $|H| = 15$ , then there is no Hall  $(3, 5)$ -subgroup in  $A_5$ .
- $|GL(3, 2)| = (2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 2^3 \cdot 3 \cdot 7$ . In  $GL(3, 2)$  there are two non-conjugate Hall  $\{2, 3\}$ -subgroups both isomorphic to  $S_4$ .
- $PSL(2, 11) = SL(2, 11)/Z(SL(2, 11))$ , it's order is  $2^2 \cdot 3 \cdot 7 \cdot 11$ . There exist Hall  $\{2, 3\}$ -subgroups that are not isomorphic,  $(A_4, D_{12})$ .

**Remark 6.2.**  $G$  is solvable if and only if for every subset  $\pi$  of  $\pi(G)$ , there exist a Hall  $\pi$ -subgroup of  $G$ , moreover,  $G$  is solvable if and only if for all  $p \in \pi(G)$ , there exists a Hall  $p'$ -subgroup of  $G$ .

**Theorem 6.6. (Gaschütz) (special case of Schur-Zassenhaus)**

Let  $G$  be a finite group,  $N$  a normal subgroup of  $G$  such that  $N$  is abelian and  $(|N|, [G : N]) = 1$  then there exists a subgroup  $H \leq G$  such that  $H \cap N = \{1\}$ , and  $HN = G$  ( $H$  is complement to  $N$  in  $G$ ).

*Proof.* Let  $|G : N| = m$ , and  $|N| = n$ . Then  $(m, n) = 1$ . The elements of the factor group  $G/N$  are cosets of  $N$ . Let  $\alpha \in G/N, x_\alpha \in \alpha$  (a representative of the coset  $\alpha$ ). Then  $G = \bigcup_{\alpha \in G/N}^* x_\alpha N$ . Let  $X := \{x_\alpha \mid \alpha \in G/N\}$ . It is enough to prove that we can choose  $X$  to be closed under multiplication. Then  $X$  will be a subgroup, since  $o(x_\alpha) = k < \infty$  for some  $k$ , thus  $x_\alpha^k = 1 \in X$  and  $x_\alpha^{k-1} = x_\alpha^{-1} \in X$  also holds. Moreover,  $X$  will be a complement to  $N$ , since  $XN = G$  and  $X \cap N = \{1\}$ .

Our aim is to find a set of coset representatives which is closed under multiplication. Since  $x_\alpha x_\beta \in x_{\alpha\beta} N$ , there exists a function  $f : G/N \times G/N \rightarrow N$  such that  $f(\alpha, \beta) \in N$  and  $x_\alpha x_\beta = x_{\alpha\beta} f(\alpha, \beta)$ .

As the multiplication in  $G$  is associative, we have that  $(x_\alpha x_\beta) x_\gamma = x_\alpha (x_\beta x_\gamma)$ . Hence  $(x_\alpha x_\beta) x_\gamma = x_{\alpha\beta} f(\alpha, \beta) x_\gamma = x_{\alpha\beta} x_\gamma x_\gamma^{-1} f(\alpha, \beta) x_\gamma = x_{\alpha\beta} x_\gamma f(\alpha, \beta)^{x_\gamma} = x_{(\alpha\beta)\gamma} f(\alpha, \beta, \gamma) f(\alpha, \beta)^{x_\gamma}$ . On the other hand,  $x_\alpha (x_\beta x_\gamma) = x_\alpha x_{\beta\gamma} f(\beta, \gamma) = x_{\alpha(\beta\gamma)} f(\alpha, \beta\gamma) f(\beta, \gamma)$ . Thus we have that

$f(\alpha\beta, \gamma)f(\alpha, \beta)^{x\gamma} = f(\alpha, \beta\gamma)f(\beta, \gamma)^{(*)}$  (a function  $f : G/N \times G/N \rightarrow N$  satisfying  $(*)$  is called a **factor set** ).

Let  $g(\beta) := \prod_{\alpha \in G/N} f(\alpha, \beta)$ . Now we multiply both sides of  $(*)$  for every  $\alpha$ .

Since  $N$  is abelian, we have that  $\prod_{\alpha \in G/N} f(\alpha\beta, \gamma) \prod_{\alpha \in G/N} f(\alpha, \beta)^{x\gamma} = \prod_{\alpha \in G/N} f(\alpha, \beta\gamma)f(\beta, \gamma)^m$ .

Hence  $g(\gamma)g(\beta)^{x\gamma} = g(\beta\gamma)f(\beta, \gamma)^m$  and  $g(\beta)^{x\gamma}g(\gamma)f(\beta, \gamma)^{-m} = g(\beta\gamma)$  (\*\*)

Since  $|G/N| = m$ ,  $|N| = n$ , and  $(m, n) = 1$ , we have that there exists an integer  $m'$  such that  $(-m)m' \equiv 1(n)$ . Thus  $-mm' = kn + 1$  and if  $z \in N$  then  $z^{-mm'} = z^{nk+1} = z$ .

Let  $h$  be a function  $h : G/N \rightarrow N$  such that  $h(\alpha) = g(\alpha)^{m'}$ . Let  $y_\alpha = x_\alpha h(\alpha)$  be another set of coset representatives of  $N$ . We prove that it is closed under multiplication.

We raise to the  $(m')^{th}$  power both sides of (\*\*), then we have that  $h(\beta)^{x\gamma}h(\gamma)f(\beta, \gamma) = h(\beta\gamma)$  (\*\*\*) .

Now,  $y_\beta y_\gamma = x_\beta h(\beta)x_\gamma h(\gamma) = x_\beta x_\gamma x_\gamma^{-1} h(\beta)x_\gamma h(\gamma) = x_\beta x_\gamma h(\beta)^{x\gamma} h(\gamma) = x_{\beta\gamma} f(\beta, \gamma) h(\beta)^{x\gamma} h(\gamma) = x_{\beta\gamma} h(\beta\gamma) = y_{\beta\gamma}$ .

Hence  $Y$  is closed under multiplication, and  $Y = \{y_\alpha \mid \alpha \in G/N\}$  complement to  $N$ .  $\square$

**Theorem 6.7. (Schur–Zassenhaus theorem)**

If  $G$  is a finite group and  $N$  is a normal subgroup of  $G$  such that  $(|N|, |G : N|) = 1$ , then there exists a subgroup  $H \leq G$  such that  $HN = G$ ,  $H \cap N = \{1\}$ , in other words  $H$  is a complement to  $N$ .

*Proof.* We proved this if  $N$  is abelian, this was Gaschütz’s theorem.

Let  $G$  be a minimal counterexample, Suppose that  $N$  does not have a complement

**Claim 1:**  $N$  is nilpotent.

If  $N$  is not nilpotent then there exists  $P \in Syl_p(N)$  such that  $P \not\triangleleft G$ . Hence  $N_G(P) \not\leq G$ . By the Frattini-argument  $G = N \cdot N_G(P)$  (\*) because  $G$  is minimal and  $N_G(P)$  is a smaller group. We have that  $N \cap N_G(P) \triangleleft N_G(P)$  and  $|N \cap N_G(P)| \mid |N|$ , moreover (\*\*)  $[N_G(P) : N_G(P) \cap N] = |N_G(P)/N_G(P) \cap N| = |N_G(P)N/N| \stackrel{(*)}{=} |G/N|$ . Since  $(|N|, |G/N|) = 1$  we have that  $(|N \cap N_G(P)|, [N_G(P) : N_G(P) \cap N]) = 1$ , by induction there exist a complement  $H$  to  $N \cap N_G(P)$  in  $N_G(P)$ . Hence

$H \cdot (N \cap N_G(P)) = N_G(P)$ ,  $H \cap (N \cap N_G(P)) = \{1\}$ . By (\*\*) we have that  $|H| = [G : N]$  and  $N_G(P)/N \cap N_G(P) \cong H$ . Hence  $|HN| = \frac{|H| |N|}{|H \cap N|} = |G|$  so  $H \cap N$  and  $H$  is also a complement to  $N$  in  $G$  and this contradiction shows that  $N$  is nilpotent.

**Claim 2:**  $N$  is abelian.

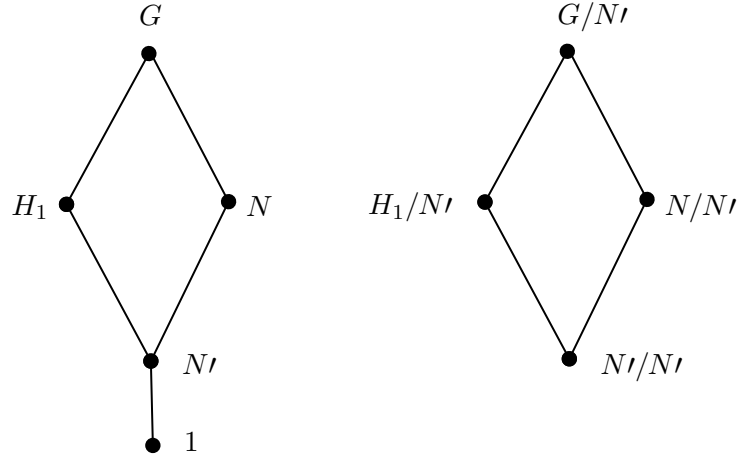
Since  $N$  is nilpotent it is also solvable. So  $N' < N$ . If  $N$  is not abelian then  $N' \neq 1$  and  $N'$  char  $N \triangleleft G$  so  $N' \triangleleft G$ . Since  $|G/N'| < G$  we can apply induction then  $N/N' \triangleleft G/N'$  and  $(|N/N'|, \underbrace{[G/N' : N/N']}_{[G:N]}) = 1$ .

By introduction there exists a complement  $H/N'$  to  $N/N'$  in  $G/N'$ . Then

$|H_1/N| = [G/N' : N/N'] = [G : N]$  and  $NH_1 = G$ ,  $N \cap H_1 = N'$ . By (\*\*\*),  $|G| = |NH_1| = \frac{|N| |H_1|}{|N' \cap H_1|}$  hence  $|H_1| = \frac{|G|}{|N|}$ , and  $\frac{|G|}{|N|} = \frac{|H_1|}{|N'|}$ . Since  $H_1 < G$ ,  $N' \triangleleft H_1$ ,

$(|N'|, \underbrace{[H_1 : N']}_{[G:N]}) = 1$ , by induction there exists a subgroup  $H_2 \leq H_1$ , such that  $N'H_2 = H_1$

and  $N' \cap H_2 = 1$ . (\*\*\*\*)



Then  $|H_2| = \frac{|H_1|}{|N'|} = \frac{|G|}{|N|}$ . We show that  $H_2$  is complement to  $N$  in  $G$ . This is because  $NH_2 = NN'H_2 \stackrel{****}{=} NH_1 = G$ ,  $N \cap H_2 \subseteq N \cap H_1 = N'$ ,  $N \cap H_2 = N \cap H_2 \cap N' = 1$  and this is contradiction.  $\square$

## 7 Normal $p$ -complement theorems and the transfer

**Definition 7.1.** If for  $P \in Syl_p(G)$ , there exists a normal subgroup  $K \triangleleft G$  such that  $KP = G$  and  $K \cap P = \{1\}$ , then we tell that  $K$  is a **normal  $p$ -complementnormal  $p$ -complement** in  $G$ .

**Remark 7.1.** Since  $G/K = KP/K \cong P/K \cap P \cong P$ , thus  $K \in Hall_{p'}(G)$ .

**Definition 7.2.** A group  $G$  is  **$p$ -nilpotent** if it has a normal  $p$ -complement.

**Theorem 7.3.** A finite group  $G$  is nilpotent if and only if  $G$  is  $p$ -nilpotent for every  $p \in \pi(G)$ .

*Proof.*  $\Leftarrow$ ) Suppose that  $G$  is  $p$ -nilpotent for every  $p \in \pi(G)$ . For every  $p_i \in \pi(G)$ ,  $K_i \in Hall_{p_i'}(G)$ ,  $K_i \cap P_i = 1$ ,  $K_i \cdot P_i = G$  and if  $p \neq p_i$  then  $P \leq K_i$  for every  $P \in Syl_p(G)$ . Hence  $P = \bigcap_{p \neq p_i} K_i \triangleleft G$ , and so  $G$  is nilpotent by Theorem 5.23.

$\Rightarrow$ ) If  $G$  is nilpotent then  $G = P_1 \times \cdots \times P_t$  and  $\prod_{j \neq i} P_j$  is a normal  $p_i$ -complement in  $G$ .

□

Our aim is to prove the Burnside's transfer theorem, see Theorem 7.8. To prove it we need the following results.

**Lemma 7.1.** Let  $Q$  be a subgroup of  $G$  of index  $n$ . Let  $\{l_1, \dots, l_n\}$  and  $\{h_1, \dots, h_n\}$  be two complete sets of representatives of left cosets (left transversals) of  $Q$  in  $G$ . Then  $G = \bigcup_{i=1}^{n^*} l_i Q = \bigcup_{i=1}^{n^*} h_i Q$  and for all  $g \in G$  and for every  $i \in \{1, \dots, n\}$ , there exists a unique,  $\sigma(i) \in \{1, \dots, n\}$  and there exists a unique  $x_i \in Q$  such that  $gh_i = l_{\sigma(i)} x_i$ . Moreover  $\sigma \in S_n$ .

*Proof.* Since  $\bigcup_{i=1}^{n^*} h_i Q = \bigcup_{i=1}^n l_i Q$ ,  $gh_i$ , there exists a unique  $j$  such that  $gh_i \in l_j Q$ . Then  $gh_i = l_j x_i$ , for a unique  $x_i \in Q$ .

Let  $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  mapping  $i \mapsto j$ . then  $\sigma$  is injective. Suppose  $\sigma(k) = j = \sigma(i)$ . It means that,  $gh_k = l_j x_k$  hence  $gh_k x_k^{-1} = l_j$  and  $gh_i = l_j x_i$  hence  $gh_i x_i^{-1} = l_j$ . So



$gh_kx_k^{-1} = gh_ix_i^{-1}$  and hence  $h_kx_k^{-1} = h_ix_i^{-1}$ . Thus  $h_i^{-1}h_k = x_i^{-1}x_k \in Q$ , which implies that  $h_iQ = h_kQ$ . So  $i = k$  and  $\sigma$  is injective on a finite set to itself so it is also surjective and  $\sigma$  is a permutation on  $\{1, \dots, n\}$ .  $\square$

**Proposition 7.1. (Special cases)**

1. If  $l_i = h_i$  then  $gl_i = l_{\sigma(i)}x_i$  (\*)
2. If  $g = 1$ , then  $1 \cdot h_i = l_{\sigma(i)}x_i$

**Definition 7.4. (Transfer)**

Let  $Q$  be a subgroup  $G$  and  $[G : Q] = n$ . The **transfer** is a function  $V : G \rightarrow Q/Q'$  such that  $g \mapsto \left(\prod_{i=1}^n x_i\right)Q'$ , where  $G = \bigcup_{i=1}^n l_iQ$  and  $gl_i = l_{\sigma(i)}x_i, x_i \in Q$ .

**Theorem 7.5.** *If  $Q$  is a subgroup of  $G$ ,  $[G : Q] = n$  and  $V : G \rightarrow Q/Q'$  is the transfer map, then  $V$  is a homomorphism and  $V$  is independent of the left transversal of  $Q$  in  $G$ .*

*Proof.* Let  $\{l_1, \dots, l_n\}, \{h_1, \dots, h_n\}$  be two left transversals of  $Q$  in  $G$ . Then  $G = \bigcup_{i=1}^{n*} l_iQ = \bigcup_{i=1}^{n*} h_iQ$ . Let  $g \in G$ . Then we have that there exist unique  $\sigma, \tau$  and  $\alpha \in S_n$  and unique  $x_i, y_i$  and  $z_i \in Q$  such that

$$\begin{aligned} gl_i &= l_{\sigma(i)}x_i \quad (*) \\ gh_i &= h_{\tau(i)}y_i \quad (**) \\ 1h_i &= l_{\alpha(i)}z_i \quad (***) \\ gh_i &\stackrel{(***)}{=} g(l_{\alpha(i)}z_i) \stackrel{(*)}{=} l_{\sigma(\alpha(i))}x_{\alpha(i)}z_i \quad (****) \end{aligned}$$

Now, let  $\alpha(j) = \sigma(\alpha(i))$  then  $j = \alpha^{-1}\sigma\alpha(i)$  (v).

Now,  $h_j \stackrel{(***)}{=} l_{\alpha(j)}z_j$  and so  $l_{\alpha(j)} = h_jz_j^{-1}$ , hence  $gh_i \stackrel{(***)}{=} l_{\alpha(j)}x_{\alpha(i)}z_i = h_jz_j^{-1}x_{\alpha(i)}z_i$ .

On the other hand,  $gh_i \stackrel{(**)}{=} h_{\tau(i)}y_i$  and we have that  $\tau(i) = j$  and  $y_i = z_j^{-1}x_{\alpha(i)}z_i \stackrel{(v)}{=} z_{\alpha^{-1}\sigma\alpha(i)}^{-1}x_{\alpha(i)}z_i$ .

So  $\prod_{i=1}^n y_iQ' = \prod_{i=1}^n z_{\alpha^{-1}\sigma\alpha(i)}^{-1}x_{\alpha(i)}z_iQ' = \prod_{i=1}^n x_{\alpha(i)}Q' = \prod_{i=1}^n x_iQ'$ . Hence  $V$  is independent of the left transversal of  $Q$  in  $G$ . We want prove that  $V : G \rightarrow Q/Q'$  is a homomorphism.

It is enough to prove that  $V(gg') = V(g)V(g')$ . Let  $G = \bigcup_{i=1}^{n*} l_iQ$ . Then  $gl_i = l_{\sigma(i)}x_i$ ,

$g'l_i = l_{\tau(i)}y_i$ . So  $gg'l_i = gl_{\tau(i)}y_i = l_{\sigma\tau(i)}x_{\tau(i)}y_i$ . Hence  $V(gg') = \pi x_{\tau(i)}y_iQ' = \pi x_{\tau(i)}Q'\pi y_iQ' = \pi x_iQ'\pi y_iQ' = V(g)V(g')$ .  $\square$

**Definition 7.6.** Let  $[G : Q] = n$ , and let  $K$  be a normal subgroup of  $G$ . Suppose that  $KQ = G$  and  $K \cap Q = \{1\}$ . Then we say that  $K$  is a **normal complement** to  $Q$ .

**Remark 7.2.** If  $K$  is a normal complement to  $Q$ , then  $|K| = [G : Q] = n$  and  $K = \{a_1, \dots, a_n\}$  is a left transversal to  $Q$  in  $G$  and  $K \leq \ker(V)$ . ( $V : G \rightarrow Q/Q'$  transfer map)

*Proof.*  $n = [G : Q] = \frac{|G|}{|Q|} = \frac{|KQ|}{|Q|} = \frac{|K||Q|}{|K \cap Q||Q|} = |K|$ . Since  $K = \{a_1, \dots, a_n\}$ , we have

that  $G = KQ = \bigcup_{i=1}^n a_iQ$ . This is a disjoint union, since if  $a_iQ = a_jQ$  then  $a_j^{-1}a_i \in Q \cap K = \{1\}$ , so  $a_i = a_j$  and then  $K = \{a_1, \dots, a_n\}$  is a left transversal to  $Q$  in  $G$ .

Let  $V : G \rightarrow Q/Q'$  be the transfer map. We want to prove that  $K \leq \ker(V)$ .

Let  $k \in K$ . Then  $ka_i = a_{\sigma(i)}x_i$  where  $\sigma \in S_n$  and  $x_i \in Q \cap K = \{1\}$ . Thus  $V(k) = \prod 1 \cdot Q' = Q'$ . Hence  $k \in \ker(V)$ , for every  $k \in K$  so  $K \leq \ker(V)$ .  $\square$

**Remark 7.3.** If  $Q$  is abelian, then  $Q/Q' = Q$  so  $\text{Im}(V) \leq Q$ .

**Corollary 7.1.** Let  $[G : Q] = n$ , let  $Q$  be abelian and let  $K$  be a normal complement to  $Q$  in  $G$ . If  $V : G \rightarrow Q/Q'$  is surjective, then  $\ker(V) = K$ .

*Proof.* We have seen  $K \leq \ker(V)$ . By the Homomorphism theorem we have that  $G/\ker(V) \cong \text{Im}(V) = Q/Q' = Q$ , since  $Q$  is abelian. Since  $\frac{|G|}{|\ker(V)|} = |Q|$  and  $\frac{|G|}{|K|} = |Q|$ , we have that  $K = \ker(V)$ .  $\square$

**Lemma 7.2. (Nice form of the transfer map)**

Let  $Q$  be a subgroup of  $G$ ,  $[G : Q] = n$ ,  $\bigcup_{i=1}^n l_iQ = G$ , then for every  $g \in G$ , there exist elements  $h_1, h_2, \dots, h_m \in G$  and integers  $n_1, \dots, n_m \in \mathbb{N}$  with (depending on  $g$ ) such that

1.  $h_i^{-1}g^{n_i}h_i \in Q$ ,
2.  $\sum_{i=1}^m n_i = n$ ,

$$3. V(g) = \prod_{i=1}^m (h_i^{-1} g^{n_i} h_i) Q'.$$

*Proof.* We have that  $gl_i = l_{\sigma(i)} x_i$ , where  $\sigma \in S_n$  and  $x_i \in Q$ . Now we write  $\sigma$  as product of disjoint cycles:  $\sigma = \alpha_1 \alpha_2 \cdots \alpha_m$ .

Let  $\alpha_i = (j_1, \dots, j_r)$ ,  $gl_1 = l_{\sigma(j_1)} x_{j_1} = l_{j_2} x_{j_1}$

$gl_{j_2} = l_{\sigma(j_2)} x_{j_2} = l_{j_3} x_{j_2}$

$\vdots$

$gl_{j_{r-1}} = l_{\sigma(j_{r-1})} x_{j_{r-1}} = l_{j_r} x_{j_{r-1}}$

$gl_{j_r} = l_{\sigma(j_r)} x_{j_r} = l_{j_1} x_{j_r}$ . Then  $x_{j_r} = l_{j_1}^{-1} gl_{j_r}$ ,  $x_{j_{r-1}} = l_{j_r}^{-1} gl_{j_{r-1}}$ ,  $\dots$ ,  $x_{j_1} = l_{j_2}^{-1} gl_1$ .

Let  $h_i = l_{j_1}$ ,  $n_i = r$  for  $i = 1, \dots, n$ . Hence we have that

$$Q \ni x_{j_r} x_{j_{r-1}} \cdots x_{j_1} = (l_{j_1}^{-1} gl_{j_r})(l_{j_r}^{-1} gl_{j_{r-1}}) \cdots (l_{j_3}^{-1} gl_{j_2})(l_{j_2}^{-1} gl_{j_1}) = (l_{j_1}^{-1} g^r l_{j_1}) = (h^{-1} g^{n_i} h).$$

Repeating this process for each  $\alpha_i, i = 1, \dots, m$ , we have that

$$V(g) = \prod_{i=1}^n x_i Q' = \prod_{i=1}^m (x_{j_r} x_{j_{r-1}} \cdots x_{j_1}) Q' = \prod_{i=1}^m h_i^{-1} g^{n_i} h_i Q'. \quad \square$$

**Theorem 7.7.** *If  $Q$  is a subgroup of  $G$ ,  $[G : Q] = n$  and  $Q$  is abelian such that  $Q \leq Z(G)$  then  $V(g) = g^n$  for every  $g \in G$ .*

*Proof.* Let  $g \in G$ . Then by Lemma 7.2 we have that  $V(g) = \prod_{i=1}^m h_i^{-1} g^{n_i} h_i Q' = \prod_{i=1}^m h_i^{-1} g^{n_i} h_i$ .

and

$h_i^{-1} g^{n_i} h_i \in Q$ . As  $Q \triangleleft G$ , then  $g^{n_i} \in Q$  also holds.

However, Since  $Q \leq Z(G)$ ,  $g^{n_i} = h_i (h_i^{-1} g^{n_i} h_i) h_i^{-1} = h_i^{-1} g^{n_i} h_i$  and

$$g^n = g^{\sum_{i=1}^m n_i} = \prod_{i=1}^m g^{n_i} = \prod_{i=1}^m h_i^{-1} g^{n_i} h_i = \prod_{i=1}^m h_i^{-1} g^{n_i} h_i Q' = V(g). \quad \square$$

**Corollary 7.2.** *If  $[G : Q] = n$  and  $Q \leq Z(G)$  then the map  $g \mapsto g^n$  is a homomorphism from  $G$  to  $Q$ .*

*Proof.* By Theorem 7.7, we have that  $V(g) = g^n$ , so it is homomorphism.  $\square$

**Lemma 7.3.** *Let  $G$  be a finite group,  $p$  a prime,  $Q \in \text{Syl}_p(G)$ . If  $g, h \in C_G(Q)$  are conjugate in  $G$ , then they are also conjugate in  $N_G(Q)$ .*

*Proof.* Let  $g, h \in C_G(Q)$  be two elements that are conjugate in  $G$ . Then there exist an element  $x \in G$  such that  $x^{-1}gx = h$ . Since conjugation by  $x$  is an automorphism of  $G$ , we have that  $h = x^{-1}gx \in x^{-1}C_G(Q)x = C_{G^x}(Q^x) = C_G(Q^x)$ , hence  $Q^x \leq C_G(h)$ . Since  $Q, Q^x \in \text{Syl}_p(C_G(h))$ , we have that there exists an element  $c \in C_G(h)$  such that  $Q = Q^{xc}$  and so  $xc \in N_G(Q)$ . Let  $n_1 := xc$ , then  $g^{n_1} = g^{xc} = (g^x)^c = h^c = h$ .  $\square$

**Theorem 7.8. (Burnside transfer theorem)**

Let  $G$  be a finite group  $Q \in \text{Syl}_p(G)$  such that  $Q \leq Z(N_G(Q))$ . Then there is a normal  $p$ -complement in  $G$ .

*Proof.* Since  $Q$  is abelian, we have that  $Q \leq C_G(Q)$  and  $V : G \rightarrow (Q/Q' = Q)$ .

Let  $[G : Q] = n$ . If  $g \in Q$ ,  $g^{n_i} \in Q \leq C_G(Q)$ , and by Lemma 7.2 (1)  $h_i^{-1}g^{n_i}h_i \in Q \leq C_G(Q)$  also holds. By Lemma 7.3  $g^{n_i}$  and  $h_i^{-1}g^{n_i}h_i$  are conjugate in  $N_G(Q)$  i.e., there exists an element  $u \in N_G(Q)$  such that  $u^{-1}g^{n_i}u = h_i^{-1}g^{n_i}h_i$ . Since  $Q \leq Z(N_G(Q))$ , we have that  $u^{-1}g^{n_i}u = g^{n_i}$  and  $V(g) = \prod_{i=1}^m g^{n_i} = g^{\sum_{i=1}^m n_i} = g^n$ . Let  $|Q| = q$ . Then  $(q, n) = 1$ , so there exist  $\alpha, \beta \in \mathbb{Z}$  such that  $\alpha q + \beta n = 1$ . If  $g \in Q$ , then  $g = g^1 = g^{\alpha q + \beta n} = (g^\beta)^n (g^\alpha)^q = (g^\beta)^n$  hence the map  $V : Q \rightarrow Q, g \mapsto g^n$  is surjective. Thus  $V$  is bijective and so  $\ker V \cap Q = \{1\}$ .

By the Homomorphism theorem  $G/\ker V \cong \text{Im } V = Q$ . Let  $K = \ker V$ . Then  $K \cap Q = 1$ .

We will prove that  $K$  is a normal  $p$ -complement in  $G$ . Obviously  $K \triangleleft G$ .

$|KQ| = \frac{|K||Q|}{|K \cap Q|} = |K||Q| = |G|$ , hence  $KQ = G$ . Thus  $K$  is a normal  $p$ -complement in  $G$ .

$\square$

**Remark 7.4.** If  $K$  is a normal  $p$ -complement then  $K$  is characteristic in  $G$ .

*Proof.* We know that  $K \in \text{Hall}_{p'}(G)$ , Let  $\varphi \in \text{Aut}(G)$ . Then  $\varphi(K) \in \text{Hall}_{p'}(G)$  and  $\varphi(K) \triangleleft G$ . Thus we have that  $K\varphi(K)$  is a  $p'$ -group, however  $[G : K] = |Q|, Q \in \text{Syl}_p(G)$ , so  $\varphi(K) \subseteq K$ , hence  $\varphi(K) = K$ .  $\square$

## 8 Free groups, the Nielsen-Schreier theorem

Let us fix a set  $X$ . We form words from elements of  $X$  and their inverses,  $w = a_1 a_2 \cdots a_n = x_i^{\varepsilon_i}$ ,  $\varepsilon_i = \pm 1$ . We define multiplication, as concatenation of words, and cancel  $xx^{-1}$  or  $x^{-1}x$ . We call a word **reduced** if it cannot be written in a shorter form.

**Theorem 8.1.** *Every word can be simplified into a unique reduced word.  
(The proof is by induction on the length of the word).*

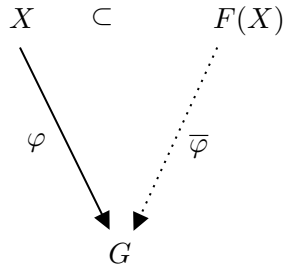
*In this way two words are equivalent if they reduce to the same word.*

**Theorem 8.2.** *The equivalence classes of words on  $X$  form a group under the above multiplication, this group is called the **free group** generated by free generations set  $X$ . We denote it  $F(X)$ . If  $|X| = n$  then we use notation  $F_n$ .*

**Theorem 8.3. (The universal property)**

*Let  $G$  be a group and let  $\varphi : X \rightarrow G$  be a map. Then  $\varphi$  can be extended in a unique way to a group homomorphism  $\tilde{\varphi} : F(X) \rightarrow G$  such that  $\tilde{\varphi}|_X = \varphi$ .*

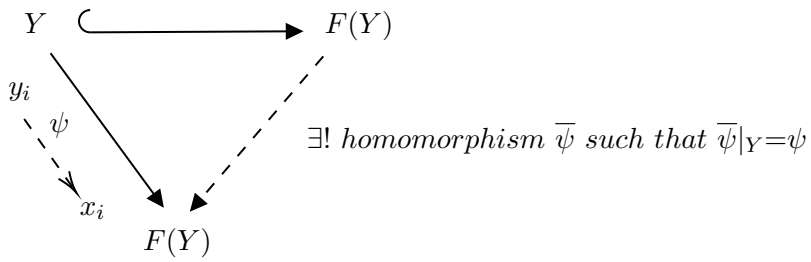
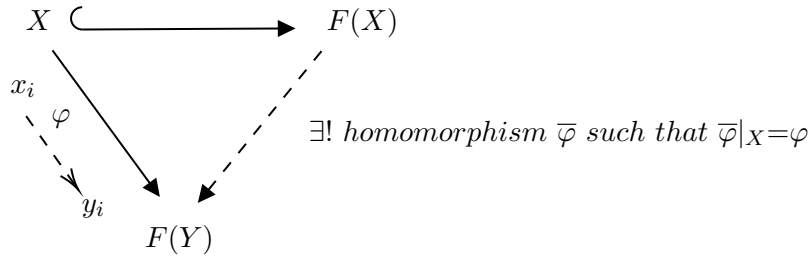
*Proof.* We define  $\tilde{\varphi}(x_1^{\varepsilon_1}, \dots, x_k^{\varepsilon_k}) := \prod_{i=1}^k \varphi(x_i)^{\varepsilon_i}$  and this a homomorphism.



□

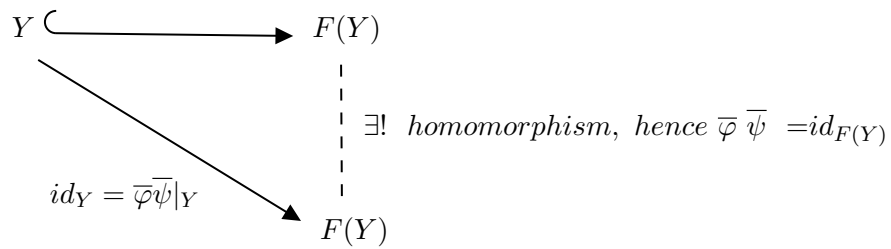
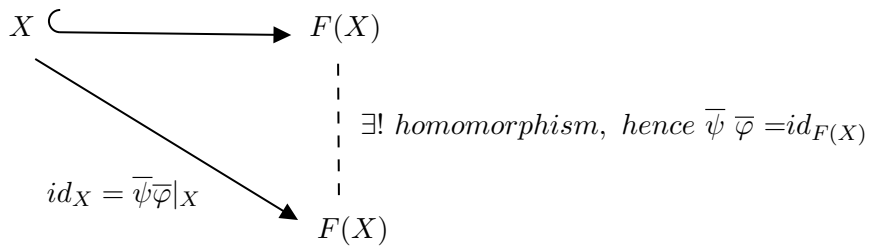
**Corollary 8.1.** *If  $|X| = |Y| \Rightarrow F(X) \cong F(Y)$ . (the converse is also true)*

Proof.



$$x_i \xrightarrow{\varphi} y_i \xrightarrow{\psi} x_i$$

$$\bar{\psi}\bar{\varphi}|_X = id_X, \varphi|_Y = id_Y.$$



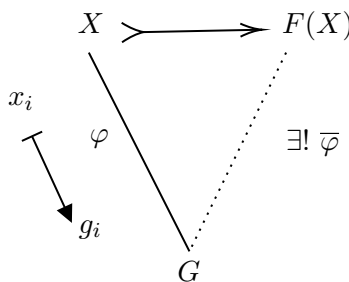
Hence  $\bar{\varphi}, \bar{\psi}$  are inverses of each other, so  $\bar{\varphi}, \bar{\psi}$  are group isomorphism, hence  $F(X) \cong F(Y)$ .

□

**Theorem 8.4.** Let  $G = \langle g_1, \dots, g_n \rangle$  be a group  $F(X)$  be the free group with free generating set  $X = \{x_1, \dots, x_n\}$ . Then  $G$  is a homomorphic image of  $F(X)$ .

*Proof.* Let  $\varphi(x_i) = g_i$ ,  $i = 1, \dots, n$ . By the universal property of  $F(X)$ , there exists a unique homomorphism  $\bar{\varphi} : F(X) \rightarrow G$  such that  $\bar{\varphi}(x_i) = g_i$ ,  $i = 1, \dots, n$  holds.

$\bar{\varphi}$  is surjective since  $\text{Im}(\bar{\varphi})$  contains a generating set of  $G$ . So by the Homomorphism theorem,  $F(X)/\ker \bar{\varphi} \cong \text{Im} \bar{\varphi} = G$ .



□

**Definition 8.5.** Let  $N := \ker \bar{\varphi}$  in the above theorem and let  $\{r_i | i \in I\}$  be the normal subgroup generators of  $N$  ( $r_i$  and their conjugates generate  $N$ ). Then the words  $r_i$  are called the **defining relations** of  $G$ .

We say that  $G = \langle x_1, \dots, x_n \mid r_1, r_2, \dots \rangle$  is given by **generators** and **relations**.

If there are finite number of generators and relations, then  $G$  is called finitely presented group.

**Theorem 8.6. (Dyck)**

Let  $R = \{r_1, r_2, \dots\}$ ,  $R' = \{r'_1, r'_2, \dots\}$ , let  $G_1 = \langle x_1, x_2, \dots \mid r_1, r_2, \dots \rangle$ ,  $G_2 = \langle x_1, x_2, \dots \mid r'_1, r'_2, \dots \rangle$  be groups are given with generators and relations. Suppose that  $R \subseteq R'$ . Then  $G_2$  is a homomorphic image of  $G_1$ .

*Proof.* Let  $N_1$  be the normal subgroup of  $F_n$  generated by normal subgroup generators  $R$ . We know that  $G_1 \cong F_n/N_1$ ,  $G_2 \cong F_n/N_2$ , and  $N_1 \leq N_2$ . By the second isomorphism theorem we have that  $N_1 \triangleleft N_2$ ,  $N_2/N_1 \triangleleft F_n/N_1$  and  $F_n/N_1 / N_2/N_1 \cong F_n/N_2 \cong G_2$ . □

**Definition 8.7.** Let  $G$  be a group, and let  $X$  be a generating set of  $G$ . Then  $\Gamma(G, X)$  is the **Cayley-graph** of  $G$  with respect to  $X$  if the vertices are  $V(\Gamma(G, X)) = G$ , the edges are  $E(\Gamma(G, X)) = \{(g, xg) \mid x \in X, g \in G\}$ . Then  $\Gamma(G, X)$  is a directed coloured graph, the edges of  $\Gamma(G, X)$  are coloured by elements of  $X$ . (In general  $X$  can also be just a subset of a generating set)

**Definition 8.8.**  $Aut_c(\Gamma(G, X))$  is the group of colour preserving automorphisms of the graph  $\Gamma(G, X)$ . This is a permutation on the vertices and each edge is mapped to an edge, a non-edge is mapped to non-edge and the colour of the edge is preserved.

**Remark 8.1.** In  $\Gamma(G, X)$  From each vertex for every  $x \in X$  there exists a unique in-edge  $(x^{-1}g, g)$  with colour  $x$  and a unique out-edge  $g, xg$  with colour  $x$ .

**Lemma 8.1.** If  $X \subseteq G$ , then  $\Gamma(G, X)$  is connected if and only if  $X$  is a generating set of  $G$ .

*Proof.*  $\Leftarrow$ ) Let  $g_1, g_2 \in G$ . Then  $g := g_2 g_1^{-1} = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} \cdots x_{i_r}^{\epsilon_r}$  where  $x_{ij} \in X$  and  $\epsilon_i = \pm 1$ . Then since  $g_2 = (g_2 g_1^{-1}) g_1 = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} \cdots x_{i_r}^{\epsilon_r} g_1$ , there is a path

$$g_1 \xrightarrow{x_{i_r}^{\epsilon_r}} x_{i_r}^{\epsilon_r} g_1 \xrightarrow{x_{i_{r-1}}^{\epsilon_{r-1}}} x_{i_{r-1}}^{\epsilon_{r-1}} x_{i_r}^{\epsilon_r} g_1 \xrightarrow{x_{i_{r-2}}^{\epsilon_{r-2}}} \cdots \xrightarrow{x_{i_1}^{\epsilon_1}} x_{i_1}^{\epsilon_1} \cdots x_{i_r}^{\epsilon_r} g_1 = g_2$$

from  $g_1$  to  $g_2$ , hence  $\Gamma(G, X)$  is connected.

$\Rightarrow$ ) Suppose that  $\Gamma(G, X)$  is connected. Then we can reach each element  $g \in G$  with a path from  $e$ . If on the edge we go in reverse direction then the label in the inverse of the generator.

$$e \xrightarrow{x_1^{\epsilon_1}} x_1^{\epsilon_1} \xrightarrow{x_2^{\epsilon_2}} x_2^{\epsilon_2} x_1^{\epsilon_1} \xrightarrow{\cdots} \cdots \xrightarrow{x_n^{\epsilon_n}} x_n^{\epsilon_n} \cdots x_1^{\epsilon_1} = g$$

thus the product on the edges gives  $g$ . Hence generates  $G$ . □

**Theorem 8.9.**  $Aut_c(\Gamma(G, X)) \cong G$ .



*Proof.* Let  $g \in G$ . Then  $g$  acts on the vertices of the graph by right multiplication  $\varphi_g : u \mapsto ug$ . Observe that this is a permutation.

If  $(h, xh)$  is an edge, then  $(hg, xhg)$  is also an edge, so  $\varphi_g$  preserves edges. If there is no edge between  $h$  and  $k$ , then  $(hg, kg)$  cannot be an edge, since  $\varphi_{g^{-1}}$  also preserves edges. Hence we can define a map  $\Phi : G \rightarrow \text{Aut}_c(\Gamma(G, X))$  by  $\Phi : g \mapsto \varphi_g$ . This map is injective.  $\Phi$  is a group homomorphism, since for every  $h \in G$ , we have that  $h\varphi_{g_1g_2} = h(g_1g_2) = (hg_1)g_2 = (h\varphi_{g_1})\varphi_{g_2}$ , hence  $\varphi_{g_1g_2} = \varphi_{g_1}\varphi_{g_2}$ .

We want to prove that  $\Phi$  is surjective.

Note: if  $\alpha \in \text{Aut}_c(\Gamma(G, X))$  fixes a vertex then it also fixes its neighbours, since to  $g$  there is a unique in-edge with colour  $x$  and a unique out-edge with colour  $x$ .

Since  $\Gamma$  is connected, we have that  $\alpha = id$ .

$$x^{-1}g \xrightarrow{x} g \xrightarrow{x} xg$$

Suppose that  $\varphi \in \text{Aut}_c(\Gamma(G, X))$ . If  $g = 1\varphi$  then  $1 = (1\varphi)\varphi_{g^{-1}}$ .

So 1 is a fixed point of  $\varphi\varphi_{g^{-1}}$ . Hence  $\varphi\varphi_{g^{-1}} = id$  and  $\varphi = \varphi_g$ . Thus  $\Phi$  is surjective and  $\Phi$  is an isomorphism.  $\square$

**Lemma 8.2.**  $G$  is freely generated by  $X \subseteq G$  if and only if  $\Gamma(G, X)$  is a tree.

*Proof.* We have seen that  $X$  is a generating set if and only if  $\Gamma(G, X)$  is connected.

If  $X$  is not a free generating set of  $G$  then there exists a nontrivial relation  $x_{i_1}^{\epsilon_1} \cdots x_{i_n}^{\epsilon_n} = 1$ , where  $x_{ij} \in X$  and  $\epsilon_i = \pm 1$ . Then

$$1 \xrightarrow{x_{i_n}^{\epsilon_n}} x_{i_n}^{\epsilon_n} \xrightarrow{x_{i_{n-1}}^{\epsilon_{n-1}}} x_{i_{n-1}}^{\epsilon_{n-1}} x_{i_n}^{\epsilon_n} \xrightarrow{\cdots} \cdots \xrightarrow{x_{i_1}^{\epsilon_1}} x_{i_1}^{\epsilon_1} \cdots x_{i_n}^{\epsilon_n} = 1$$

gives a circle in the graph of length  $\geq 3$ , since  $x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} = 1$  would imply that  $x_{i_1}^{\epsilon_1}$  and  $x_{i_2}^{\epsilon_2}$  are inverses of each other, and this is a trivial relation.

Conversely if we have a circle in  $\Gamma$  then the product of labels gives a nontrivial relation.  $\square$

### Zorn's lemma

Let  $P$  is a partial ordered set  $(P, \leq)$ . Suppose that every ordered subset of  $P$  has an upper bound. Then there is a maximal element in  $P$ .

### Theorem 8.10. (Nielsen-Schreier)

*Every non-trivial subgroup of a free group is free.*

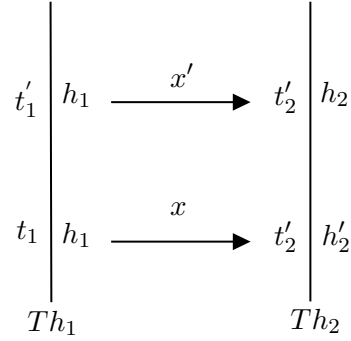
*Proof.* Let  $G = F(X)$ , and let  $\{1\} \neq H \leq G$ . We want to prove that  $H$  is free. By Lemma 8.2 we have that  $\Gamma(G, X)$  is a tree.

We have to prove there exists a generating set  $Y$  of  $H$  such that  $\Gamma(H, Y)$  is a tree. Let us define the set  $S := \{\Gamma' \leq \Gamma \mid \Gamma' \text{ is a spanning subgraph of } \Gamma \text{ (an edge in } \Gamma \text{ is in } \Gamma' \text{ if the end points are in the set } \Gamma') \text{ and } \Gamma' \text{ connected, } \Gamma' \text{ contains from each left coset of } H \text{ at most one element}\}$ .

We apply for the set  $S$  Zorn's lemma. The conditions of Zorn's lemma are satisfied: if  $\Gamma_1 \leq \Gamma_2 \leq \dots$  is a chain in  $S$ , then  $\bigcup \Gamma_i \in S$ . Then by Zorn's lemma there is a maximal element  $T$  in  $S$ . We want to prove that  $T$  contains from each left coset of  $H$  exactly one element. Suppose by contradiction that  $g_1H \cap T = \emptyset$  for some  $g_1 \in G$ . Since  $\Gamma(G, X)$  is connected,  $g_1$  is reachable by a path from an element of  $T$ . So there exists an element  $g$  such that  $(g, xg) \in E(\Gamma(G, X))$   $gH \cap T \neq \emptyset$ ,  $xgH \cap T = \emptyset$ . So there exists an element  $h \in H$  such that  $gh \in T$ ,  $xgh \notin T$ , and  $(gh, xgh) \in E(\Gamma(G, X))$ . Thus  $T \cup \{xgh\}$  is a bigger spanning subgraph in  $\Gamma(G, X)$ , which is connected and contains from each coset of  $H$  at most one element. This is a contradiction, since  $T$  as maximal. Hence  $T$  contains from each left coset exactly one element, so  $T$  is a left transversal of  $H$  in  $G$ . We suppose that  $1 \in T$ , since there exists an element  $h \in H \cap T$ . Thus  $1 \in Th^{-1} \cong T$  (this is an isomorphism of graphs), and  $Th^{-1}$  left transversal of  $H$  in  $G$ .

Let  $\mathcal{T} = \{Th \mid h \in H\}$ . We want to prove that  $\mathcal{T}$  is a set of disjoint left transversals of  $H$  in  $G$ . If  $Th_1 \cap Th_2 \neq \emptyset$  then there exist elements  $t_1, t_2 \in T$  and  $h_1, h_2 \in H$  such that  $t_1h_1 = t_2h_2$ . Then  $t_1H = t_2H$  and so  $t_1, t_2 \in T$  are in the same coset of  $H$ . Hence  $t_1 = t_2$ , since  $T$  was a left transversal, so  $h_1 = h_2$ . Thus, if we map  $h$  to  $Th$ , then we get a bijection between  $H$  and  $\mathcal{T}$ . On  $\mathcal{T}$  we define a directed  $H$ -coloured graph. The vertices of this graph will be  $\{Th \mid h \in H\}$ . Now we define when the transversals  $Th_1$  and  $Th_2$  are connected

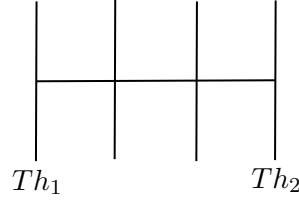
with an edge coloured by  $x$ . Let  $h_1 \neq h_2$ , and  $t_1h_1 \in Th_1, t_2h_2 \in Th_2$ . If there exists an element  $x \in G$  such that  $x(t_1h_1) = t_2h_2$ , then  $t_1h_1 \xrightarrow{x} t_2h_2$  is an edge in  $\Gamma(G, X)$ . Then  $t_2^{-1}xt_1h_1 = h_2$  and  $h_2^{-1}xt_1 = h_2h_1^{-1} \in H$ . Let  $(Th_1, Th_2)$  be an edge coloured by  $h_2h_1^{-1}$ . Observe that there is at most one element  $x \in Y$  such that an edge coloured by  $x$  connect elements of  $Th_1$  with elements  $Th_2$ . Suppose that  $x'(t'_1h_1) = t'_2h_2$  and  $x(t_1h_1) = t_2h_2$ . Since  $Th_1$  and  $Th_2$  are connected,



we get a circle in the original graph, and this is a contradiction, since  $\Gamma(G, X)$  was a tree. We repeat this for all possible  $Th_i, Th_j$  then we define  $Y$  as the set of possible colours in  $\mathcal{T}$ .

We want to prove that  $Y$  is a free generating set of  $H$  and  $\Gamma(H, Y) \cong \mathcal{T}$ . Let  $\phi$  be the map  $h \mapsto Th$ . This is a bijection between  $H$  and  $\mathcal{T}$ . If  $(h, yh) \in E(\Gamma(H, Y))$  then  $y = h_2h_1^{-1}$  where  $xt_1h_1 = t_2h_2$  for some  $t_1, t_2 \in T$ . Then  $t_2^{-1}xt_1 = h_2h_1^{-1}$ . and  $x(t_1h) = t_2(h_2h_1^{-1}h) \in Th_2h_1^{-1}h$ , so from  $Th$  to  $Th_2h_1^{-1}h$  there is an edge of colour  $y_i$ . So the map  $h \mapsto Th$  preserve coloured edges.

If there is no edge  $y \in Y$  between  $h$  and  $h'$  then there cannot be an edge  $y \in Y$  between  $Th$  and  $Th'$ , since then  $y = h'h^{-1}$  and this takes  $h$  to  $h'$ , which is a contradiction.  $\Gamma(H, Y)$  is connected, since  $\Gamma(G, X)$  is connected, and there is a path between certain points of  $Th_1$  and  $Th_2$ .



$\mathcal{T}$  is a tree, otherwise would be a circle also in  $\Gamma(G, X)$  and this is a contradiction. Since  $\mathcal{T} \cong \Gamma(H, Y)$ ,  $H$  is a free group with free generators  $Y$ .

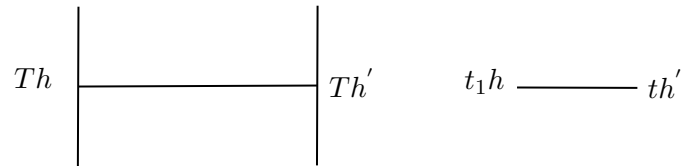
□

**Remark 8.2.** If  $[F_n : H] = m$  then  $H \cong F_{m(n-1)+1}$ .

*Proof.* In the previous proof we have seen that  $\Gamma_c(H, Y) \cong \mathcal{T}$ , where  $h \mapsto Th$  gives the isomorphism.  $T$  is also a tree, since it is connected and without any circles, as  $\Gamma_c(G, X)$  had no circles. The vertices of  $\mathcal{T}$  are  $Th$ , where  $h \in H$ , these are disjoint. There was an edge between  $Th_1$  and  $Th_2$  iff there exist elements  $t_1, t_2 \in T$  and  $x \in X$  such that  $t_1 h_1 \xrightarrow{x} t_2 h_2$ .

We have seen that between  $Th_1$  and  $Th_2$  there is at most one edge, and its colour is  $h_2 h_1^{-1}$ . In the isomorphism between  $\Gamma_c(H, Y)$  and  $\mathcal{T}$ ,  $Y$  maps to the edges of  $\mathcal{T}$ . We have seen that  $\Gamma_c(H, Y)$  is also a tree. ( $H$  is a free group with free generators  $Y$ ). We want to determine  $|Y|$ .

We have to calculate how many edges go from  $Th$  to  $Th'$ : this is exactly  $m \cdot n$ , since we can choose  $x$  in  $n$  different ways and  $t_1$  in  $m$  different ways.



But edges that go from  $Th$  to  $Th$  are not good, so we have to subtract the number of edges in the tree  $Th$ . This is exactly  $|Th| - 1 = m - 1$ .

So  $|Y| = m \cdot n - (m - 1) = m(n - 1) + 1$ . □

## 9 Problem sheets

### Problem sheet 1.

1. Prove that two elements of  $S_n$  are conjugate if and only if writing them as products of disjoint cycles, in both decompositions the lengths of cycles  $(c_1, \dots, c_t)$  are the same up to the order of the cycles. How can one conjugate two permutations with the same cycle structure into each other?
2. Show that the centre  $Z(S_n)$  of the symmetric group contains only the unit element if  $n \geq 3$ . Moreover,  $Z(A_n) = 1$  and  $C_{S_n}(A_n) = 1$ , if  $n \geq 4$ .
3. Determine the conjugacy classes of  $A_n$ . Prove that if  $\sigma \in A_n$  then there are two cases:  
(a) If the centralizer  $C_{S_n}(\sigma)$  contains an odd permutation, then the conjugacy classes of  $\sigma$  in  $A_n$  and  $S_n$  are the same:  $K_{A_n}(\sigma) = K_{S_n}(\sigma)$ . (b) If  $C_{S_n}(\sigma)$  contains only even permutations then  $K_{S_n}(\sigma)$  splits into two conjugacy classes of  $A_n$  of equal size.
4. Show that  $A_n$  is simple if  $n \geq 5$  with the following steps:
  - a) Let us suppose by contradiction that there is a normal subgroup  $1 < N < A_n$ . Let  $\sigma \in N$  be a nontrivial element with maximal possible number of fixed points. Prove that we may suppose that  $\sigma$  is of prime order.
  - b) Prove that in the decomposition of  $\sigma$  into the product of disjoint cycles every cycle length is either  $p$  or 1.
  - c) Prove that  $A_n$  is generated by the 3-cycles of  $S_n$  if  $n \geq 3$ .
  - d) Prove that if  $p = 3$  and  $\sigma$  is one 3-cycle, then  $N$  contains all 3-cycles of  $S_n$ , hence  $N = A_n$ .
  - e) Prove that if  $p = 3$  and  $\sigma$  is the product of at least two 3-cycles, say  $(1, 2, 3)(4, 5, 6) \cdots$ , or  $p \geq 5$  and  $\sigma = (1, 2, \dots, p) \cdots$  then if  $\tau = (3, 4, 5) \in A_n$ , we form the element  $\sigma\tau\sigma^{-1}\tau^{-1}$ . This also belongs to  $N$ , it is not 1, it fixes all the fixed points of  $\sigma$ , moreover it also fixes 1, contradicting that  $\sigma$  has the maximal number of fixed points among nontrivial elements of  $N$ .

f) If  $p = 2$ , then  $\sigma$  is the product of at least 2 transpositions, e.g.  $(1, 2)(3, 4) \cdots$ . Then  $\sigma(1, 2, 3)\sigma^{-1}(3, 2, 1) = (1, 4)(2, 3)$  and this belongs to  $N$ .

g)  $(1, 4)(2, 3)$  can be conjugated to any double transpositions by an element of  $A_n$ , hence  $N = A_n$ , which is a contradiction.

5.(a) Prove that if  $x$  is an element of a group  $G$  and  $x^N = 1$ , then its order  $o(x)$  divides  $N$ .

(b) Prove that if  $G_1, G_2$  are groups and  $\phi : G_1 \rightarrow G_2$  is a multiplicative map ( $\phi(ab) = \phi(a)\phi(b)$ ), then  $\phi(1_{G_1}) = 1_{G_2}$  and for every  $x \in G_1$   $\phi(x^{-1}) = \phi(x)^{-1}$ .

6. Prove that if  $n \geq 5$  and  $|S_n : H| < n$  for a subgroup  $H \leq S_n$ , then either  $H = A_n$  or  $H = S_n$ .

7. Prove that if  $n \geq 5$ , then  $S_n$  has only the following normal subgroups:  $S_n, A_n, \{1\}$ .

8. Prove that if  $\alpha \in S_n$  and its decomposition into disjoint cycles there are  $n_i$  cycles of length  $i$ , then  $|C_{S_n}(\alpha)| = \prod i^{n_i} n_i!$ .

### Problem sheet 2.

1. Prove that if  $H$  is a subgroup of the group  $G$ , then  $\bigcap_{x \in G} H^x$  is a normal subgroup in  $G$ , it lies inside  $H$  and contains each normal subgroup of  $G$  which lies in  $H$ .

2. Let  $\Gamma$  be a graph, the vertices of  $\Gamma$  are the transpositions of  $S_n$ . Two vertices are connected with an edge if and only if the two transpositions have a common moved point. Prove that if  $n \geq 5$ , then every  $n - 1$  point complete subgraph of  $\Gamma$  is of the form  $\mathcal{G}_a := \{(a, x) \mid x \in \{1, 2, \dots, n\} \setminus \{a\}\}$ , in other words the vertices of this subgraph are all transpositions with exactly 1 common moved point  $a$ .

3. Prove that if  $G$  is a finite group acting on the finite set  $\Omega$ , then

a) the number of  $G$ -orbits is  $\frac{1}{|G|} \sum_{\pi \in G} |Fix(\pi)|$ , where  $|Fix(\pi)|$  is the number of fixed

points of the element  $\pi$ . ( Cauchy-Frobenius-Burnside lemma) b) Deduce from (a) that if the action is transitive on  $\Omega$ , then for every  $\alpha, \beta \in \Omega$  the number of orbits of  $G_\alpha$  és  $G_\beta$  is the same.

4. Prove that the group  $GL(V)$  of **invertible linear transformations** of a vector space  $V$  is not transitive on the vectors of  $V$ , however, it is transitive on the nonzero vectors of  $V$ .

5. Prove that if the group  $G$  is acting on the set  $\Omega$ , then  $G_\alpha g = \{h \in G \mid \alpha^h = \alpha^g\}$ .

6. Prove that every faithful, transitive action of  $G$  on  $\Omega$  is equivalent to an action on the right cosets of a subgroup  $H$  with the property that  $H$  does not contain any proper normal subgroups of  $G$ .

7. a) Prove that every nontrivial group of prime power order has nontrivial centre.

b) Prove that every nontrivial normal subgroup of a group of prime power order intersects nontrivially the centre of the group.

8.a) Prove that if  $G/Z(G)$  is cyclic, then  $G$  is abelian.

b) Prove that every index 2 subgroup is normal.

c) Prove that every group of prime order is cyclic.

d) Prove that every group of primesquare order is abelian.

e) Prove that the direct product of two cyclic groups of coprime order is cyclic.

9. Let  $G$  be a nonabelian group of order 8. Prove that  $G \simeq D_8$  or  $G \simeq Q_8$ .

a) Prove that  $G$  has an element  $g$  of order 4.

b) Prove that for every  $h \in G \setminus \langle g \rangle$   $h^{-1}gh = g^{-1}$  holds.

c) If there exist an element  $h \in G \setminus \langle g \rangle$  of order 2 show that  $G \simeq D_8$ .

d) If every element  $h \in G \setminus \langle g \rangle$  is of order 4, then show that  $h^2 \in \langle g \rangle$ ,  $h^2 = g^2$  and  $G$  satisfies the defining relations of  $Q_8 = \langle a, b, a^4 = 1, b^4 = 1, a^2 = b^2, a^b = a^{-1} \rangle$  and  $G \simeq Q_8$ .

10. Prove that if  $n \geq 5$  and  $|S_n : H| < n$  for a subgroup  $H \leq S_n$ , then either  $H = A_n$  or  $H = S_n$ .

### Problem sheet 3

1. Prove that in the alternating group  $G = A_5$  there is no element of order 15 and no subgroup of order 15, however,  $|G|$  is divisible by 15.

2. Prove that if the order of the group  $G$  is bigger than  $n!$  and  $H < G$  is a subgroup with  $|G : H| < n$ , then  $G$  cannot be a simple group. (Hint: Represent  $G$  on the right cosets of  $H$  with right multiplication)

3. Prove that if the group element  $a$  has order  $n$ , then its  $k^{\text{th}}$  power has order  $o(a^k) = \frac{n}{\gcd(n,k)}$ .

4. Prove that nonabelian groups of order 12 have three isomophy types:  $D_{12}$ ,  $A_4$  and the split extension of  $C_3$  by  $C_4$ :

a) Let  $P \in \text{Syl}_3(G)$ , represent  $G$  on the right cosets of  $P$ . Show that if this representation is faithful, then  $G \simeq A_4$ !

b) Show that if this representation is not faithful, then its kernel is  $P \in \text{Syl}_3(G)$ , in other words:  $P \triangleleft G$ .

c) Let  $b$  be a generator of the cyclic group  $P$ . Prove that  $|K_G(b)| \leq 2$ , and  $|C_G(b)| \in \{6, 12\}$ !

d) Show that if  $P \in \text{Syl}_3(G)$  is a normal subgroup, then  $G$  has elements of order 6.

e) Show that the Sylow 2-subgroup  $S$  of  $G$  is either  $C_4$ , or  $C_2 \times C_2$ .

f) Prove that if  $P \in \text{Syl}_3(P)$  is normal, then  $G = PS$ ,  $P \cap S = 1$ .

g) Show that this product is isomorphic to  $D_{12}$  if  $S \simeq C_2 \times C_2$ !

5. Prove that if  $G$  is a simple group of order 60, then  $G \simeq A_5$ :

a) If  $G$  contains a subgroup of index 5, then show that  $G \simeq A_5$ .



- b) Suppose that  $G$  does not contain a subgroup of index 5!
- b/1 Show that each subgroup has index bigger than 5.
- b/2 Determine the number of Sylow 2, 3 and 5-subgroups of  $G$ .
- b/3 Prove that if the intersection  $D$  of two Sylow 2-subgroups  $P_1, P_2$  of  $G$  would not be trivial, then  $D$  would be a normal subgroup in the subgroup  $T = \langle P_1, P_2 \rangle$ . Prove that in this case  $T < G$  and  $T$  would contain at least 3 Sylow 2-subgroups of  $G$ , hence  $|T| \geq 12$ , which contradicts b/1.
- b/4 Calculate the number of elements in Sylow 2, 3 and 5-subgroups, show that this is bigger than 60, which is a contradiction.

6. Prove that **the affine linear transformations of a vector space**  $V$   $AGL(V) := \{\underline{v} \mapsto A\underline{v} + \underline{b} \mid A \in GL(V), \underline{b} \in V\}$  is a doubly transitive group on the vectors of  $V$ .

A group action  $G$  on  $\Omega$  is called **regular** or **sharply 1-transitive** if it is transitive, and for every  $\alpha, \beta \in \Omega$  a **unique**  $g \in G$  exists, such that  $\alpha^g = \beta$ .

7. a) Prove that the Cayley-representation is regular, however the generalized Cayley representation is not.
- b) Show that in the case of a regular group action the point stabilizer is trivial and  $|G| = |\Omega|$ .

#### Problem sheet 4

- Determine all the primitive actions of  $S_3$ . Which of them are faithful? Which of them are equivalent? (Use the statement of Exercise 6.)
- We say that the group  $G$  acts on the set  $\Omega$  **sharply  $k$ -transitively**, if for every distinct points  $\alpha_1, \dots, \alpha_k \in \Omega$  and for every distinct points  $\beta_1, \dots, \beta_k$  there exists a **unique**  $g \in G$  such that  $\alpha_i^g = \beta_i$   $i = 1, \dots, k$ . Prove that  $S_n$  is sharply  $n$ -transitive and sharply  $n - 1$ -transitive and  $A_n$  is sharply  $n - 2$ -transitive.

3. Prove that the following are equivalent for  $k \geq 2$ :
- (i) The group  $G$  acts on  $\Omega$  sharply  $k$ -transitively.
  - (ii)  $G$  acts  $k$ -transitively and  $G_{\alpha_1, \dots, \alpha_k} = \{1\}$ , for every distinct  $\alpha_1, \dots, \alpha_k \in \Omega$ .
  - (iii)  $G$  is transitive on  $\Omega$  and  $G_\alpha$  is sharply  $(k - 1)$ -transitive on  $\Omega \setminus \{\alpha\}$ .
4. Prove that  $AGL(K) = \{x \mapsto ax + b \mid a, b \in K, a \neq 0\}$  is sharply 2-transitive on the field  $K$ .
- 5.a) Prove that every transitive permutation group on  $p$  points ( $p$  prime) is primitive.
- b) Prove that if a group is 2-transitive on a set  $\Omega$  that contains at least 3 points, then the action is primitive.
6. Prove that every primitive group action is equivalent to an action on the right cosets of a maximal subgroup with right multiplication. When is it faithful?
7. Prove that if  $G$  is  $k$ -transitive on a set  $\Omega$  of  $n$  points, then  $|G| = n(n - 1) \dots (n - k + 1)|G_{\alpha_1, \dots, \alpha_k}|$ , for every  $\alpha_1, \dots, \alpha_k$  distinct points. What will be the group order if the action is sharply  $k$ -transitive?
8. Prove that every nontrivial normal subgroup of every primitive permutation group  $G \leq S_\Omega$  is transitive on  $\Omega$ .
9. Show an example that a nontrivial normal subgroup of a transitive permutation group is not necessarily transitive on  $\Omega$ . (Consider  $GL(V)$  on  $V \setminus \{0\}$  and look at the scalar matrices)
10. Let  $N \triangleleft G$ .  $G$  acts on  $N \setminus \{1\}$  by conjugation.
- a) Prove that if this action is transitive, then  $N$  is an elementary abelian  $p$ -group, for  $p$  prime.
  - b) If this action is 2-transitive, then  $p = 2$  or  $|N| = 3$ .
  - c) If the action is 3-transitive, then  $|N| = 4$ .

c) This action is never 4-transitive.

11. Suppose that  $G$  acts on  $\Omega$  and  $N \triangleleft G$  acts regularly (sharply 1-transitively) on  $\Omega$ . Prove that the action of  $G_\omega$  on  $\Omega \setminus \{\omega\}$  is equivalent to the action of  $G_\omega$  on  $N \setminus \{1\}$  by conjugation.

12. Prove that if  $G$  is a transitive permutation group on a set  $\Omega$  with  $n$  points and  $G$  is abelian, then the action is regular (sharply 1-transitive on  $\Omega$ ).

### Problem sheet 5

1. Prove that the Sylow  $p$ -subgroup of  $S_m$  is isomorphic to  $\oplus_{i=0}^t X_i^{a_i}$ , where  $X_i$  is the  $i$  times iterated wreath product of  $C_p$  and  $m = \sum_{i=0}^t a_i p^i$ , where  $a_i \in \{0, 1, \dots, p-1\}$ .

2. Let  $Q, K$  be groups and  $\theta : Q \rightarrow \text{Aut}(K)$  be a homomorphism. Let us define on the direct product set  $K \times Q$  the following multiplication:  $(k_1, q_1)(k_2, q_2) := (k_1 k_2^{k_1 \theta(q_1)}, q_1 q_2)$ .

a) Prove that this is associative!

b) Determine the unit element and determine the inverse of each element.

c) Prove that the group constructed this way is a split extension of  $(K, 1) \simeq K$  by  $(1, Q) \simeq Q$ .

d) Calculate the product:  $(1, q)(k, 1)(1, q)^{-1}$ .

3. Let  $A$  be a nontrivial  $p$ -group and let  $K$  be an infinite  $p$ -group. Consider both of them as permutation groups on themselves by right multiplication. Consider the wreath product  $A \wr K$ . Prove that this a  $p$ -group whose centre is trivial.

4. Prove that the derived subgroup of the wreath product  $G \wr C_p$  consists of elements  $(g_1, \dots, g_p, 1)$  where  $g_1, \dots, g_p \in G$  and  $g_1 \cdots g_p \in G'$ .

5. Let  $G$  be a cyclic group of order 4 with cyclic generator  $a$ . Prove that to the normal subgroup  $\langle a^2 \rangle$  there is no complement in  $G$ .

6. Prove that the group of automorphisms of Klein four group is isomorphic to  $S_3$ !
7. Prove that the group of automorphisms of the elementary abelian group of order  $p^n$  is  $GL(n, p)$ !
8. Prove that the group of automorphisms of  $C_n$  is the unit group of the ring  $\mathbb{Z} \bmod n$  hence it is abelian of order  $\phi(n)$ , if  $p$  is a prime, then  $Aut(C_p) \simeq C_{p-1}$ .
9. Prove that the group of automorphisms of the 3 level binary tree is  $C_2 \wr C_2$ .
10. Prove that if  $G = G_1 \times \dots \times G_n$  and  $(|G_i|, |G_j|) = 1$ , then  $Aut(G) = Aut(G_1) \times \dots \times Aut(G_n)$ .
11. Determine, how many non-isomorphic split extensions of  $C_5$  by  $C_4$  can one construct?
12. Prove that  $Aut(C_{p^n}) \simeq C_{(p-1)p^{n-1}}$ , if  $p > 2$  is a prime, and  $Aut(C_{p^n}) \simeq C_{2^{n-2}} \times C_2$ , if  $p = 2$  and  $n \geq 2$ .
13. Prove that if  $A, B \leq G$  are subgroups, then  $|AB| = |A||B|/|A \cap B|$ .

### Problem sheet 6

1. A subgroup  $H \leq G$  is called **characteristic** in  $G$  (denoted by:  $HcharG$ ), if for all  $\phi \in Aut(G)$ ,  $\phi(H) = H$ . Prove that if  $HcharK$  and  $KcharG$ , then  $HcharG$ .
2. Prove that:
  - a)  $[xy, z] = [x, z]^y[y, z]$ ,
  - b)  $[x, yz] = [x, z][x, y]^z$ .
  - c)  $[x, y^{-1}] = ([x, y]^{y^{-1}})^{-1}$ ,

d)  $[x^{-1}, y] = ([x, y]^{x^{-1}})^{-1}$

e)  $[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = 1$  (Witt-identity)

Here  $[x, y, z] := [[x, y], z]$

3. Prove that the centre  $Z(G)$  of a group  $G$  and in general  $Z^i(G)$ , are characteristic subgroups in  $G$ .

4.a) Prove that every finite  $p$ -group is solvable.

b) Prove that every group of order  $pq$  is solvable ( $p, q$  primes).

c) Prove that all groups of orders  $1 - 15$  are solvable.

5. Prove that if  $G$  is a finite solvable group,  $N$  a minimal normal subgroup in  $G$ , then the elements of  $G$  induce linear transformations on  $N$ , as on a vector space over a field of  $p$  elements.

6.(Frattini-argument) Prove that if  $H \triangleleft G$  and  $P \in \text{Syl}_p(H)$ , then  $G = HN_G(P)$ .

7. Prove that if  $P \in \text{Syl}_p(G)$  and  $N_G(P) \leq H \leq G$ , then  $N_G(H) = H$ .

8. Prove that a maximal subgroup is not necessarily of prime index.

9.a) Let  $H, K, L$  be subgroups in  $G$ . Let  $[H, K, L] := \langle [h, k, l] \mid h \in H, k \in K, l \in L \rangle$ . Prove that if  $[H, K, L] = 1 = [K, L, H]$ , then  $[L, H, K] = 1$ .

b) Let  $N$  be a normal subgroup in  $G$ . Prove that if  $[H, K, L] \leq N$  and  $[K, L, H] \leq N$ , then  $[L, H, K] \leq N$  (Three subgroup lemma)

10. Prove that if  $G = G'$ , then the centre of  $G/Z(G)$  is trivial.

11. Prove that if  $H \triangleleft G$  and  $H \cap G' = 1$ , then  $H \leq Z(G)$ .

12. Let  $[H, K] := \langle [h, k] \mid h \in H, k \in K \rangle$ .

a) Prove that  $[H, K] \leq H \leftrightarrow K \leq N_G(H)$ .

b) Prove that  $H/N \leq Z(G/N) \leftrightarrow [H, G] \leq N$ .

13. Prove that every characteristically simple group (i.e. subgroup without proper characteristic subgroups) is a direct product of isomorphic simple groups.

### Problem sheet 7

1. Let  $K_0(G) := G$ ,  $K_1(G) = G'$ ,  $K_{i+1}(G) := [K_i(G), G]$  (this is the **lower central series** of  $G$ ). Prove that  $K_i(G) \text{ char } G$  for all  $i$ .

A group  $G$  is **nilpotent**, if  $K_i(G) = 1$  for suitable  $i$ . The smallest such  $i$  is the **nilpotence class** of  $G$ , denoted by  $c = cl(G)$ . This holds if and only if  $Z^c(G) = G$ . (Proved on the lecture)

2. Prove that the nilpotency class of every non-abelian group of order  $p^3$  is 2.

3. Prove that every nilpotent group is solvable, but not conversely.

4. Characterize nilpotent group of class 1 and 2.

5. Prove that  $[xy, z] = [x, z][y, z]$  and  $[x, yz] = [x, z][x, y]$  hold in groups of nilpotence class 2.

6.a) Prove that  $[K_i(G), K_j(G)] \leq K_{i+j}(G)$ .

b) Prove that  $G^{(i)} \leq K_{2^i}(G)$ , in other words if the nilpotence class of  $G$  is at most  $2^i$ , then the derived length of  $G$  is at most  $i$ .

7. Prove that  $D_{2^n}$  is nilpotent if and only if  $n$  is a 2-power.

8. Let  $G$  be a finite nilpotent group,  $|G| = n$ . Prove that for every  $m|n$  there exists a subgroup in  $G$  of order  $m$ .
9. Prove that if  $H, K$  are nilpotent normal subgroups in  $G$ , then  $HK$  is also a nilpotent normal subgroup. Prove that in a finite group  $G$  there exists always a biggest nilpotent normal subgroup and this is a characteristic subgroup. (its name is **Fitting subgroup**, denoted by  $F(G)$ ).
10. Let  $G$  be a finite  $p$ -group,  $N \triangleleft G$ ,  $|N| = p^i$ . Prove that there exists a chain of normal subgroups of  $G$ :  $N_0 = 1 < N_1 < \dots < N_i = N < \dots < N_k = G$ , where  $|N_i : N_{i-1}| = p$ .
11. Prove that every finite  $p$ -group is nilpotent but this is not necessarily true for infinite  $p$ -groups.
12. Prove that in every finite nilpotent group every nontrivial normal subgroup contains a nontrivial element of the centre.

### Problem sheet 8

The **Frattini-subgroup**  $\Phi(G)$  of a group  $G$  is the intersection of maximal subgroups of  $G$ . If there is no maximal subgroup in  $G$ , then  $\Phi(G) = G$ .

1. Prove that  $\Phi(G) \text{ char } G$ .
2. Let  $G$  be a finite  $p$ -group. Prove that  $G^{p^i} := \langle x^{p^i} \mid x \in G \rangle$  is a characteristic subgroup in  $G$ .
3. Prove that in  $(Q, +)$  there is no maximal subgroup.

An element  $x \in G$  is a **non-generator**, if it can be left out from every generating set of  $G$ .

4. Prove that if  $G$  is a finite group, then  $\Phi(G)$  is exactly the set of non-generators in  $G$ .
5. Prove that in every finite group  $G$ ,  $\Phi(G)$  is nilpotent.
- 6.a) Prove that in every finite  $p$ -group  $G$ ,  $\Phi(G) = G'G^p$ . b) Prove that in every finite  $p$ -group  $G$   $G/\Phi(G)$  is a vector space over  $GF(p)$ . c) Let  $G$  be a finite  $p$ -group. Prove that

$\Phi(G)$  is the minimal normal subgroup in  $G$ , the factor group by which is an elementary abelian  $p$ -group.

7. A generating set is **minimal**, if every proper subset does not generate the group. Show that a minimal generating set need not be a generating set of minimal size. (Consider:  $C_2 \times C_3$ ).

8.(Burnside basis theorem) Prove that in a finite  $p$ -group  $G$  every minimal generating set is of the same size, and this size is equal to  $\dim_{GF(p)}(G/\Phi(G))$ . b) Moreover, every  $x \in G \setminus \Phi(G)$  is in a suitable minimal generating set of  $G$ .

9. Show example that  $\Phi(H) \not\leq \Phi(G)$  for some  $H \leq G$ . (Consider the semidirect product of  $C_5 = \langle a \rangle$  and  $C_4 = \langle b \rangle$  where  $a^b = a^2$ . Here  $\Phi(G) = 1$ , but  $\Phi(C_4)$  is of order 2.)

10. Prove that a finite  $p$ -group  $G$  is cyclic, if and only if  $G/\Phi(G)$  is cyclic.

11. Prove that a finite group  $G$  is nilpotent iff  $G' \leq \Phi(G)$

12. A finite  $p$ -group  $G$  is **extraspecial**, if  $\Phi(G) = Z(G) = G'$  are of order  $p$ . Prove that every non-abelian group of order  $p^3$  is extraspecial.

### Problem sheet 9.

1. Prove that if  $G$  is a group  $H \leq G$  subgroup, then  $C_G(H) \triangleleft N_G(H)$  and  $N_G(H)/C_G(H) \leq \text{Aut}(H)$ .

A group  $G$  is  **$p$ -nilpotent**, if it has a normal  $p$ -complement  $K$ :  $K \triangleleft G$ ,  $KP = G$ ,  $K \cap P = \{1\}$ , where  $P \in \text{Syl}_p(G)$ .

2. Prove that if  $K_1$  is a normal  $p_1$ -complement in  $G$  and  $K_2$  is a normal  $p_2$ -complement in  $G$  where  $p_1 \neq p_2$  primes, then  $K_1 \cap K_2$  is a normal  $p_2$ -complement in  $K_1$ .

3.a) Prove that if  $p \mid |G|$  is a minimal prime divisor and  $P \in \text{Syl}_p(G)$  is cyclic, then  $G$  is  $p$ -nilpotent. b) Prove, that if  $G$  is a finite non-abelian simple group then its Sylow 2-subgroup cannot be cyclic!

4.a) Prove that if for a finite group  $G$ , for every prime divisor  $p \in \pi(G)$   $P \in \text{Syl}_p(G)$  is cyclic, then  $G$  is solvable. b) Prove that if  $|G|$  is squarefree, then  $G$  is solvable.

5. Prove that if  $G$  is a non-abelian simple group, then if  $p \in \pi(G)$  is a minimal prime divisor, then either  $p^3 \mid |G|$  or  $12 \mid |G|$ .

6. Prove that if  $G$  is a finitely generated group and  $|G : H| = n$ , then  $H$  is also finitely



generated.

7. Prove that in a finite solvable group, the centralizer  $C_G(F(G))$  of the Fitting- subgroup is contained in  $F(G)$ .
8. Let  $H, K$  be subgroups in  $G$ . Prove that  $[H, K]$  is a normal subgroup in  $\langle H, K \rangle$ .
9. Let  $P$  be a finite  $p$ -group. Prove that if an automorphism  $\alpha \in \text{Aut}(P)$  of  $p'$  order of  $P$  is acting on  $P/\Phi(P)$  trivially, then  $\alpha = id_P$ .
10. Prove that if  $l_i, i = 1, \dots, n$  is a left transversal of a subgroup  $Q$  in  $G$ , then  $l_i^{-1}, i = 1, \dots, n$  is a right transversal of  $Q$  in  $G$ .
11. Let  $Q \leq G$  and  $y_i, i = 1, \dots, n$  is a right transversal of  $Q$  in  $G$ . Prove that if for  $a \in G$ ,  $y_i a = p_i y_{\tau(i)}$  holds, then for  $R(a) = \prod p_i Q'$  the equality  $V(a) = R(a)$  holds.
- 12.a) Let  $n = p_1 \cdots p_t$ , where  $p_1 < p_2 < \dots < p_t$  are primes. Prove that in every group of order  $n$ , the Sylow  $p_t$ - subgroup is normal. b) If additionally,  $(p_i, p_j - 1) = 1$  for every  $i < j$ , then  $G$  is cyclic.
13. Prove that there is no non-abelian simple group of order less than 60.

## Index

- $G$ -invariant partition, 19
- $G$ -orbit of  $\omega$ , 8
- $GL(V)$ , 55
- $\pi$ -subgroup, 35
- $k$ -transitive, 18
- $p$ -nilpotent, 40
- $Core_G(H)$ , 9
  
- AGL(K), 58
- AGL(V), 57
- alternating group, 8, 56
- automorphism group of a group, 13
  
- biggest solvable normal, 30
- block, 20
- Burnside, 29
- Burnside basis theorem, 64
  
- Cauchy, 8
- Cauchy-Frobenius-Burnside, 55
- Cayley, 9
- Cayley-graph, 48
- characteristic subgroup, 26
- characteristically simple, 28
- commutator element, 25
- commutator subgroup, 30
- composition series, 25
- conjugation action on elements, 11
- conjugation action on subgroups, 11
  
- connected, 15
  
- derived length, 27
- derived series, 27
- derived subgroup, 26
- Dyck, 47
  
- elementary abelian group, 29
- equivalence of actions, 13
- even permutation, 7
- exact, 22
- extraspecial  $p$ -group, 64
  
- factor set, 38
- faithful, 6
- Feit-Thompson, 29
- finitely generated group, 64
- Fitting subgroup, 63
- Fratini-subgroup, 63
- free generating set, 47
- Free groups, 45
  
- Gaschütz, 37
- generators and relations, 47
- graph automorphism, 15
- group, 6
- group action, 6
- group extensions, 22
- group of inner automorphisms, 14

Hall  $\pi$ -subgroup, 35  
 Hall $_{\pi}(G)$ , 35  
 imprimitive, 20  
 inner semidirect product, 22  
 inversion, 7  
 iterated wreath product, 24  
 Jordan, 22  
 Kaloujnine, 24  
 lower central series, 31  
 metabelian, 27  
 minimal normal subgroup, 28  
 Nielsen-Schreier, 50  
 nilpotency class, 31  
 nilpotent group, 31  
 non-generator, 63  
 normal  $p$ -complement, 40  
 normal complement, 42  
 odd permutation, 7  
 outer semidirect product, 23  
 permutation, 6  
 permutation group, 6  
 permutation representation, 6  
 point stabilizer, 8  
 primitive, 20  
 reduced word, 45  
 right multiplication, 10  
 Schur–Zassenhaus, 38  
 set of prime divisors, 35  
 sharply  $k$ -transitive, 22  
 small groups, 18  
 solvable group, 25  
 solvable radical, 30  
 split, 22  
 subnormal, 25  
 supersolvable, 32  
 Sylow  $p$ -subgroup, 16, 24  
 Sylow theorems, 16  
 symmetric group, 6  
 transfer, 41  
 transitive, 6  
 transposition, 8  
 tree, 49  
 universal property, 45  
 upper central series, 31  
 wreath product, 23  
 Zorn’s lemma, 50