Group theory

Technische Universität Braunschweig

SS 2007

Jürgen Müller

Contents

1 Groups and subgroups

(1.1) Definition and Remark. a) A set G together with a **multiplication** $\cdot\colon G \times G \to G\colon [g,h] \mapsto g \cdot h$ fulfilling the following conditions is called a **group**:
i) We have **associativity** $(fg)h = f(gh)$, for all $f, g, h \in G$.
ii) There is a **right neutral element** $1 \in G$ such that $g = g \cdot 1$, for all $g \in G$.
iii) For any $g \in G$ there is a **right inverse** $g^{-1} \in G$ such that $gg^{-1} = 1$.

If additionally $gh = hg$ holds, for all $g, h \in G$, then G is called **commutative** or **abelian**. If G is a finite set, the cardinality $|G| \in \mathbb{N}$ is called its **order**; if G is infinite we write $|G| = \infty$.

b) It is immediate that the product $g_1 g_2 \cdots g_n \in G$ is well-defined independently from the bracketing, for all $g_1, \ldots, g_n \in G$. If G is abelian, then it is also immediate that the product $g_1 g_2 \cdots g_n \in G$ is independent from the order of the factors.

For $g \in G$ we have $1 \cdot (g^{-1})^{-1} = gg^{-1}(g^{-1})^{-1} = g \cdot 1 = g$, hence $g = 1 \cdot 1 \cdot (g^{-1})^{-1} = 1 \cdot g$, showing that $1 \in G$ is left neutral. Moreover, $1 = g^{-1}(g^{-1})^{-1} = g^{-1} \cdot gg^{-1} \cdot (g^{-1})^{-1} = g^{-1}g$ shows that g^{-1} is also a left inverse.

Now let $1' \in G$ be any right neutral element, then we have $1' = 1 \cdot 1' = 1$, hence the right neutral element is uniquely determined. Let $g' \in G$ be a right inverse of $g \in G$, then we have $g^{-1} = g^{-1} \cdot 1 = g^{-1} \cdot gg' = g'$, hence the right inverse of $g \in G$ is uniquely determined.

For $g \in G$ let $g^0 := 1$ and recursively $g^{n+1} := g^n \cdot g$ and $g^{-n} := (g^{-1})^n$, for all $n \in \mathbb{N}_0$. Then it is immediate that $g^m g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$, for all $m, n \in \mathbb{Z}$. Moreover, if $g, h \in G$ **commute**, i. e. we have $gh = hg$, then it is also immediate that we have $(gh)^n = g^n h^n = h^n g^n$, for all $n \in \mathbb{Z}$.

c) A subset $U \subseteq G$ is called a **subgroup**, if $1 \in U$ and U is closed under taking products and inverses; then U again is a group. We write $U \leq G$, and if $U \neq G$ then $U < G$ is called a **proper** subgroup. A proper subgroup $U < G$ is called **maximal**, if $U < V \leq G$ implies $V = G$. E. g. the **trivial group** $\{1\}$ and G are subgroups of G.

(1.2) Example. a) Let R be a ring. Then $(R, +)$ is an abelian group.
b) Let K be a field and $K^* := K \setminus \{0\}$. Then $(K^*, \cdot)$ is an abelian group.
c) For $n \in \mathbb{N}$, the set of invertible matrices $GL_n(K) := \{A \in K^{n \times n}; \det(A) \neq 0\}$, together with matrix multiplication, is called the **general linear group** in dimension n over K; it is abelian if and only if $n = 1$.

(1.3) Definition and Remark. a) Let $X \neq \emptyset$ be a set. Then $\mathcal{S}_X := \{\pi\colon X \to X; \pi \text{ bijective}\}$, together with concatenation of maps, is called the **symmetric group** on X; its elements are called **permutations**.

In particular, if $X = \{1, \ldots, n\}$ for some $n \in \mathbb{N}$ we write $\mathcal{S}_n := \mathcal{S}_{\{1,\ldots,n\}}$; for $n = 0$, i. e. $X = \emptyset$, we let $\mathcal{S}_0 := \{1\}$.

b) For $n \in \mathbb{N}$ we have $|\mathcal{S}_n| = n!$, as is seen by induction: For $n = 1$ we have $\mathcal{S}_1 = \{\mathrm{id}_{\{1\}}\}$. For $n \geq 2$ and $\pi \in \mathcal{S}_n$ we have $n\pi = m$ for some $m \in \{1, \ldots, n\}$, and hence $\pi \colon \{1, \ldots, n-1\} \rightarrow \{1, \ldots, n\} \setminus \{m\}$ is bijective as well. Since there are n possibilities to choose m, there are $n \cdot |\mathcal{S}_{n-1}| = n!$ possibilities for π.

c) Any permutation in $\mathcal{S}_n$ can be written uniquely, up to reordering the factors, as a product of **disjoint cycles**. Hence we use **cycle notation**, where often 1-cycles are left out: E. g. we have $\mathcal{S}_1 = \{()\}$, and $\mathcal{S}_2 = \{(), (1,2)\}$, and $\mathcal{S}_3 = \{(), (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$. While $\mathcal{S}_1$ and $\mathcal{S}_2$ are abelian, we from $(1,2,3) \cdot (1,2) = (1,3) \neq (2,3) = (1,2) \cdot (1,2,3)$ deduce that for $n \geq 3$ the group $\mathcal{S}_n$ is not abelian.

(1.4) Example. Let $O_2(\mathbb{R}) := \{g \in \mathrm{GL}_2(\mathbb{R}); g \text{ orthogonal}\} \leq \mathrm{GL}_2(\mathbb{R})$ be the **orthogonal group** of rank 2 over $\mathbb{R}$. We have $O_2(\mathbb{R}) = \{g \in O_2(\mathbb{R}); \det(g) = 1\} \mathbin{\dot\cup} \{g \in O_2(\mathbb{R}); \det(g) = -1\}$, where $\mathrm{SO}_2(\mathbb{R}) := \{g \in O_2(\mathbb{R}); \det(g) = 1\} \leq O_2(\mathbb{R})$ is the **special orthogonal group** consisting of **rotations**, and where $\{g \in O_2(\mathbb{R}); \det(g) = -1\}$ consists of **reflections**.

For $n \geq 3$, let $\mathcal{D} \subseteq \mathbb{R}^2$ be a regular n-gon centred at the origin of the Euclidean plane, and let $G := \{g \in O_2(\mathbb{R}); \mathcal{D}g = \mathcal{D}\} \leq O_2(\mathbb{R})$ be its **group of symmetries**. The elements of G permute the vertices of $\mathcal{D}$, and since the vertices contain an $\mathbb{R}$-basis of $\mathbb{R}^2$ the elements of G are uniquely described by these permutations. Thus assuming the vertices to be numbered $1, \ldots, n$ counterclockwise, we may identify G with the **dihedral group** $D_{2n} \leq \mathcal{S}_n$. We describe the elements of D_{2n}, showing that $|D_{2n}| = 2n$:

Since rotations in $O_2(\mathbb{R})$ are determined by their rotation angle, the rotations in D_{2n} are those with angle $k \cdot \frac{2\pi}{n}$, for $k \in \{0, \ldots, n-1\}$. Thus D_{2n} contains precisely the n rotations τ_n^k, for $k \in \{0, \ldots, n-1\}$, where $\tau_n := (1, 2, \ldots, n) \in \mathcal{S}_n$. Since reflections in $O_2(\mathbb{R})$ are determined by their reflection axis, we have to distinguish the cases n odd and n even:

For n odd the reflection axis of an element of D_{2n} runs through one of the vertices of $\mathcal{D}$ and the edge opposite. Thus in this case D_{2n} contains precisely n reflections, one of them being $\sigma_n := (1)(2,n)(3,n-1) \cdots (\frac{n+1}{2}, \frac{n+3}{2}) \in \mathcal{S}_n$.

For n even the reflection axis of an element of D_{2n} either runs through a pair of opposite vertices, or runs through a pair of opposite edges. Thus in this case D_{2n} also contains precisely n reflections, one of the former being $\sigma_n := (1)(\frac{n+2}{2})(2,n)(3,n-1) \cdots (\frac{n}{2}, \frac{n+4}{2}) \in \mathcal{S}_n$, and one of the latter being $(1,2)(3,n)(4,n-1) \cdots (\frac{n+2}{2}, \frac{n+4}{2}) \in \mathcal{S}_n$.

E. g. for $n = 3$ we have $D_6 = \{(), (1,2,3), (1,3,2); (2,3), (1,3), (1,2)\} = \mathcal{S}_3$, and for $n = 4$ and $n = 5$ we have, respectively,

$$\begin{array}{rcl} D_8 & = & \{(), (1,2,3,4), (1,3)(2,4), (1,4,3,2); \\ & & (2,4), (1,3), (1,2)(3,4), (1,4)(2,3)\}, \\ D_{10} & = & \{(), (1,2,3,4,5), (1,3,5,2,4), (1,4,2,5,3), (1,5,4,3,2); \\ & & (2,5)(3,4), (1,3)(4,5), (1,5)(2,4), (1,2)(3,5), (1,4)(2,3)\}. \end{array}$$

(1.5) Definition and Remark. a) Let G be a group, and let $\{U_i \leq G; i \in \mathcal{I}\}$ where $\mathcal{I} \neq \emptyset$ is an index set. Then $\bigcap_{i\in\mathcal{I}} U_i \leq G$ is a subgroup, while $\bigcup_{i\in\mathcal{I}} U_i \subseteq G$ in general is not.

Let $S \subseteq G$. Then $\langle S \rangle := \bigcap\{U \leq G; S \subseteq U\} \leq G$ is the smallest subgroup of G containing S. It is called the subgroup **generated** by S, where S called a **generating set** of $\langle S \rangle$, and if S is finite then $\langle S \rangle$ is called **finitely generated**.

Letting $S^{-1} := \{g^{-1}; g \in S\}$, it is immediate that $\langle S \rangle$ consists of all finite products of elements of $S \cup S^{-1}$. We have $\langle \emptyset \rangle = \langle 1 \rangle = \{1\}$ and $\langle G \rangle = G$, hence in particular any finite group is finitely generated.

b) A subgroup $U \leq G$ is called **cyclic**, if there is $g \in U$ such that $U = \langle g \rangle$. We have $\langle g \rangle = \{g^k; k \in \mathbb{Z}\}$, which implies that cyclic groups are abelian. Given $g \in G$, let $|g| := |\langle g \rangle| \in \mathbb{N} \,\dot\cup\, \{\infty\}$ be its **order**.

E. g. we have $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$, and for $n \in \mathbb{Z}$ we have $(\mathbb{Z}/n\mathbb{Z}, +) = \langle \overline{1} \rangle$.

(1.6) Theorem. Let $C = \langle g \rangle$, and let $I_g := \{k \in \mathbb{Z}; g^k = 1\} \trianglelefteq \mathbb{Z}$.
a) Then $|g|$ is finite if and only if $I_g \neq \{0\}$. In this case, we have $I_g = |g|\mathbb{Z} \trianglelefteq \mathbb{Z}$ and $C = \{g^k; k \in \{0, \ldots, |g| - 1\}\}$.
b) Any subgroup of C is cyclic as well. If $|g|$ is finite, then there is a subgroup $U \leq C$ of order $d \in \mathbb{N}$ if and only if $d \mid |g|$; in this case U is uniquely determined.

Proof. a) If $|g|$ is finite, then there are $i \neq j$ such that $g^i = g^j$, hence $g^{i-j} = 1$, thus $0 \neq i - j \in I_g$. If conversely $I_g = n\mathbb{Z} \neq \{0\}$, where $n > 0$, then for any $i \in \mathbb{Z}$ there are $k, j \in \mathbb{Z}$ such that $0 \leq j < n$ and $i = kn + j$, implying $g^i = g^j$, thus $\langle g \rangle = \{g^k; k \in \{0, \ldots, n - 1\}\}$ is finite. Finally, assume that there are $0 \leq j < i < n$ such that $g^i = g^j$, then $i - j \in I_g$ such that $0 < i - j < n$, a contradiction; hence the g^k, where $k \in \{0, \ldots, n - 1\}$, are pairwise distinct.

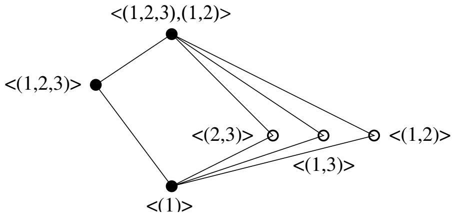
b) Let $\{1\} \neq U \leq C$, and let $I_U := \{k \in \mathbb{Z}; g^k \in U\} = m\mathbb{Z} \trianglelefteq \mathbb{Z}$, where $m > 0$. Hence we have $\langle g^m \rangle \leq U$. Conversely, if $g^i \in U$ for some $i \in \mathbb{Z}$, let $k, j \in \mathbb{Z}$ such that $0 \leq j < m$ and $i = km + j$. This yields $g^j = g^{i-km} = g^i(g^m)^{-k} \in U$, thus $j \in I_U$ and hence $j = 0$, implying $g^i = (g^m)^k \in \langle g^m \rangle$. Thus we have $U = \langle g^m \rangle$.

Let $n := |C| = |g|$ be finite, and let $m \in \mathbb{Z}$. Then for $k \in \mathbb{Z}$ we have $g^{mk} = 1$ if and only if $n \mid mk$, which holds if and only if $\frac{n}{\gcd(m,n)} \mid k$. Hence we have $|g^m| = \frac{n}{\gcd(m,n)}$, showing that the order of any subgroup of C divides n.

Let now $n = dm$ for some $d \in \mathbb{N}$. Then we have $|g^m| = d$. If moreover $|g^k| = d$ for some $k \in \mathbb{Z}$, then $\frac{n}{\gcd(k,n)} = d = \frac{n}{m}$, hence $m = \gcd(k, n) \mid k$, thus we have $\langle g^k \rangle \leq \langle g^m \rangle$, and hence $|g^k| = d = |g^m|$ implies $\langle g^k \rangle = \langle g^m \rangle$. ♯

(1.7) Example. We determine the subgroups of the symmetric group $\mathcal{S}_3$: It is immediate that any non-cyclic subgroup already coincides with $\mathcal{S}_3$. Hence the only non-trivial proper subgroups are the three cyclic subgroups $\langle(1, 2)\rangle$, and $\langle(1, 3)\rangle$, and $\langle(2, 3)\rangle$ of order 2, and the cyclic subgroup $\langle(1, 2, 3)\rangle = \langle(1, 3, 2)\rangle$ of

Table 1: Subgroup lattice of $\mathcal{S}_3$.



order 3. Hence the **lattice of subgroups** is as depicted in the **Hasse diagram** in Table 1.

(1.8) Definition and Remark. a) Let G be a group, and let $U \leq G$. For $g \in G$ let $Ug := \{ug; u \in U\} \subseteq G$ be the associated **(right) coset**, and let $U\backslash G := \{Ug; g \in G\}$ be the set of all cosets of U in G.

A subset $T \subseteq G$ such that $T \to U\backslash G \colon t \mapsto Ut$ is a bijection is called a **(right) transversal** of the cosets of U in G, and the cardinality $[G \colon U] := |T| \in \mathbb{N} \,\dot\cup\, \{\infty\}$ is called the **index** of U in G; transversals exist by the Axiom of Choice.

b) Similarly we define **left cosets** and **left transversals**. For any right coset $Ug \subseteq G$, where $g \in G$, inversion yields the left coset $g^{-1}U \subseteq G$. Hence there is a bijection between right and left cosets, and the index $[G \colon U]$ is independent from whether right or left cosets are considered.

In general right cosets and left cosets do not coincide: E. g. for $U = \langle(1,2)\rangle < \mathcal{S}_3 = G$ we have $\mathcal{S}_3 = \{(), (1,2)\} \,\dot\cup\, \{(1,2,3), (2,3)\} \,\dot\cup\, \{(1,3,2), (1,3)\}$ as right cosets and $\mathcal{S}_3 = \{(), (1,2)\} \,\dot\cup\, \{(1,2,3), (1,3)\} \,\dot\cup\, \{(1,3,2), (2,3)\}$ as left cosets, hence $T = \{(), (1,2,3), (1,3)\}$ is a right transversal but not a left transversal.

(1.9) Theorem: Lagrange.
Let G be a group, let $U \leq G$, and let $T \subseteq G$ be a transversal of U in G.
a) Then we have $G = \coprod_{t \in T} Ut$.
b) If $|G|$ is finite, then we have $|G| = |U| \cdot |T|$.

Proof. a) We have $G = \bigcup_{g \in G} Ug$. Given $g, h \in G$ we show that $Ug \cap Uh \neq \emptyset$ implies $Ug = Uh$: Let $vh \in Ug \cap Uh$ for some $v \in U$, then for all $u \in U$ we have $uh = uv^{-1}vh \in Ug$, thus $Uh \subseteq Ug$, and similarly $Ug \subseteq Uh$.
b) Since $ug = u'g$ implies $u = u'$ for all $g \in G$ and $u, u' \in U$, the map $U \to Ug \colon u \mapsto ug$ is a bijection. Hence we have $|Ug| = |U|$ for all $g \in G$. ♯

(1.10) Corollary. Let $|G|$ be finite. Then for all $g \in G$ we have $|g| \mid |G|$.

In particular we have $g^{|G|} = 1$. Letting $\exp(G) := \mathrm{lcm}\{|g|; g \in G\} \in \mathbb{N}$ denote the **exponent** of G, we have $\exp(G) \mid |G|$. If $|G|$ is a prime, then G is cyclic.

(1.11) Theorem: Characterisation of cyclic groups.
Let G be a finite group. Then G is cyclic if and only if G for any $d \in \mathbb{N}$ has at most one subgroup of order d.

Proof. For $n \in \mathbb{N}$ let $(\mathbb{Z}/n\mathbb{Z})^* := \{\overline{k} \in \mathbb{Z}/n\mathbb{Z}; \gcd(k, n) = 1\}$ and $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^*| \in \mathbb{N}$ be **Euler's totient function**. Hence for a cyclic group C of order n there are precisely $\varphi(n)$ elements $g \in C$ such that $C = \langle g \rangle$. Thus the subgroup structure of cyclic groups implies $\sum_{d \in \mathbb{N}, d \mid n} \varphi(d) = n$.

We only have to show the 'if' part: Let $n = |G| > 1$. For any $d \in \mathbb{N}$ there is an element of order d only if $d \mid n$, and in this case there at most $\varphi(d)$ of them. Thus by $\sum_{d \in \mathbb{N}, n \neq d \mid n} \varphi(d) = n - \varphi(n) > 0$ there is an element of order n. ♯

2 Homomorphisms

(2.1) Definition and Remark. a) Let G and H be groups. A map $\varphi\colon G \to H$ is called a **(group) homomorphism** if $(gg')\varphi = g\varphi \cdot g'\varphi$ for all $g, g' \in G$.

If φ is surjective it is called an **epimorphism**; if φ is injective it is called a **monomorphism**; if φ is bijective it is called an **isomorphism**, in this case we write $G \cong H$, and the inverse map $\varphi^{-1}\colon H \to G$ is an isomorphism as well. If $G = H$, then φ is called an **endomorphism**; if φ is a bijective endomorphism it is called an **automorphism**.

b) Then $1\varphi = (1 \cdot 1)\varphi = 1\varphi \cdot 1\varphi$ implies $1\varphi = 1$. For $g \in G$ we have $1 = 1\varphi = (gg^{-1})\varphi = g\varphi \cdot (g^{-1})\varphi$, hence $(g^{-1})\varphi = (g\varphi)^{-1}$.

From this it is immediate that for $U \leq G$ we have $U\varphi \leq H$, in particular $\mathrm{im}(\varphi) \leq H$, and for $V \leq H$ we have $\varphi^{-1}(V) \leq G$, in particular the **kernel** $\ker(\varphi) := \varphi^{-1}(\{1\}) = \{g \in G; g\varphi = 1\} \leq G$ is a subgroup.

c) A subgroup $U \leq G$ is called **normal** if $Ug \subseteq gU$ for all $g \in G$; in this case we write $U \trianglelefteq G$. If $U \trianglelefteq G$ then inversion yields $gU \subseteq Ug$ for all $g \in G$, implying $Ug = gU$ and $g^{-1}Ug = U$ for all $g \in G$, hence in particular right and left cosets of U in G coincide. E. g. any subgroup of an abelian group is normal.

A normal subgroup $\{1\} < U \trianglelefteq G$ is called **minimal**, if $V \trianglelefteq G$ such that $V < U$ implies $V = \{1\}$; and $U \triangleleft G$ is called **maximal**, if $U < V \trianglelefteq G$ implies $V = G$.

(2.2) Theorem: Homomorphism Theorem.
Let G be a group.
a) Let $N \trianglelefteq G$. Then the set G/N is a group with multiplication $gN \cdot hN := ghN$ for all $g, h \in G$, called the associated **factor group**. The **natural map** $\nu_N\colon G \to G/N\colon g \mapsto gN$ is an epimorphism such that $\ker(\nu_N) = N$.

b) Let $\varphi\colon G \to H$ be a homomorphism. Then $\ker(\varphi) \trianglelefteq G$ and $\overline{\varphi}\colon G/\ker(\varphi) \to \mathrm{im}(\varphi)\colon g\ker(\varphi) \mapsto \varphi g$ is an isomorphism such that $\varphi = \nu_{\ker(\varphi)} \cdot \overline{\varphi}$.

Proof. a) We only have to show that multiplication is well defined: Let $g' \in gN$ and $h' \in hN$. Then we have $g' = gm$ and $h' = hn$ for some $m, n \in N$, and thus $g'h' = gm \cdot hn = gh \cdot h^{-1}mh \cdot n \in ghN$. Hence ν_N is an epimorphism, and for $g \in G$ we have $g \in \ker(\nu_N)$ if and only if $gN = N$.

b) Let $g \in G$ and $h := g\varphi \in \mathrm{im}(\varphi)$. Then we have $\ker(\varphi)g = \varphi^{-1}(\{h\}) = g\ker(\varphi)$: We have $(\ker(\varphi)g)^{\varphi} = \{h\} = (g\ker(\varphi))^{\varphi}$, and for $g' \in \varphi^{-1}(\{h\})$ we have $(g'g^{-1})\varphi = 1 = (g^{-1}g')\varphi$, thus $g'g^{-1}, g^{-1}g' \in \ker(\varphi)$, hence $g' \in \ker(\varphi)g \cap g\ker(\varphi)$. Thus $\ker(\varphi) \trianglelefteq G$, and φ is injective if and only if $\ker(\varphi) = \{1\}$.

Moreover, $\overline{\varphi}$ is well-defined and an epimorphism. We have $(g\ker(\varphi))^{\overline{\varphi}} = 1$ if and only if $g \in \ker(\varphi)$, hence $\ker(\overline{\varphi}) = \{1\}$, implying that $\overline{\varphi}$ is injective. ♯

(2.3) Example. a) The trivial homomorphism $\varphi\colon G \to \{1\}\colon g \mapsto 1$ yields $\ker(\varphi) = G \trianglelefteq G$ and $G/G \cong \{1\}$. The identity automorphism $\mathrm{id}_G\colon G \to G\colon g \mapsto g$ yields $\ker(\mathrm{id}_G) = \{1\} \trianglelefteq G$ and $G/\{1\} \cong G$. A group $G \neq \{1\}$ having $\{1\}$ and G as its only normal subgroups is called **simple**.
b) Let $C = \langle g \rangle$ be a cyclic group. Then $\varphi\colon \mathbb{Z} \to C\colon k \mapsto g^k$ is an epimorphism. If $|g| = \infty$ then we have $\ker(\varphi) = \{0\} \trianglelefteq \mathbb{Z}$ and thus $\mathbb{Z} \cong C$. If $n := |g| \in \mathbb{N}$ then we have $\ker(\varphi) = n\mathbb{Z} \trianglelefteq \mathbb{Z}$ and thus $\mathbb{Z}/n\mathbb{Z} \cong C$, where the natural epimorphism of additive groups is given as $\nu_n\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}\colon k \mapsto \overline{k}$. Hence for any $n \in \mathbb{N} \,\dot{\cup}\, \{\infty\}$ up to isomorphism there is precisely one cyclic group of order n; in multiplicative notation denoted by C_n.
c) Let K be a field. Then $\det\colon GL_n(K) \to K^*$ is an epimorphism, and we have $SL_n(K) := \ker(\det) = \{A \in GL_n(K); \det(A) = 1\} \trianglelefteq GL_n(K)$, being called the **special linear group** in dimension n over K. Thus we have $GL_n(K)/SL_n(K) \cong K^*$.

(2.4) Lemma. Let $n \in \mathbb{N}$, and let $\pi \in \mathcal{S}_n$ be a product of $r \in \mathbb{N}$ disjoint cycles. If $\pi = \tau_1 \cdots \tau_s \in \mathcal{S}_n$, where $s \in \mathbb{N}_0$ and the $\tau_i \in \mathcal{S}_n$ are **transpositions**, i. e. 2-cycles, then we have $s \equiv n - r \pmod 2$.

Proof. We proceed by induction on $s \in \mathbb{N}_0$: For $s = 0$ we have $\pi = ()$ and $r = n$. For $s > 0$ let $\tau_s = (i, j) \in \mathcal{S}_n$ and $\sigma := \tau_1 \cdots \tau_{s-1} \in \mathcal{S}_n$. Let σ be a product of $r' \in \mathbb{N}$ disjoint cycles, by induction we have $s - 1 \equiv n - r' \pmod 2$.

If i, j occur in the same cycle of σ, then $\pi = \sigma\tau_s = (\ldots)(i, \ldots, k, j, l, \ldots)(i, j) = (\ldots)(i, \ldots, k)(j, l, \ldots)$. Hence π is a product of $r = r' + 1$ disjoint cycles, and $n - r \equiv n - r' - 1 \equiv s - 2 \equiv s \pmod 2$. If i, j occur in distinct cycles of σ, then we have $\pi = \sigma\tau_s = (\ldots)(i, \ldots, k)(j, \ldots, l)(i, j) = (\ldots)(i \ldots k, j, \ldots, l)$. Hence π is a product of $r = r' - 1$ disjoint cycles, and $n - r \equiv n - r' + 1 \equiv s \pmod 2$. ♯

(2.5) Definition and Remark. a) For a k-cycle, where $k \geq 2$, we have $(a_1, a_2, \ldots, a_k) = (a_1, a_2)(a_1, a_3) \cdots (a_1, a_k)$, which is a product of $k-1$ transpositions. Hence any finite permutation can be written as a product of transpositions. This representation in general is not unique, not even the number of transpositions is: $(1,2,3) = (1,3)(1,2) = (1,2)(2,3) = (1,2)(1,3)(2,3)(1,2) \in \mathcal{S}_3$.

b) Thus the **sign** map $\mathrm{sgn}\colon \mathcal{S}_n \to \{\pm 1\} \cong C_2 \colon \pi = \tau_1 \cdot \cdots \cdot \tau_s \mapsto (-1)^s$, where $n \in \mathbb{N}$ and the $\tau_i \in \mathcal{S}_n$ are transpositions, is a homomorphism. Its kernel $\mathcal{A}_n := \ker(\mathrm{sgn}) \leq \mathcal{S}_n$ is called the associated **alternating group**; the elements of $\mathcal{A}_n$ and $\mathcal{S}_n \setminus \mathcal{A}_n$ are called **even** and **odd** permutations, respectively.

For $n = 1$ we have $\mathrm{im}(\varphi) = \{1\}$, hence $\mathcal{A}_1 = \mathcal{S}_1$. For $n \geq 2$, since $\mathrm{sgn}((1,2)) = -1$, the sign homomorphism is surjective, hence $\mathcal{A}_n \trianglelefteq \mathcal{S}_n$ such that $\mathcal{S}_n / \mathcal{A}_n \cong C_2$, in particular we have $|\mathcal{A}_n| = \frac{n!}{2}$.

3 Actions

(3.1) Definition and Remark. a) Let G be a group, and let $X \neq \emptyset$ be a set. Then G is called to **act** on X, and X is called a **G-set**, if there is an **action map** $X \times G \to X \colon [x, g] \mapsto x \cdot g$ such that **i)** $x1 = x$ and **ii)** $x(gh) = (xg)h$ for all $g, h \in G$ and $x \in X$.

If X and Y are G-sets, then a map $\alpha\colon X \to Y$ such that $(xg)\alpha = (x\alpha)g$ for all $x \in X$ and $g \in G$ is called a **homomorphism** of G-sets. Isomorphic G-sets are also called **equivalent**.

b) Given an action of G on X, for $g \in G$ let $\varphi_g \colon X \to X \colon x \mapsto xg$. Hence we have $\varphi_g \varphi_{g^{-1}} = \mathrm{id}_X = \varphi_{g^{-1}} \varphi_g = \mathrm{id}_X$, thus $\varphi_g \in \mathcal{S}_X$ for all $g \in G$. From $\varphi_g \varphi_h = \varphi_{gh}$, for all $g, h \in G$, we get an **action homomorphism** $\varphi\colon G \to \mathcal{S}_X \colon g \mapsto \varphi_g$. If φ is injective, then the action is called **faithful**.

Conversely, if $\varphi\colon G \to \mathcal{S}_X \colon g \mapsto \varphi_g$ is a homomorphism, then $X \times G \to X \colon [x, g] \mapsto x\varphi_g$ defines an action of G on X: From $\varphi_1 = \mathrm{id}_X$ we get $x1 = x$, and $\varphi_g \varphi_h = \varphi_{gh}$ implies $x(gh) = (xg)h$ for all $g, h \in G$ and $x \in X$.

c) The relation $\mathcal{O} := \{[x, y] \in X \times X; y = xg \text{ for some } g \in G\}$ is an equivalence relation on X: From $x1 = x$ we infer that $\mathcal{O}$ is reflexive; from $y = xg$ we get $yg^{-1} = x$, implying that $\mathcal{O}$ is symmetric; and from $y = xg$ and $z = yh$ we get $z = xgh$, implying that $\mathcal{O}$ is transitive.

Given $x \in X$, its equivalence class $xG := \{xg \in X; g \in G\}$ again is a G-set, called the **G-orbit** of x ; its cardinality $|xG|$ is called its **length**, and a subset $T \subseteq G$ such that $T \to xG \colon t \mapsto xt$ is a bijection is called a **transversal** of xG with respect to x; transversals exist by the Axiom of Choice. Let $X/G := \{xG \subseteq X; x \in X\}$; if $|X/G| = 1$, i. e. X consists of a single G-orbit, then X is called a **transitive** G-set.

d) For $x \in X$ let $\mathrm{Stab}_G(x) = G_x := \{g \in G; xg = x\} \subseteq G$ be the **(point) stabiliser** of x in G; it is immediate that $\mathrm{Stab}_G(x) \leq G$ is a subgroup.

(3.2) Example. **a)** Let G be a group, and let $X \neq \emptyset$. Then $G \to \mathcal{S}_X : g \mapsto \mathrm{id}_X$ induces the **trivial** action; its orbits are the singleton subsets of X, and hence $\mathrm{Stab}_G(x) = G$ for all $x \in X$.

Using the identity map $\mathrm{id}_{\mathcal{S}_n} : \mathcal{S}_n \to \mathcal{S}_n$, any subgroup $G \leq \mathcal{S}_n$ acts **naturally** on $\{1, \ldots, n\}$. The natural action of the full symmetric group $\mathcal{S}_n$ is transitive, and we have $\mathrm{Stab}_{\mathcal{S}_n}(n) = \mathcal{S}_{n-1}$.

b) Let G be a group, and let $U \leq G$. Then U acts on G by **left multiplication** $\lambda_u \colon G \to G \colon g \mapsto u^{-1}g$ for all $u \in U$: We have $g\lambda_1 = 1^{-1}g = g$ and $g\lambda_{uv} = (uv)^{-1}g = v^{-1}u^{-1}g = (g\lambda_u)\lambda_v$ for all $g \in G$ and $u, v \in U$. Hence the U-orbit of $g \in G$ is the right coset $Ug \subseteq G$, and we have $\mathrm{Stab}_U(g) = \{1\}$.

c) The group G acts transitively on $U\backslash G$ by **right multiplication** $\rho_g \colon U\backslash G \to U\backslash G \colon Ux \mapsto Uxg$ for all $g \in G$: We have $(Ux)1 = Ux$ and $(Ux)gh = (Uxg)h$ for all $g, h, x \in G$, as well as $Ug = (U1)g$. Moreover, we have $\mathrm{Stab}_G(U) = U$.

(3.3) Theorem. Let X be a transitive G-set, and let $x \in X$.
a) Then $\beta \colon \mathrm{Stab}_G(x)\backslash G \to X \colon \mathrm{Stab}_G(x)g \mapsto xg$ is an isomorphism of G-sets. Hence $|X| = [G \colon \mathrm{Stab}_G(x)]$, and if $|G|$ is finite then $|X| = \frac{|G|}{|\mathrm{Stab}_G(x)|} \mid |G|$.
b) For $g \in G$ we have $\mathrm{Stab}_G(xg) = g^{-1}\mathrm{Stab}_G(x)g$. Hence for the associated action homomorphism $\varphi \colon G \to \mathcal{S}_X$ we have $\ker(\varphi) = \bigcap_{g \in G} g^{-1}\mathrm{Stab}_G(x)g \trianglelefteq G$.
c) Let Y be a transitive G-set, and let $y \in Y$. Then there is an isomorphism of G-sets $\beta \colon X \to Y$ if and only if there is $g \in G$ such that $\mathrm{Stab}_G(y) = g^{-1}\mathrm{Stab}_G(x)g$.

Proof. **a)** For $g \in G$ and $h \in \mathrm{Stab}_G(x)$ we have $xhg = xg$, hence β is well-defined, and since G acts transitively β is surjective. For $g, g' \in G$ such $xg = xg'$ we have $g'g^{-1} \in \mathrm{Stab}_G(x)$, hence $g' \in \mathrm{Stab}_G(x)g$, thus β is injective as well. We have $(\mathrm{Stab}_G(x)gh)^\beta = xgh = (xg)h = (\mathrm{Stab}_G(x)g)^\beta \cdot h$ for all $g, h \in G$.

b) For $h \in G$ we have $h \in \mathrm{Stab}_G(xg)$ if and only if $xgh = xg$, which holds if and only if $ghg^{-1} \in \mathrm{Stab}_G(x)$, which in turn holds if and only if $h \in g^{-1}\mathrm{Stab}_G(x)g$. Hence $\ker(\varphi) = \{g \in G; g\varphi = \mathrm{id}_X\} = \bigcap_{y \in X} \mathrm{Stab}_G(y) = \bigcap_{g \in G} \mathrm{Stab}_G(xg)$.

c) Let $\alpha \colon X \to Y$ be an isomorphism of G-sets. For $h \in \mathrm{Stab}_G(x)$ we then have $(x\alpha)h = (xh)\alpha = x\alpha$, implying $\mathrm{Stab}_G(x) \leq \mathrm{Stab}_G(x\alpha)$, and similarly $\mathrm{Stab}_G(x\alpha) \leq \mathrm{Stab}_G(x)$. Letting $g \in G$ such that $(x\alpha)g = y$ we get $\mathrm{Stab}_G(x) = \mathrm{Stab}_G(x\alpha) = g\mathrm{Stab}_G(y)g^{-1}$.

Conversely, replacing $x \in X$ by $xg \in X$, we may assume that $\mathrm{Stab}_G(x) = \mathrm{Stab}_G(y)$. Using $\beta \colon \mathrm{Stab}_G(x)\backslash G \to X$ and $\beta' \colon \mathrm{Stab}_G(y)\backslash G \to Y$ from (a) yields the isomorphism of G-sets $\beta^{-1}\beta' \colon X \to Y$. ♯

(3.4) Corollary: Cayley's Theorem.
Let G be a group. Then G is isomorphic to a subgroup of $\mathcal{S}_G$.

Proof. G acts transitively on $\{1\}\backslash G \cong G$, called the **regular** action, and we have $\mathrm{Stab}_G(1) = \{1\}$. Hence for the associated action homomorphism $\varphi \colon G \to$

$\mathcal{S}_G$ we have $\ker(\varphi) \leq \mathrm{Stab}_G(1) = \{1\}$, thus φ is injective. ♯

(3.5) Example. a) Let G be a group. Then G acts on G by **conjugation** $\kappa_g \colon G \to G \colon x \mapsto x^g := g^{-1}xg$ for all $g \in G$. The associated orbits are called the **conjugacy classes** of G; the action is transitive if and only if $G = \{1\}$.

Given $x \in G$, the stabiliser $C_G(x) := \mathrm{Stab}_G(x) = \{g \in G; gx = xg\}$ is called the **centraliser** of x in G. For the action homomorphism $\kappa \colon G \to \mathcal{S}_G$ we have $Z(G) := \ker(\kappa) = \{x \in G; gx = xg \text{ for all } g \in G\} \trianglelefteq G$, called the **centre** of G.

b) Similarly, G acts on $\{U \leq G\}$ by conjugation $\kappa_g \colon U \mapsto U^g := g^{-1}Ug$ for all $g \in G$. The associated orbits are called the **conjugacy classes** of subgroups of G; the action is transitive if and only if $G = \{1\}$.

Given $U \leq G$, the stabiliser $N_G(U) := \mathrm{Stab}_G(U) = \{g \in G; gU = Ug\}$ is called the **normaliser** of U in G. Hence $U \leq N_G(U) \leq G$ is the largest subgroup of G having U as a normal subgroup, and we have $N_G(U) = G$ if and only if $U \trianglelefteq G$.

c) Let $\mathcal{D} \subseteq \mathbb{R}^2$ and $G \leq O_2(\mathbb{R})$ be as in (1.4). Then the map $\varphi \colon G \to \mathcal{S}_n$, associating to each element of G the permutation it induces on the vertices $\{1, \ldots, n\}$ of $\mathcal{D}$, is a monomorphism, yielding a transitive action of $G \cong \mathrm{im}(\varphi) = D_{2n} \leq \mathcal{S}_n$ on $\{1, \ldots, n\}$. We have $|\mathrm{Stab}_{D_{2n}}(1)| = \frac{|D_{2n}|}{|1 \cdot D_{2n}|} = \frac{2n}{n} = 2$, and since $1\sigma_n = 1$ we conclude $\mathrm{Stab}_{D_{2n}}(1) = \langle \sigma_n \rangle \leq D_{2n}$.

(3.6) Theorem: Cauchy-Frobenius-Burnside Lemma.
Let G be a finite group, and let X be a finite G-set. Then the number of orbits is given by $|X/G| = \frac{1}{|G|} \cdot \sum_{g \in G} |\mathrm{Fix}_X(g)|$, where $\mathrm{Fix}_X(g) := \{x \in X; xg = x\}$ is the set of **fixed points** of $g \in G$.

Proof. Letting $\mathcal{O} := \{[x, g] \in X \times G; xg = x\}$, we use **double counting**: On the one hand we have $|\mathcal{O}| = \sum_{g \in G} |\{x \in X; xg = x\}| = \sum_{g \in G} |\mathrm{Fix}_X(g)|$.

On the other hand we have $|\mathcal{O}| = \sum_{x \in X} |\{g \in G; xg = x\}| = \sum_{x \in X} |\mathrm{Stab}_G(x)|$. For $y \in xG$ we have $|yG| = |xG|$, and thus $|\mathrm{Stab}_G(x)| = |\mathrm{Stab}_G(y)|$. Letting $T \subseteq X$ be a set of orbit representatives, we get $\sum_{x \in X} |\mathrm{Stab}_G(x)| = \sum_{x \in T} \sum_{y \in xG} |\mathrm{Stab}_G(y)| = \sum_{x \in T} |xG| \cdot |\mathrm{Stab}_G(x)| = \sum_{x \in T} |G| = |X/G| \cdot |G|$. ♯

(3.7) Example. A **necklace** with $n \geq 3$ pearls having $k \in \mathbb{N}$ colours is a map $\eta \colon \{1, \ldots, n\} \to \{1, \ldots, k\}$. The set $\{1, \ldots, n\}$ may be considered as the set of vertices of a regular n-gon $\mathcal{D}$, and necklaces are called **equivalent** if they arise from each other by a symmetry of $\mathcal{D}$.

Let $\mathcal{N}_{n,k} := \{\eta \colon \{1, \ldots, n\} \to \{1, \ldots, k\}\}$; hence we have $|\mathcal{N}_{n,k}| = k^n$. It is immediate that $D_{2n} \leq \mathcal{S}_n$ acts on $\mathcal{N}_{n,k}$ by $\eta \mapsto \eta^\pi := \pi^{-1}\eta$ for all $\pi \in D_{2n}$. The equivalence classes of necklaces are precisely the D_{2n}-orbits on $\mathcal{N}_{n,k}$, their number $t_{n,k} := |\mathcal{N}_{n,k}/D_{2n}| \in \mathbb{N}$ can be determined using Burnside's Lemma:

Table 2: Cycles of D_6 and D_8.

$\pi \in D_6$	r
$()$	3
$(1,2,3)$	1
$(1,3,2)$	1
$(2,3)$	2
$(1,2)$	2
$(1,3)$	2

$\pi \in D_8$	r
$()$	4
$(1,2,3,4)$	1
$(1,3)(2,4)$	2
$(1,4,3,2)$	1
$(2,4)$	3
$(1,2)(3,4)$	2
$(1,3)$	3
$(1,4)(2,3)$	2

For $\pi \in \mathcal{S}_n$ and $\eta \in \mathcal{N}_{n,k}$ we have $\eta^\pi = \eta$ if and only if $i\pi^{-1}\eta = i\eta$ for all $i \in \{1, \ldots, n\}$. This holds if and only if η is constant on the various disjoint cycles of π. Hence if π has $r \in \mathbb{N}$ disjoint cycles then we have $|\mathrm{Fix}_{\mathcal{N}_{n,k}}(\pi)| = k^r$.

E. g. for $n = 3$ and $n = 4$ we from Table 2 get $t_{3,k} = \frac{1}{6} \cdot (k^3 + 3k^2 + 2k) = \frac{1}{6} \cdot k(k+1)(k+2) = \binom{k+2}{3}$ and $t_{4,k} = \frac{1}{8} \cdot (k^4 + 2k^3 + 3k^2 + 2k) = \frac{1}{8} \cdot k(k+1)(k^2+k+2)$.

(3.8) Lemma: Schreier.
Let $G = \langle M \rangle$ be a group, let X be a G-set, and let $T := \{t_y \in G; y \in X\}$ be a transversal of $xG \subseteq X$ with respect to $x \in X$, such that $y = xt_y$ for all $y \in X$ and $t_x := 1$. Then we have $\mathrm{Stab}_G(x) = \langle t_y \cdot g \cdot t_{yg}^{-1} \in G; y \in X, g \in M \rangle$.

Proof. Let $S := \{t_y \cdot g \cdot t_{yg}^{-1} \in G; y \in X, g \in M\}$ and $S' := \{t_y \cdot g \cdot t_{yg}^{-1} \in G; y \in X, g \in M^{-1}\}$. For $y \in X$ and $g \in M$ we have $(t_y \cdot g \cdot t_{yg}^{-1})^{-1} = t_{yg} \cdot g^{-1} \cdot t_y^{-1}$, implying $S^{-1} \subseteq S'$ and by symmetry $S^{-1} = S'$, hence $\langle S \rangle = \langle S, S' \rangle \leq \mathrm{Stab}_G(x)$.

Let $1 \neq h = g_1 \cdot \cdots \cdot g_r \in \mathrm{Stab}_G(x)$ where $r \in \mathbb{N}$ and $g_i \in M \cup M^{-1}$, let $t_1 := 1 \in T$ as well as $t_{i+1} := t_{xt_ig_i} \in T$ and $s_i := t_i g_i t_{i+1}^{-1} \in S \cup S'$ for $i \in \{1, \ldots, r\}$. Hence $s_1 \cdot \cdots \cdot s_r = t_1 g_1 t_2^{-1} \cdot t_2 g_2 t_3^{-1} \cdot \cdots \cdot t_r g_r t_{r+1}^{-1} = h t_{r+1}^{-1} \in \mathrm{Stab}_G(x)$, and from $h \in \mathrm{Stab}_G(x)$ we get $t_{r+1} \in T \cap \mathrm{Stab}_G(x) = \{1\}$, hence $h = s_1 \cdot \cdots \cdot s_r \in \langle S, S' \rangle$, implying $\langle S \rangle = \langle S, S' \rangle = \mathrm{Stab}_G(x)$. $\sharp$

(3.9) Algorithm: Orbit-stabiliser.
Let $G = \langle M \rangle$ be a group, where $M \subseteq G$ is finite, let X be G-set, and let $x \in X$. If $xG \subseteq X$ is finite, then xG is enumerated, and a transversal of xG and a generating set of $\mathrm{Stab}_G(x)$ are found as follows:

```
• $Y \leftarrow [x]$    # orbit
○ $T \leftarrow [1]$    # transversal
○ $S \leftarrow []$    # stabiliser
• $i \leftarrow 1$
• while $i \leq$ length($Y$) do
```

```
    • for $g \in M$ do
        • $z \leftarrow Y[i] \cdot g$
        • if $z \notin Y$ then
            • append$(Y, z)$
            ◦ append$(T, T[i] \cdot g)$
        ◦ else
            ◦ $j \leftarrow$ position$(Y, z)$
            ◦ append$(S, T[i] \cdot g \cdot T[j]^{-1})$
    • $i \leftarrow i + 1$
• return $[Y, T, S]$
```

At any time we have $Y \subseteq xG \subseteq X$, where the elements of Y are pairwise distinct. Since xG is finite the algorithm terminates. Letting $\varphi\colon G \to \mathcal{S}_{xG}\colon g \mapsto \overline{g}$ be the associated action homomorphism, any $\overline{g} \in \mathrm{im}(\varphi)$ can be written as $\overline{g} = \overline{g_1} \cdot \dots \cdot \overline{g_r}$ where $r \in \mathbb{N}_0$ and $g_i \in M$. Induction on r shows that on termination we have $xG \subseteq Y$. At any time we for all $i \leq \mathsf{length}(Y)$ have $xT[i] = Y[i]$, hence $S \subseteq \mathrm{Stab}_G(x)$, and on termination we have $\langle S \rangle = \mathrm{Stab}_G(x)$. ♯

4 Sylow's Theorem

(4.1) Definition. Let p be a prime.
a) A finite group G such that $|G| = p^d$ for some $d \in \mathbb{N}_0$ is called a ***p*-group**.
b) A p-subgroup $P \leq G$ of a finite group G such that $p \not| [G\colon P] = \frac{|G|}{|P|}$ is called a **Sylow *p*-subgroup** of G. Let $\mathrm{Syl}_p(G)$ be the set of Sylow p-subgroups of G; if $p \not| |G|$ then we have $\mathrm{Syl}_p(G) = \{\{1\}\}$.

(4.2) Theorem. Let p be a prime, let G be a p-group, and let $\{1\} \neq N \trianglelefteq G$. Then we have $Z(G) \cap N \neq \{1\}$. In particular we have $Z(G) \neq \{1\}$.

Proof. The normal subgroup $N \trianglelefteq G$ consists of a union of G-conjugacy classes. Let $T \subseteq G$ be a set of representatives of these classes. Since $Z(G)$ consists of the conjugacy classes of length 1, we have $Z(G) \cap N = Z(G) \cap T$ and thus $|N| = |Z(G) \cap N| + \sum_{x \in T \setminus Z(G)} \frac{|G|}{|C_G(x)|}$. For all $x \in G \setminus Z(G)$ we have $1 \neq \frac{|G|}{|C_G(x)|} \mid |G|$, which is a p-power, and hence $p \mid |N|$ implies $p \mid |Z(G) \cap N|$. ♯

(4.3) Theorem: Sylow (1872).
Let p be a prime, and let G be a finite group.
a) If $p^d \mid |G|$ for some $d \in \mathbb{N}$, then $N_d := |\{Q \leq G; |Q| = p^d\}| \equiv 1 \pmod{p}$.
b) Let $P \in \mathrm{Syl}_p(G)$ and $Q \leq G$ be a p-subgroup. Then $Q^g \leq P$ for some $g \in G$.

In particular, we have $\mathrm{Syl}_p(G) \neq \emptyset$, all Sylow p-subgroups are conjugate in G, all normalisers of Sylow p-subgroups are conjugate in G, and $|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}$ as well as $|\mathrm{Syl}_p(G)| = [G\colon N_G(P)] = \frac{|G|}{|N_G(P)|} \mid \frac{|G|}{|P|}$.

Proof: Wielandt (1959).
a) G acts on $X := \{M \subseteq G; |M| = p^d\}$ by right multiplication. Let $X = \coprod_{i\in\mathcal{I}} X_i$ be its decomposition into G-orbits, where $\mathcal{I}$ is an index set, let $\{M_i \subseteq G; i \in \mathcal{I}\}$ be a set of orbit representatives, and let $G_i := \mathrm{Stab}_G(M_i) \leq G$. From $M_iG_i = M_i \subseteq G$ we conclude that M_i is a union of left cosets of G_i in G, and thus $|G_i| \mid |M_i| = p^d$. Hence we have $|G_i| = p^{d_i}$ for some $d_i \in \{0,\ldots,d\}$.

If $Q \leq G$ such that $|Q| = p^d$, then $|\mathrm{Stab}_G(Q)| = |Q| = p^d$, and hence $Q \in X_i$ for some $i \in \mathcal{I}$ such that $d_i = d$. If $Q, Q' \leq G$ such that $|Q| = p^d = |Q'|$ are in the same G-orbit, then $Q' = Qg$ for some $g \in G$, thus $g \in Q'$, and hence $Q = Q'g^{-1} = Q'$. If $i \in \mathcal{I}$ such that $d_i = d$, then from $|M_i| = p^d = |G_i|$ we infer $M_i = g_iG_i$ for some $g_i \in G$. Thus for $M_ig_i^{-1} \in X_i$ we have $M_ig_i^{-1} = g_iG_ig_i^{-1} \leq G$. In conclusion, there is a bijection between the subgroups $Q \leq G$ such that $|Q| = p^d$ and the G-orbits X_i such that $d_i = d$.

If $d_i < d$, then $|X_i| = \frac{|G|}{|G_i|} = \frac{|G|}{p^{d_i}} \equiv 0 \pmod{\frac{|G|}{p^{d-1}}}$, yielding $\binom{|G|}{p^d} = |X| = \sum_{i\in\mathcal{I}} |X_i| \equiv \sum_{i\in\mathcal{I};d_i=d} \frac{|G|}{p^d} = N_d \cdot \frac{|G|}{p^d} \pmod{\frac{|G|}{p^{d-1}}}$. In particular for the cyclic group $C_{|G|}$ we from $|\{Q \leq C_{|G|}; |Q| = p^d\}| = 1$ get $\binom{|G|}{p^d} \equiv \frac{|G|}{p^d} \pmod{\frac{|G|}{p^{d-1}}}$. This yields $\frac{|G|}{p^d} \equiv N_d \cdot \frac{|G|}{p^d} \pmod{\frac{|G|}{p^{d-1}}}$, thus $\frac{|G|}{p^{d-1}} \mid \frac{|G|}{p^d} \cdot (N_d - 1)$, hence $p \mid (N_d - 1)$.

b) Q acts by right multiplication on $P\backslash G$, and the associated orbits $PgQ \subseteq G$, where $g \in G$, are called **P-Q-double cosets**. Let $G = \coprod_{i\in\mathcal{I}} Pg_iQ$, where $\mathcal{I}$ is an index set and $g_i \in G$. For $h \in Q$ we have $Pgh = Pg$ if and only if $ghg^{-1} \in P$, thus $\mathrm{Stab}_Q(Pg) = Q \cap P^g$, hence $|G| = \sum_{i\in\mathcal{I}} |Pg_iQ| = \sum_{i\in\mathcal{I}} \frac{|Q|}{|Q\cap P^{g_i}|} \cdot |P|$. Assume that $Q \cap P^{g_i} < Q$ for all $i \in \mathcal{I}$, then $p \mid \frac{|Q|}{|Q\cap P^{g_i}|}$, hence $p \mid \frac{|G|}{|P|}$, a contradiction. Thus there is $i \in \mathcal{I}$ such that $Q \cap P^{g_i} = Q$, implying $Q \leq P^{g_i}$. ♯

(4.4) Corollary: Cauchy's Theorem.
If $p \mid |G|$ then G possesses an element of order p. Thus G is a p-group if and only if any element of G has p-power order.

(4.5) Corollary: Frattini argument.
a) Let $P \in \mathrm{Syl}_p(G)$ and $N_G(P) \leq U \leq G$. Then we have $N_G(U) = U$.
b) Let $N \trianglelefteq G$ and $P \in \mathrm{Syl}_p(N)$. Then we have $N_G(P)N = G$.

Proof. a) Let $g \in N_G(U)$, then we have $P^g \leq N_G(P)^g \leq U^g = U$. Since $P, P^g \in \mathrm{Syl}_p(U)$ there is $h \in U$ such that $P^g = P^h$. Hence we have $gh^{-1} \in N_G(P) \leq U$ and thus $g \in U$, implying $N_G(U) \leq U$.
b) Let $g \in G$, then we have $P, P^g \in \mathrm{Syl}_p(N)$. Thus there is $h \in N$ such that $P^g = P^h$, hence $gh^{-1} \in N_G(P)$ and $g \in N_G(P)N$, implying $G \leq N_G(P)N$. ♯

(4.6) Theorem: Brodkey (1963).
Let p be a prime, let G be a finite group, and let $P \in \mathrm{Syl}_p(G)$ be abelian. Then there is $P' \in \mathrm{Syl}_p(G)$ such that $P \cap P' = O_p(G) := \bigcap_{Q\in\mathrm{Syl}_p(G)} Q \trianglelefteq G$.

Proof. It is immediate that $O_p(G) \trianglelefteq G$ is the largest normal p-subgroup of G, and that for any $Q \in \mathrm{Syl}_p(G)$ we have $Q/O_p(G) \in \mathrm{Syl}_p(G/O_p(G))$. We proceed by induction on $|G|$, and hence we may assume that $O_p(G) = \{1\}$. Moreover we may assume that $p \mid |G|$, and hence let $r \in \mathbb{N}$ minimal such that there are $P_1, \ldots, P_r \in \mathrm{Syl}_p(G)$ such that $P \cap \bigcap_{i=1}^r P_i = \{1\}$.

Let $A := \bigcap_{i=1}^r P_i \leq H := \langle P_1, \ldots, P_r\rangle \leq G$. By conjugacy of Sylow p-subgroups we have $A \neq \{1\}$. Since the P_i are abelian we have $A \leq Z(H)$, hence $A \leq O_p(H)$, and since $P_i \in \mathrm{Syl}_p(H) \subseteq \mathrm{Syl}_p(G)$ we conclude $A \geq O_p(H)$, thus $A = O_p(H)$, and hence $H < G$. Let $Q \in \mathrm{Syl}_p(H)$ such that $P \cap H \leq Q$. Since $H < G$ by induction there is $P' \in \mathrm{Syl}_p(H) \subseteq \mathrm{Syl}_p(G)$ such that $A = O_p(H) = Q \cap P'$. Thus $P \cap P' = P \cap H \cap P' \leq P \cap Q \cap P' = P \cap A = P \cap \bigcap_{i=1}^r P_i = \{1\}$. ♯

(4.7) Example: The alternating group $\mathcal{A}_5$.

a) Let $G := \mathcal{A}_5$, hence $|G| = 60 = 2^2 \cdot 3 \cdot 5$, and G contains 24 elements of cycle type $[5]$, as well as 20 elements of cycle type $[3, 1^2]$, and 15 elements of cycle type $[2^2, 1]$, as well as the identity which has cycle type $[1^5]$. We consider the subgroups of G:

i) For any $P_5 \in \mathrm{Syl}_5(G)$ we have $P_5 \cong C_5$, thus P_5 contains 4 elements of order 5. Since has the **trivial intersection property** $P_5 \cap P_5^\pi = \{1\}$ for all $\pi \in G \setminus N_G(P_5)$, we have $|\mathrm{Syl}_5(G)| = 6$ and thus $|N_G(P_5)| = 10$. Conversely it is immediate that any subgroup $U < G$ such that $|U| = 10$ is of the form $N_G(P_5)$ for some $P_5 \in \mathrm{Syl}_5(G)$. We have $D_{10} = \langle \sigma_5, \tau_5\rangle = \langle (2,5)(3,4), (1,2,3,4,5)\rangle < G$, thus for $C_5 \cong T_5 := \langle \tau_5\rangle \lhd D_{10}$ we have $N_G(T_5) = D_{10}$.

ii) For any $P_3 \in \mathrm{Syl}_3(G)$ we have $P_3 \cong C_3$, thus P_3 contains 2 elements of order 3. Since $P_3 \cap P_3^\pi = \{1\}$ for all $\pi \in G \setminus N_G(P_3)$, we have $|\mathrm{Syl}_3(G)| = 10$ and thus $|N_G(P_3)| = 6$. Conversely it is immediate that any subgroup $U < G$ such that $|U| = 6$ is of the form $N_G(P_3)$ for some $P_3 \in \mathrm{Syl}_3(G)$. For $C_3 \cong \mathcal{A}_3 := \langle (1,2,3)\rangle < G$ we have $N_G(\mathcal{A}_3) = \langle (1,2,3), (1,2)(4,5)\rangle$, and since $N_G(\mathcal{A}_3) \to \mathcal{S}_3 \colon \pi \mapsto \pi|_{\{1,2,3\}}$ is an epimorphism we conclude $N_G(\mathcal{A}_3) \cong \mathcal{S}_3$.

iii) Let $V_4 := \langle (1,2)(3,4), (1,3)(2,4)\rangle \lhd \mathcal{A}_4 = \mathcal{S}_4 \cap \mathcal{A}_5 < \mathcal{S}_5$ be the **Klein 4-group**, hence $|V_4| = 4$, thus $V_4 \in \mathrm{Syl}_2(G)$ and $\mathcal{A}_4 \leq N_G(V_4) \leq G$. Since G has 15 elements of order 2 we have $|\mathrm{Syl}_2(G)| > 1$, implying $N_G(V_4) = \mathcal{A}_4 = \langle (1,2,3), (1,2)(3,4)\rangle$. Thus $|\mathrm{Syl}_2(G)| = 5$, and counting elements of order 2 yields $V_4 \cap V_4^\pi = \{1\}$ for all $\pi \in G \setminus N_G(V_4)$.

Conversely, let $U < G$ such that $|U| = 12$, let $P_3 \in \mathrm{Syl}_5(G)$ and $P_2 \in \mathrm{Syl}_2(G)$ such that $P_3, P_2 < U$. We have $|\mathrm{Syl}_2(U)| \mid \frac{|U|}{|P_2|} = 3$. Assume $|\mathrm{Syl}_2(U)| = 3$, then since $P_2 \cong V_4$ is a trivial intersection subgroup, U has 9 elements of order 2, and thus 2 elements of order 3, implying that $|\mathrm{Syl}_3(U)| = 1$, thus $P_3 \lhd U$, hence $U \leq N_G(P_3)$, a contradiction. We conclude that $|\mathrm{Syl}_2(U)| = 1$, thus $P_2 \lhd U$, hence $U = N_G(P_2)$.

iv) Assume there is $U < G$ such that $|U| = 15$, and let $P_5 \in \mathrm{Syl}_5(G)$ such that $P_5 < U$. From $|\mathrm{Syl}_5(U)| \mid \frac{|U|}{|P_5|} = 3$ and $|\mathrm{Syl}_5(U)| \equiv 1 \pmod 5$ we get

$|\mathrm{Syl}_5(U)| = 1$, thus $P_5 \lhd U$, hence $U \leq N_G(P_5)$, a contradiction.

Assume there is $U < G$ such that $|U| = 20$, and let $P_5 \in \mathrm{Syl}_5(G)$ such that $P_5 < U$. From $|\mathrm{Syl}_5(U)| \mid \frac{|U|}{|P_5|} = 4$ and $|\mathrm{Syl}_5(U)| \equiv 1 \pmod 5$ we get $|\mathrm{Syl}_5(U)| = 1$, thus $P_5 \lhd U$, hence $U \leq N_G(P_5)$, a contradiction.

Assume there is $U < G$ such that $|U| = 30$, then $U \lhd G$, and since $G/U \cong C_2$ we conclude that U contains all of the 24 elements of order 5 and all of the 20 elements of order 3, a contradiction.

v) Let $C_2 \cong U := \langle \tau \rangle < V_4 < N_G(V_4) = \mathcal{A}_4 < G$. Then from $C_{\mathcal{A}_4}(\tau) = V_4 < \mathcal{A}_4$ we get $\tau \notin Z(G)$, hence $U \not\trianglelefteq G$.

We conclude that G does not have non-trivial proper normal subgroups, i. e. $G = \mathcal{A}_5$ is simple. Moreover, a Sylow-type existence statement even for arbitrary divisors $d \mid |G|$ such that $\mathrm{ggT}(d, \frac{|G|}{d}) = 1$ does not hold in general.

b) We show that any simple group G of order 60 is isomorphic to $\mathcal{A}_5$: First assume that there is $U < G$ such that $|U| = 20$, then there is a monomorphism $G \rightarrow \mathcal{S}_{U\backslash G} \cong \mathcal{S}_3$, a contradiction. Moreover, letting $P \in \mathrm{Syl}_5(G)$ we have $1 \neq \frac{|G|}{|N_G(P)|} \mid 12$ and $\frac{|G|}{|N_G(P)|} \equiv 1 \pmod 5$, thus $\frac{|G|}{|N_G(P)|} = 6$. Hence there are 24 elements of order 5.

Now let $S, S' \in \mathrm{Syl}_2(G)$ such that $S \neq S'$. If $T := S \cap S' \neq \{1\}$, then $T \cong C_2$. Since S is abelian and $Z(G) = \{1\}$ we conclude $S < C_G(T) < G$, and thus $|C_G(T)| = 12$. If $S \cap S' = \{1\}$ for all $S \neq S'$, then assuming that $N_G(S) = S$ we get $|\mathrm{Syl}_2(G)| = 15$, and thus there are 45 elements having 2-power order, a contradiction. Hence we have $S < N_G(S) < G$, and thus $|N_G(S)| = 12$.

In any case there is a monomorphism $\varphi \colon G \rightarrow \mathcal{S}_5$. Assume that $\mathrm{im}(\varphi) \not\leq \mathcal{A}_5$, then $\varphi \cdot \mathrm{sgn} \colon G \rightarrow C_2$ is non-trivial, a contradiction. Thus we have $\varphi \colon G \rightarrow \mathcal{A}_5$.

c) We consider the **truncated icosahedron (Buckminsterfullerene, soccer ball)**, centred at the origin of the Euclidean space $\mathbb{R}^3$: The **icosahedron** is one of the 5 regular **platonic solids**, next to the **tetrahedron**, the **cube**, the **octahedron**, and the **dodecahedron**. The icosahedron has 20 triangular faces, and 12 vertices at each of which 5 of the faces meet. Truncating at the 12 vertices yields a regular solid having 60 vertices, and 12 pentagonal and 20 hexagonal faces, where each pentagonal face is surrounded by hexagonal ones, and each hexagonal face is surrounded by hexagonal and pentagonal ones.

We consider its group of symmetries, i. e. the group $G \leq SO_3(\mathbb{R})$ of rotations mapping the truncated icosahedron to itself. G acts on the $12 \cdot 5 = 60$ pairs of adjacent pentagon-hexagon pairs. It is immediate that G acts transitively, and that any element is uniquely determined by the image of a fixed adjacent pentagon-hexagon pair. Thus we have $|G| = 60$. There are 6 pairs of opposite pentagons, giving rise to 6 rotation axes of order 5, yielding $6 \cdot 4 = 24$ elements of order 5. There are 10 pairs of opposite hexagons, giving rise to 10 rotation axes of order 3, yielding $10 \cdot 2 = 20$ elements of order 3. Finally, there are 30 hexagon-hexagon edges, giving rise to 15 opposite pairs, yielding 15 rotation axes of order 2, hence 15 elements of order 2.

We show that $G \cong \mathcal{A}_5$: Fixing a rotation axis of order 2, there are precisely two other rotation axes of order 2 orthogonal to the given one. The associated rotations $\tau_1, \tau_2 \in G$ and $\tau_3 = \tau_1\tau_2 \in G$ generate a non-cyclic abelian subgroup $V_4 \cong V := \langle \tau_1, \tau_2 \rangle \in \mathrm{Syl}_2(G)$. Moreover, the orthogonality argument implies $V \cap V^\pi = \{1\}$ for all $\pi \in G \setminus N_G(V)$, hence counting elements of order 2 yields $|\mathrm{Syl}_2(G)| = 5$ and $|N_G(V)| = 12$. Thus the conjugation action of G on $\mathrm{Syl}_2(G)$, which is isomorphic as a G-set to $N_G(V)\backslash G$ acted on by G by right multiplication, yields a homomorphism $\varphi\colon G \to \mathcal{S}_5$. We show that φ is injective such that $\mathrm{im}(\varphi) \leq \mathcal{A}_5$:

There is a rotation axis of order 3 such that conjugation with the associated rotation $\rho \in G$ yields $\kappa_\rho\colon \tau_1 \mapsto \tau_2 \mapsto \tau_3 \mapsto \tau_1$. Hence $N_G(V) = \langle \rho, V \rangle \cong \langle \rho \rangle \ltimes_\kappa V$, a **semidirect product**. It is immediate that $N_G(V) \to \mathcal{A}_4\colon \rho \mapsto (1,2,3), \tau_1 \mapsto (1,2)(3,4), \tau_2 \mapsto (1,4)(2,3)$ is an isomorphism. Hence $N_G(V)$ is generated by elements of order 3. Joining an element of order 5 shows that G is generated by elements of odd order, thus $\mathrm{im}(\varphi) \leq \mathcal{A}_5$. We have $\ker(\varphi) = \bigcap_{\pi \in G} N_G(V)^\pi \trianglelefteq N_G(V) \cong \mathcal{A}_4$. Since $V \triangleleft N_G(V)$ is the only non-trivial proper normal subgroup of $N_G(V)$, and since for $\pi \in G \backslash N_G(V)$ we have $V \cap N_G(V)^\pi = V \cap V^\pi = \{1\}$, we conclude $V \cap \ker(\varphi) = \{1\}$ and thus $\ker(\varphi) = \{1\}$.

5 Primitivity

(5.1) Definition. Let G be a group, and let X be a transitive G-set. A subset $\emptyset \neq B \subseteq X$ such that $Bg = B$ or $Bg \cap B = \emptyset$ for all $g \in G$ is called a **block**. The set X and the subsets $\{x\} \subseteq X$ are called the **trivial** blocks; if these are the only blocks then X is called **primitive**, and **imprimitive** otherwise.

The transitive G-set $\mathcal{B} := \{Bg \subseteq X; g \in G\}$ is called the associated **block system**. It is immediate that $\mathcal{B}$ partitions X, and we have a natural homomorphism of G-sets $X \to \mathcal{B}$ mapping each element of X to the block it is contained in. Using the **block stabiliser** $\mathrm{Stab}_G(B) = G_B := \{g \in G; Bg = B\} \leq G$ we have $X = \coprod_{g \in \mathrm{Stab}_G(B)\backslash G} Bg$. If X is finite then we have $|X| = |B| \cdot [G\colon \mathrm{Stab}_G(B)]$; in particular if $|X|$ is a prime then G acts primitively.

(5.2) Proposition. Let G be a group, let X be a transitive G-set, and let $x \in X$. Then the map $\beta\colon \{H \leq G; \mathrm{Stab}_G(x) \leq H\} \to \{B \subseteq X \text{ block}; x \in B\}\colon H \mapsto xH$ is an inclusion-preserving bijection with inverse map $\beta^{-1}\colon B \mapsto \mathrm{Stab}_G(B)$.

In particular, any block $B \subseteq X$ is a transitive $\mathrm{Stab}_G(B)$-set, and if $|X| \geq 2$ then X is primitive if and only if $\mathrm{Stab}_G(x) < G$ is a maximal subgroup.

Proof. Let $y \in xH \cap xHg$ for some $g \in G$. Then there are $h, h' \in H$ such that $y = xh = xh'g$, hence $h'gh^{-1} \in \mathrm{Stab}_G(x) \leq H$, implying $g \in H$ and $xH = xHg$. Thus xH is a block, showing that β is well-defined. Conversely, from $x \in B$ we get $\mathrm{Stab}_G(x) \leq \mathrm{Stab}_G(B)$, showing that β^{-1} is well-defined.

If for $g \in G$ we have $xHg = xH$, then in particular there is $h \in H$ such that $gh^{-1} \in \mathrm{Stab}_G(x) \leq H$, implying that $g \in H$. Since $xHh = xH$ for all $h \in H$ we conclude $\mathrm{Stab}_G(xH) = H$ and thus $\beta\beta^{-1} = \mathrm{id}$. Conversely, for a block $B \subseteq X$ and $x, x' \in B$ there is $g \in G$ such that $xg = x'$. Hence $Bg \cap B \neq \emptyset$, implying $Bg = B$, thus $g \in \mathrm{Stab}_G(B)$. Hence $B = x\mathrm{Stab}_G(B) \subseteq X$, thus $\beta^{-1}\beta = \mathrm{id}$. ♯

(5.3) Proposition. Let G be a group, let $N \trianglelefteq G$, and let X be a transitive G-set. Then the N-orbits in X form a block system for G.

In particular, if X is a primitive faithful G-set and $N \neq \{1\}$ then N is transitive.

Proof. Let $B \subseteq X$ be an N-orbit. From $Bgn = Bgng^{-1} \cdot g = Bg$ for all $n \in N$ we conclude that Bg is a union of N-orbits, for $g \in G$. For $x, x' \in Bg$ there is $n \in N$ such that $xg^{-1}n = x'g^{-1}$, thus $xg^{-1}ng = x'$, hence Bg is an N-orbit. ♯

(5.4) Definition and Remark. a) Let G be a group, let $U \leq G$, and let $X := U \backslash G$; hence G acts on X by right multiplication. Let $T := \{t_x \in G; x \in X\} \subseteq G$ be a transversal of U in G, and for $g \in G$ and $x \in X$ let $u_{x,g} := t_x g t_{xg}^{-1} \in U$.

Let H be a group, and let $H^X := \{f \colon X \to H\}$, which is a group by pointwise multiplication and called the X-fold **direct product** of H with itself. Let $\tau \colon U \to \mathrm{Aut}(H)$ be a homomorphism. Then G acts on H^X by $f \mapsto f^g \colon x \mapsto (xg^{-1}f)^{u_{xg^{-1},g}}$, where the U-action on H is given by τ, but omitted from the notation: For all $g, h \in G$ we have $u_{xh^{-1}g^{-1},g} \cdot u_{xh^{-1},h} = u_{xh^{-1}g^{-1}} g u_{xh^{-1}}^{-1} \cdot u_{xh^{-1}} h u_x^{-1} = u_{xh^{-1}g^{-1}} gh u_x^{-1} = u_{xh^{-1}g^{-1},gh}$, hence $x(f^g)^h = (xh^{-1}f^g)^{u_{xh^{-1},y}} = (xh^{-1}g^{-1}f)^{u_{xh^{-1}g^{-1},g} \cdot u_{xh^{-1},h}} = (xh^{-1}g^{-1}f)^{u_{xh^{-1}g^{-1},gh}} = xf^{gh}$ for all $x \in X$.

We have $x(ff')^g = (xg^{-1}ff')^{u_{xg^{-1},g}} = (xg^{-1}f)^{u_{xg^{-1},g}} \cdot (xg^{-1}f')^{u_{xg^{-1},g}} = x(f^g f'^g)$, yielding a homomorphism $\widehat{\tau} \colon G \to \mathrm{Aut}(H^X)$. The semidirect product $H \wr_{X,\tau} G := G \ltimes_{\widehat{\tau}} H^X$ is called the associated **twisted wreath product**. If τ is trivial, then $H \wr_X G$ is called the associated **(ordinary) wreath product**.

We show independence of the choice of the transversal T: Let $T' := \{t'_x \in G; x \in X\}$ be a transversal of U in G, hence we have $t'_x := u_x t_x \in G$ where $u_x \in U$. Then for all $g \in G$ we have $u'_{x,g} = u_x t_x g t_{xg}^{-1} u_{xg}^{-1} = u_x u_{x,g} u_{xg}^{-1} \in U$, and $\gamma := \prod_{x \in X} (u_x^{-1})^\tau \in \prod_{x \in X} \mathrm{Aut}(H) \leq \mathrm{Aut}(H^X)$, thus $f^{\gamma^{-1} g \gamma} \colon x \mapsto (xg^{-1}f^{\gamma^{-1}})^{u_{xg^{-1},g} \cdot u_x^{-1}} = (xg^{-1}f)^{u_{xg^{-1}} u_{xg^{-1},g} u_x^{-1}} = (xg^{-1}f)^{u'_{xg^{-1},g}}$. From this it is immediate that the semidirect products afforded by T and T' are isomorphic.

b) Let Y be an H-set. Then the wreath product $H \wr_X G$ acts on $X \times Y$ by the **standard action** $[x, y](g, f) := [xg, y^{(xgf)}]$: For all $g, h \in G$ and $f, f' \in H^X$ we have $[x, y](g, f)(h, f') = [xg, y^{(xgf)}](h, f') = [xgh, (y^{(xgf)})^{(xghf')}] = [xgh, y^{(xgf)(xghf')}] = [xgh, y^{(xghf^h)(xghf')}] = [xgh, y^{xgh(f^h f')}] = [x, y](gh, f^h f')$.

If X and Y are faithful then so is $X \times Y$: If $[x, y] = [x, y](g, f) = [xg, y^{(xgf)}]$ for all $[x, y] \in X \times Y$, then we have $g \in \ker(\varphi_X) = \{1\}$, where $\varphi_X \colon G \to \mathcal{S}_X$ is the action homomorphism associated to X, and thus $xgf = xf \in \ker(\varphi_Y) = \{1\}$

for all $x \in X$, where $\varphi_Y \colon H \rightarrow \mathcal{S}_Y$ is the action homomorphism associated to Y, hence we have $f = 1$ as well.

If Y is transitive, then so is $X \times Y$: Let $[x, y], [x', y'] \in X \times Y$, and let $g \in G$ such that $xg = x'$ and $h \in H$ such that $yh = y'$. Letting $f \in H^X$ such that $xgf = h$ yields $[x, y](g, f) = [xg, y^{(xgf)}] = [x', yh] = [x', y']$.

(5.5) Proposition. Let G be a group, let X be a transitive G-set with associated action homomorphism φ_X, let $\mathcal{B}$ be a block system, and let $B \in \mathcal{B}$ be a block. Then there is a homomorphism $\beta \colon G \rightarrow \mathcal{S}_B \wr_{\mathcal{B}} \mathcal{S}_{\mathcal{B}}$, such that the G-actions φ_X and $\beta \cdot \varphi_{\mathcal{B} \times B}$ are isomorphic, where $\varphi_{\mathcal{B} \times B}$ is the action homomorphism associated to the standard action of $\mathcal{S}_B \wr_{\mathcal{B}} \mathcal{S}_{\mathcal{B}}$.

Proof. Let $T \subseteq G$ be a transversal of $U := \mathrm{Stab}_G(B)$ in G. Then we have a bijection $\iota \colon X \rightarrow \mathcal{B} \times B \colon x \mapsto [Bt, xt^{-1}]$, where $t \in T$ such that $x \in Bt$. Let φ_B be the restriction of $(\varphi_X)|_U$ to the transitive U-set B, and let $\varphi_{\mathcal{B}}$ be the action homomorphism associated to the transitive G-set $\mathcal{B}$, being induced by the natural map $X \rightarrow \mathcal{B}$. Then let $\beta \colon G \rightarrow \mathcal{S}_B \wr_{\mathcal{B}} \mathcal{S}_{\mathcal{B}} \colon g \mapsto (g\varphi_{\mathcal{B}}, (\mathcal{B} \rightarrow \mathcal{S}_B \colon Bt \mapsto u_{Btg^{-1},g}\varphi_B))$, the wreath product being formed with respect to T.

We show that ι induces an isomorphism between the G-actions φ_X and $\beta \cdot \varphi_{\mathcal{B} \times B}$; it then follows from the injectivity of $\varphi_{\mathcal{B} \times B}$ that β indeed is a homomorphism: Let $x \in X$ and $g \in G$, let $t \in T$ such that $x \in Bt$, and let $t' \in T$ such that $Btg = Bt'$, hence $xg \in Bt'$. Then the standard action yields $(x\iota)^{(g\beta)} = [Bt, xt^{-1}](g\beta) = [Btg, xt^{-1}u_{Bt,g}] = [Btg, xg(t')^{-1}] = (xg)\iota$. ♯

(5.6) Definition and Remark. a) Let G be a group, let X be a G-set, and let $k \in \mathbb{N}$. If $X^{(k)} := \{[x_1, \ldots, x_k] \in X^k; x_i \neq x_j \text{ for } i \neq j\}$ is a transitive G-set, where we let $[x_1, \ldots, x_k]g := [x_1 g, \ldots, x_k g]$ for all $g \in G$, then X is called ***k*-fold transitive**. Hence X is 1-fold transitive if and only if X is transitive.

It is immediate that X is k-fold transitive, where $k \geq 2$, if and only if X is transitive and $\mathrm{Stab}_G(x)$ acts $(k-1)$-fold transitively on $X \setminus \{x\}$, for some and hence for all $x \in X$. In particular, if $|G|$ and $|X|$ are finite and X is k-fold transitive, where $k \in \mathbb{N}$, then $\frac{|X|!}{(|X|-k)!} \mid |G|$.

b) If X is k-fold transitive and $\mathrm{Stab}_G([x_1, \ldots, x_k]) = \{1\}$ for some and hence for all $[x_1, \ldots, x_k] \in X^{(k)}$, then X is called **sharply** k-fold transitive. If X is sharply (1-fold) transitive, then X is called **regular**; in this case the map $G \rightarrow X \colon g \mapsto xg$ is a bijection for any $x \in X$.

c) If X is 2-fold transitive then X is primitive: Let $B \subseteq X$ be a block, let $x \neq x' \in B$, and let $x'' \in X$. Then there is $g \in G$ such that $xg = g$ and $x'g = x''$, implying that $x'' \in B$, and hence $B = X$.

(5.7) Lemma: Rudio (1888).
Let G be a group, and let X be a finite transitive G-set.

a) Let $\emptyset \neq Y \subset X$ and $y \in Y$ as well as $y \neq x \in X$. If X is primitive, then there is $g \in G$ such that $y \in Yg$ and $x \notin Yg$.
b) Let $H \leq G$, and let $Y \subseteq X$ be a primitive H-set such that $|Y| > \frac{|X|}{2}$. Then X is primitive.

Proof. **a)** Let $B := \bigcap\{Yg \subseteq X; g \in G; y \in Yg\}$. We show that $B \subseteq X$ is a block for G, which since $y \in B \subseteq Y \subset X$ implies $B = \{y\}$: Let $h \in G$ such that $B \cap Bh \neq \emptyset$. If $y \in Bh = \bigcap\{Ygh \subseteq X; g \in G, y \in Yg\}$, then we have $B \subseteq Bh$, and thus by finiteness $B = Bh$. Now let $z \in B \cap Bh$, and let $g \in G$ such that $yg = z$. Hence we have $y \in B \cap Bg^{-1} \cap Bhg^{-1}$, by the above implying $Bg^{-1} = B = Bhg^{-1}$ and hence $B = Bh$.
b) Let $B \subseteq X$ be a block for G such that $B \cap Y \neq \emptyset$. Hence $B \cap Y \subseteq Y$ is a block for H. Thus $|B \cap Y| \geq 2$ implies $B \cap Y = Y$, hence $|B| \geq |Y| > \frac{|X|}{2}$ and $B = X$. Thus we may assume that $|Bg \cap Y| \leq 1$ for all $g \in G$, implying $|\{Bg; g \in G\}| \geq |Y| > \frac{|X|}{2}$, hence $|\{Bg; g \in G\}| = |X|$ and $|B| = 1$. ♯

(5.8) Theorem: Jordan (1871).
Let G be a group, let X be a finite primitive G-set, let $X = Y \,\dot\cup\, Z$ such that $2 \leq |Y| < |X|$, and assume that $H := \bigcap_{x \in Z} \mathrm{Stab}_G(x) \leq G$ acts primitively on Y. Then G acts $(|X| - |Y| + 1)$-fold transitively on X.

Proof. We first show that G acts 2-**fold primitively** on X, i. e. G acts 2-fold transitively where $\mathrm{Stab}_G(x)$ acts primitively on $X \setminus \{x\}$ for $x \in X$. We proceed by induction on $|Z| \in \mathbb{N}$, where for $Z = \{z\}$ the stabiliser $H = \mathrm{Stab}_G(z)$ acts primitively on $Y = X \setminus \{z\}$. Letting $|Z| \geq 2$ we distinguish two cases:

i) Let $|Y| > \frac{|X|}{2}$, and let $y, z \in Z$ such that $y \neq z$. Hence by Rudio's Lemma there is $g \in G$ such that $z \in Zg$ and $y \notin Zg$. We have $X = (Y \cup Yg) \,\dot\cup\, (Z \cap Zg)$, where since $z \in Z \cap Zg$ and $y \notin Z \cap Zg$ we have $1 \leq |Z \cap Zg| < |Z|$. Let $K := \langle H, H^g \rangle \leq \bigcap_{x \in Z \cap Zg} \mathrm{Stab}_G(x) \leq G$, hence K acts on $Y \cup Yg$. From $|Y| > \frac{|X|}{2}$ we infer $Y \cap Yg \neq \emptyset$. Since H acts transitively on Y we conclude that K acts transitively on $Y \cup Yg$, and since H acts primitively on Y where $|Y| > \frac{|Y \cup Yg|}{2}$ we conclude that K acts primitively on $Y \cup Yg$.

ii) Let $|Y| \leq \frac{|X|}{2}$, and let $y, z \in Y$ such that $y \neq z$. Hence by Rudio's Lemma there is $g \in G$ such that $y \in Yg$ and $z \notin Yg$. We have $X = (Y \cup Yg) \,\dot\cup\, (Z \cap Zg)$, where since $y \in Y \cap Yg$ we have $|Y \cup Yg| < 2|Y| \leq |X|$, and hence from $z \in Y \setminus Yg$ we infer $Y \subset Y \cup Yg \subset X$, and thus $1 \leq |Z \cap Zg| < |Z|$. Let $K := \langle H, H^g \rangle \leq \bigcap_{x \in Z \cap Zg} \mathrm{Stab}_G(x) \leq G$, hence K acts on $Y \cup Yg$. Since $y \in Y \cap Yg$ and H acts transitively on Y we conclude that K acts transitively on $Y \cup Yg$, and since H acts primitively on Y where $|Y| > \frac{|Y \cup Yg|}{2}$ we conclude that K acts primitively on $Y \cup Yg$.

This by induction shows the above assertion. We now proceed by induction on $|Z| = |X| - |Y| \in \mathbb{N}$; for $|Z| = 1$ the group G acts 2-fold transitively by the above assertion. Let $|Z| \geq 2$, and let $z \in Z$, hence we have $X \setminus \{z\} = Y \,\dot{\cup}\, (Z \setminus \{z\})$. Since G acts 2-fold primitively we conclude that $\mathrm{Stab}_G(z)$ acts primitively on $X \setminus \{z\}$, implying that $\mathrm{Stab}_G(z)$ acts $(|X| - |Y|)$-fold transitively on $X \setminus \{z\}$. $\sharp$

(5.9) Corollary: Jordan (1871).
Let G be a finite group, and let X be a primitive faithful G-set.
a) If G contains a transposition, then we have $G \cong \mathcal{S}_X$.
b) If G contains a 3-cycle, then we have $\mathcal{A}_X \leq G$.

Proof. a) For $|Y| = 2$ we get $(|X| - 1)$-fold transitivity, implying $|X|! \mid |G|$.
b) For $|Y| = 3$ we get $(|X| - 2)$-fold transitivity, implying $\frac{|X|!}{2} \mid |G|$. It follows from (6.5), and by inspection for $n \leq 4$, that $\mathcal{A}_n \lhd \mathcal{S}_n$ for any $n \geq 2$ is the only subgroup of index 2. $\sharp$

6 Multiple transitivity

(6.1) Theorem. Let G be a group, and let X be a sharply 4-fold transitive faithful G-set. Then we have $|X| \in \{4, 5, 6, 11\}$.

Proof: Tits (1952).
i) We may assume that $\{1, 2, 3, 4\} \subseteq X$, and let $t \in G$ be the uniquely determined element such that $t = (1, 2)(3)(4) \cdot \cdots \in \mathcal{S}_X$. Hence we have $t^2 \in \bigcap_{i=1}^4 \mathrm{Stab}_G(i) = \{1\}$, and since $\{3, 4\} \subseteq \mathrm{Fix}_X(t)$ we have $|\mathrm{Fix}_X(t)| \in \{2, 3\}$. Let $H := C_G(t) \cap \mathrm{Stab}_G(1) = C_{\mathrm{Stab}_G(1)}(t)$. It is immediate that $H \leq C_G(t)$ acts on $\mathrm{Fix}_X(t)$, as well as on the set $\mathcal{C} := \{\{i, j\} \subseteq X; i \neq it = j\}$ of 2-cycles of t. Since $H \leq \mathrm{Stab}_G(1)$ we have $1^H = 1$ and thus $2^H = 2$, and since $\{3, 4\} \subseteq \mathrm{Fix}_X(t)$ we conclude that H acts faithfully on $\mathrm{Fix}_X(t)$, hence $|H| \leq 6$.

Since $\{1, 2\}^H = \{1, 2\}$ we infer that H also acts on $\mathcal{C}' := \mathcal{C} \setminus \{\{1, 2\}\}$, provided $\mathcal{C}' \neq \emptyset$. In this case let $i, j, k, l \in X \setminus \{1, 2\}$ such that $\{i, j\}, \{k, l\} \in \mathcal{C}'$, i. e. we have $t = (1, 2)(3)(4) \cdot \cdots \cdot (i, j) \cdot \cdots \cdot (k, l) \cdot \cdots$, and let $g \in G$ be the uniquely determined element such that $1g = 1$ and $2g = 2$ as well as $ig = k$ and $jg = l$. Then we have $t^g = (1, 2) \cdot \cdots \cdot (k, l) \cdot \cdots$, implying that $t^g = t$ and thus $g \in H$, hence H acts transitively on $\mathcal{C}'$. Let $h \in G$ be the uniquely determined element such that $1h = 1$ and $2h = 2$ as well as $ih = j$ and $jh = i$. Then we have $t^h = (1, 2) \cdot \cdots \cdot (i, j) \cdot \cdots$, hence $t^h = t$ and $h \in H$. Since $h^2 = 1$ we infer $2 \mid |\mathrm{Stab}_H(\{i, j\})|$. Thus we have $|\mathcal{C}'| \leq 3$, implying that $|X| = |\mathrm{Fix}_X(t)| + 2 \cdot |\mathcal{C}'| + 2 \leq 11$. Moreover, if $|X|$ is even then we have $|\mathrm{Fix}_X(t)| = 2$, implying that $|H| = 2$ and thus $|\mathcal{C}'| \leq 1$ and $|X| \leq 6$.

ii) Assume we have $|X| \in \{7, 9\}$, then $|X| = p + 2$ for some prime $p \geq 5$. Let $P \in \mathrm{Syl}_p(G)$. From $|G| = (p + 2)(p + 1)p(p - 1)$ we infer $P = \langle s \rangle \cong C_p$, where we may assume $X = \{1, \ldots, p + 2\}$ and $s := (1, \ldots, p)(p + 1)(p + 2) \in \mathcal{S}_X$. It is immediate that for any $g \in C_G(s)$ we have $g = (1, \ldots, p)^k(p + 1)(p + 2)$ or $g = (1, \ldots, p)^k(p + 1, p + 2)$, for some $k \in \{0, \ldots, p - 1\}$. From $P \leq C_G(P)$ we thus get $p \mid |C_G(P)| \mid 2p$. Then from $[N_G(P) \colon C_G(P)] \mid |\mathrm{Aut}(P)| =$

$|(\mathbb{Z}/p\mathbb{Z})^*| = p-1$ we obtain $p \mid |C_G(P)| \mid |N_G(P)| \mid 2p(p-1)$, implying $\frac{(p+2)(p+1)}{2} \mid [G\colon N_G(P)] \mid 2(p-1)\cdot\frac{(p+2)(p+1)}{2}$.

Assume there is $1 \neq n \mid 2(p-1)$ such that $n \equiv 1 \pmod p$, then we have $n = p+1 = 2(p-1)$, implying $p=3$, a contradiction. Hence from $\frac{(p+2)(p+1)}{2} \equiv 1 \pmod p$ and $[G\colon N_G(P)] \equiv 1 \pmod p$ we get $[G\colon N_G(P)] = \frac{(p+2)(p+1)}{2}$, and thus $|N_G(P)| = 2p(p-1)$. This implies $2 \mid 2p \mid |C_G(P)|$, thus $C_G(P) \leq G$ contains the transposition $(p+1,p+2) \in \mathcal{S}_X$. For $i \neq j \in X$ let $g \in G$ such that $(p+1)g = i$ and $(p+2)g = j$, then we have $(p+1,p+2)^g = (i,j)$. Hence $G \leq \mathcal{S}_X$ contains all transpositions, thus $G \cong \mathcal{S}_{p+2}$, a contradiction. ♯

(6.2) Remark. a) The above case indeed occur, and by **Jordan's Theorem** (1870) the sharply 4-fold transitive finite groups are given as follows: **i)** For $|X| = 4$ we have $G \cong \mathcal{S}_4$, **ii)** for $|X| = 5$ we have $G \cong \mathcal{S}_5$, **iii)** for $|X| = 6$ we have $G \cong \mathcal{A}_6$, and **iv)** for $|X| = 11$ we have $G \cong M_{11}$, one of the **sporadic simple Mathieu groups**. By **extension theory** of transitive actions all sharply k-fold transitive finite groups for $k \geq 4$ can be classified; see also (b).

The sharply 3-fold transitive finite groups are as follows (**Zassenhaus**, 1936):
i) The **projective linear group** $\mathrm{PGL}_2(\mathbb{F}_q) := \mathrm{GL}_2(\mathbb{F}_q)/Z(\mathrm{GL}_2(\mathbb{F}_q))$, where q is any prime power and $Z(\mathrm{GL}_2(\mathbb{F}_q)) = \{\alpha E_2 \in \mathrm{GL}_2(\mathbb{F}_q); \alpha \in \mathbb{F}_q^*\} \cong C_{q-1}$,
ii) G is such that $\mathrm{PSL}_2(\mathbb{F}_{q^2}) \lhd G$ has index 2, where q is an odd prime power, $\mathrm{PSL}_2(\mathbb{F}_q) := \mathrm{SL}_2(\mathbb{F}_q)/Z(\mathrm{SL}_2(\mathbb{F}_q))$ is the **projective special linear group**, where since q is odd we have $Z(\mathrm{SL}_2(\mathbb{F}_q)) = \{\alpha E_2 \in \mathrm{SL}_2(\mathbb{F}_q); \alpha \in \mathbb{F}_q^*, \alpha^2 = 1\} \cong C_2$, and the outer automorphism of $\mathrm{PSL}_2(\mathbb{F}_{q^2})$ induced by G is the product of the commuting automorphisms of order 2 induced by $\mathrm{PSL}_2(\mathbb{F}_{q^2}) \lhd \mathrm{PGL}_2(\mathbb{F}_q)$ and by the Galois automorphism of $\mathbb{F}_q \subseteq \mathbb{F}_{q^2}$, respectively.

In both cases we have the natural action on the **projective line** $\mathbb{P}(\mathbb{F}_q^2) := \{\langle v\rangle \leq \mathbb{F}_q^2; v \neq 0\}$. In particular, for $q=3$ we have $\mathcal{A}_6 \cong \mathrm{PSL}_2(\mathbb{F}_{3^2}) \lhd G \cong \mathrm{Stab}_{M_{11}}(1)$. The sharply 2-fold transitive finite groups are classified as well (**Zassenhaus**, 1936). Finally, any finite group acts regularly on itself by right multiplication.

b) Using the type classification of primitive groups in the **O'Nan-Scott Theorem** (1979) and the classification of finite simple groups **(CFSG)** (∼1981), it can be shown that all 4-fold transitive finite groups are given as follows:
i) $\mathcal{S}_n$ for $n \geq 4$ is sharply n-fold transitive.
ii) $\mathcal{A}_n$ for $n \geq 6$ is sharply $(n-2)$-fold transitive.
iii) The **sporadic simple Mathieu groups** (1860/1873): $M_{11} < \mathcal{S}_{11}$ is sharply 4-fold transitive, $M_{12} < \mathcal{S}_{12}$ is sharply 5-fold transitive, $M_{23} < \mathcal{S}_{23}$ is (not sharply) 4-fold transitive, and $M_{24} < \mathcal{S}_{24}$ is (not sharply) 5-fold transitive.

The Mathieu group $\mathrm{Stab}_{M_{23}}(1) \cong M_{22} < \mathcal{S}_{22}$ is (not sharply) 3-fold transitive.

(6.3) Theorem. Let G be a finite group, let $N \unlhd G$, let X be a k-fold transitive faithful G-set such that N acts regularly, let $x \in X$ and $H := \mathrm{Stab}_G(x) \leq G$. Then we have $G \cong H \ltimes N$ and $k \leq 4$. Moreover:

i) If $k = 2$ then N is **p-elementary abelian**, i. e. N is abelian such that $\exp(N) \mid p$, where p is a prime.
ii) If $k = 3$ then either $N \cong C_3$ and $G \cong \mathcal{S}_3$, or N is 2-elementary abelian.
iii) If $k = 4$ then $N \cong V_4 \cong C_2^2$ and $G \cong \mathcal{S}_4$.

Proof. Since N acts regularly on X we have $H \cap N = \{1\}$. For $g \in G$ letting $n \in N$ such that $xn = xg$ shows $gn^{-1} \in H$, implying $G = HN$ and thus $G \cong H \ltimes N$. We have a bijection $\varphi\colon N^\sharp := N \setminus \{1\} \to X \setminus \{x\} \colon n \mapsto xn$. For all $h \in H$ and $n \in N^\sharp$ we have $(n^h)\varphi = xh^{-1}nh = xnh = (n\varphi)h$, hence φ is an isomorphism of H-sets, where H acts faithfully on $N^\sharp$ by conjugation.

Let $k \geq 2$. Then H acts transitively on $N^\sharp$, and thus all elements of $N^\sharp$ have the same order, which by Cauchy's Theorem is a prime p. Thus N is a p-group, and since $Z(N) \cap N^\sharp \neq \emptyset$ is H-invariant we conclude that N is abelian.

Let $|N| = |X| \geq k \geq 3$. If $|N| = |X| = k = 3$ then $N \cong C_3$ and $G \cong \mathcal{S}_3$. If $|N| \geq 4$ then assume that $p \geq 3$, let $x \in N^\sharp$ and $x^{\pm 1} \neq y \in N^\sharp$. Since $x \neq x^{-1}$ and H acts 2-fold transitively on $N^\sharp$, there is $h \in H$ such that $x^h = x$ and $(x^{-1})^h = y$, which since $(x^{-1})^h = (x^h)^{-1} = x^{-1}$ is a contradiction.

Let $|N| = |X| \geq k \geq 4$. Hence N is 2-elementary abelian. Assume that $|N| > 4$, then let $x \neq y \in N^\sharp$, hence $\langle x, y \rangle = \{1, x, y, xy\} \cong C_2^2$, and $z \in N^\sharp \setminus \{x, y, xy\}$. Since H acts 3-fold transitively on $N^\sharp$ there is $h \in H$ such that $x^h = x$ and $y^h = y$ and $(xy)^h = z$, which since $(xy)^h = x^h y^h = xy$ is a contradiction. Hence $|N| = |X| = 4$ and $G \cong \mathcal{S}_4$. $\sharp$

(6.4) Remark. Using the O'Nan-Scott Theorem and CFSG, it can be shown that the 3-fold transitive finite groups G having a regular normal subgroup N are given as follows: It is immediate that $N \cong C_p^n \cong \mathbb{F}_p^n$, where $[p, n] = [3, 1]$ or $p = 2$ and $n \geq 2$, and we have $H := \mathrm{Stab}_G(0) \leq \mathrm{GL}_n(\mathbb{F}_p)$, hence $G \leq \mathrm{GL}_n(\mathbb{F}_p) \ltimes \mathbb{F}_p^n \cong \mathrm{AGL}_n(\mathbb{F}_p)$, the **affine linear group**, which acts naturally on $\mathbb{F}_p^n$ by **affine $\mathbb{F}_p$-linear maps** $[g, t]\colon \mathbb{F}_p^n \to \mathbb{F}_p^n \colon x \mapsto xg + t$ for all $g \in \mathrm{GL}_n(\mathbb{F}_p)$ and $t, x \in \mathbb{F}_p^n$. Moreover we have:

i) $N \cong \mathbb{F}_3$ and $H = \mathrm{GL}_1(\mathbb{F}_3) \cong C_2$, hence $G \cong \mathcal{S}_3$ is sharply 3-fold transitive.
ii) $N \cong \mathbb{F}_2^2$ and $H = \mathrm{GL}_2(\mathbb{F}_2) \cong \mathcal{S}_3$, hence $G \cong \mathcal{S}_4$ is sharply 4-fold transitive.
iii) $N \cong \mathbb{F}_2^n$ for $n \geq 3$ and $H = \mathrm{GL}_n(\mathbb{F}_2)$, hence $G \cong \mathrm{AGL}_n(\mathbb{F}_2)$. It is immediate that $\mathrm{GL}_n(\mathbb{F}_2)$ is 2-fold transitive on $\mathbb{F}_2^n \setminus \{0\}$, hence G indeed is 3-fold transitive.
iv) $N \cong \mathbb{F}_2^4$ and $H = \mathcal{A}_7 \leq \mathcal{A}_8 \cong \mathrm{GL}_4(\mathbb{F}_2)$. There is a unique conjugacy class of subgroups of $\mathrm{GL}_4(\mathbb{F}_2)$ isomorphic to $\mathcal{A}_7$, from which it is immediate that $G \cong \mathcal{A}_7 \ltimes \mathbb{F}_2^4$ is unique up to isomorphism; moreover $\mathcal{A}_7$ acts 2-fold transitively on $\mathbb{F}_2^4 \setminus \{0\}$, hence G indeed is 3-fold transitive.

(6.5) Theorem. For $n \geq 5$ the alternating group $\mathcal{A}_n$ is simple.

Proof. We proceed by induction, the group $\mathcal{A}_5$ being simple. Let $n \geq 6$, hence $\mathcal{A}_n$ acts 4-fold transitively, thus primitively, implying that $\mathrm{Stab}_{\mathcal{A}_n}(n) = \mathcal{A}_{n-1} <$

$\mathcal{A}_n$ is a non-normal maximal subgroup. Assume there is $\{1\} \neq N \lhd \mathcal{A}_n$, hence N acts transitively. Since $\mathcal{A}_{n-1} \not\leq N$ and $\mathcal{A}_{n-1}$ is simple, we have $N \cap \mathcal{A}_{n-1} = \{1\}$, thus N acts regularly. Hence (6.3) implies $n = 4$, a contradiction. $\sharp$

7 Soluble and nilpotent groups

(7.1) Definition. Let G be a group.
a) Let A be a group, and let $\alpha\colon A \to \mathrm{Aut}(G)$ be a homomorphism. Then A acts on G by $g^a := g^{(a\alpha)}$, for $a \in A$ and $g \in G$; the A-set G is called an **A-group**.

A subgroup $H \leq G$ such that $H^a \subseteq H$, for all $a \in A$, is called **A-invariant**; in this case H also is an A-group and we write $H \leq_A G$. If $N \trianglelefteq_A G$ then G/N is an A-group by $(Ng)^a := Ng^a$, for $a \in A$ and $g \in G$. The $\mathrm{Inn}(G)$-invariant subgroups of G are its normal subgroups. An $\mathrm{Aut}(G)$-invariant subgroup of G is called **characteristic**.

If G and H are A-groups, then a group homomorphism $\varphi\colon G \to H$ which also is a homomorphism of A-sets is called an **A-homomorphism**. It is immediate that in this case $\ker(\varphi) \trianglelefteq_A G$ and $\mathrm{im}(\varphi) \leq_A H$, and that the induced map $\overline{\varphi}\colon G/\ker(\varphi) \to \mathrm{im}(\varphi)$ is an A-isomorphism; we write $G/\ker(\varphi) \cong_A \mathrm{im}(\varphi)$.

b) Let G be an A-group. Then $\mathcal{G}\colon \{1\} = G_0 < G_1 < \cdots < G_{l-1} < G_l = G$, where $G_i \leq_A G$ for all $i \in \{0, \ldots, l\}$, is called an **A-chain** of subgroups of **length** $l \in \mathbb{N}_0$. If moreover $G_{i-1} \lhd G_i$ for all $i \in \{1, \ldots, l\}$ then $\mathcal{G}$ is called an **A-subnormal series**, we write $G_i \trianglelefteq\trianglelefteq_A G$; in this case the factor groups G_i/G_{i-1} for $i \in \{1, \ldots, l\}$ are called the **sections** of $\mathcal{G}$. If moreover $G_i \trianglelefteq G$ for all $i \in \{0, \ldots, l\}$ then $\mathcal{G}$ is called an **A-normal series**.

If $\mathcal{G}$ is a $\{\mathrm{id}_G\}$-chain it is called a **subnormal series**; we write $G_i \trianglelefteq\trianglelefteq G$. If $\mathcal{G}$ is an $\mathrm{Inn}(G)$-chain, i. e. we have $G_i \trianglelefteq G$ for all $i \in \{0, \ldots, l\}$, it is called a a **normal series**. If $\mathcal{G}$ is an $\mathrm{Aut}(G)$-chain, i. e. $G_i \trianglelefteq G$ is characteristic for all $i \in \{0, \ldots, l\}$, it is called a **characteristic series**.

If $G_{i-1} \lhd G_i$ is maximal A-invariant for all $i \in \{1, \ldots, l\}$, i. e. the sections G_i/G_{i-1} are **A-simple**, then $\mathcal{G}$ is called an **A-composition series**, its sections are called **A-composition factors**; an $\{\mathrm{id}_G\}$-composition series is called a **composition series**, its sections are called **composition factors**. An $\mathrm{Inn}(G)$-composition series is called a **chief series**, its sections are called **chief factors**. An $\mathrm{Aut}(G)$-simple section is called **characteristically simple**.

Any A-subnormal series can be **refined** by inserting A-invariant subnormal subgroups; hence if G is finite this after a finite number of steps yields an A-composition series of G. E. g. for $G = \mathcal{S}_4$ we have a composition series $\{1\} < \langle(1,2)\rangle < V_4 = \langle(12)(34), (13)(24)\rangle < \mathcal{A}_4 < \mathcal{S}_4$, and a unique chief series $\{1\} < V_4 < \mathcal{A}_4 < \mathcal{S}_4$, where the latter also is a characteristic series.

(7.2) Theorem: Jordan-Hölder (1870/1893).
Let G be an A-group, and let $\{1\} = G_0 < \cdots < G_l = G$ and $\{1\} = H_0 < \cdots <$

$H_m = G$ be A-composition series of G where $l, m \in \mathbb{N}_0$. Then we have $l = m$ and there is $\pi \in \mathcal{S}_l$ such that for all $i \in \{1, \ldots, l\}$ we have $G_{i\pi}/G_{i\pi-1} \cong_A H_i/H_{i-1}$.

Proof. We may assume that $G \neq \{1\}$. Then $N := H_{m-1} \lhd_A G$ is a maximal A-invariant normal subgroup. For all $i \in \{0, \ldots, l\}$ we have either $G_i \leq N$ or $G_i N = G$: If $G_i \not\leq N$ we have $N \lhd G_i N \trianglelefteq G_{i+1} N \trianglelefteq \cdots \trianglelefteq G_l N = G$, thus by A-invariance we successively get $G = G_l N = G_{l-1} N = \cdots = G_i N$. Let $j \in \{1, \ldots, l\}$ minimal such that $G_j \not\leq N$, and for $i \geq j$ let $G_i' := G_i \cap N \leq_A G$.

Let $i \geq j+1$. Assume that $G_i' = G_{i-1}'$, then since $G_i N/N = G/N = G_{i-1}N/N$ for any $g \in G_i$ there are $h \in G_{i-1}$ and $n \in N$ such that $g = hn$, which implies $n \in G_i \cap N = G_i' = G_{i-1}'$ and hence $g \in G_{i-1}$, a contradiction. Hence we have $G_{i-1}' \lhd_A G_i'$. Moreover, $G_i' \cap G_{i-1} = G_i \cap N \cap G_{i-1} = N \cap G_{i-1} = G_{i-1}'$ implies $\{1\} \neq G_i'/G_{i-1}' = G_i'/(G_i' \cap G_{i-1}) \cong_A G_i' G_{i-1}/G_{i-1} \trianglelefteq_A G_i/G_{i-1}$, thus we have $G_i'/G_{i-1}' \cong_A G_i/G_{i-1}$.

Since $G_{j-1} = G_{j-1} \cap N \leq G_j' = G_j \cap N \lhd_A G_j$ implies $G_{j-1} = G_j'$, we have $H_m/H_{m-1} = G/N = G_j N/N \cong_A G_j/(G_j \cap N) = G_j/G_j' = G_j/G_{j-1}$. Moreover, $\{1\} = G_0 < \cdots < G_{j-1} = G_j' < G_{j+1}' < \cdots < G_l' = N$ and $\{1\} = H_0 < \cdots < H_{m-1} = N$ are A-composition series of N of length $l-1$ and $m-1$, respectively, and we are done by induction on the minimal length of an A-composition series of the group under consideration. ♯

(7.3) Definition and Remark. a) Let G be a group. For $g, h \in G$ let $[g, h] := g^{-1}h^{-1}gh = g^{-1} \cdot g^h \in G$ be the associated **commutator**. More generally, for $g_1, \ldots, g_n \in G$, where $n \geq 2$, we let $[g_1, \ldots, g_n] := [[\cdots[g_1, g_2], g_3], \ldots] \in G$ be the associated **left normed** commutator.

For $U, V \subseteq G$ let $[U, V] := \langle [u, v] \in G; u \in U, v \in V \rangle \leq G$. In particular, the **derived subgroup** $[G, G] \leq G$ is characteristic, and $[G, G] \trianglelefteq G$ is the smallest normal subgroup of G having an abelian factor group: Since $gh = hg \cdot [g, h]$ for all $g, h \in G$ we conclude that $G/[G, G]$ is abelian, and if conversely $N \trianglelefteq G$ is a normal subgroup such that G/N is abelian, then we have $[g, h] \in N$ for all $g, h \in G$, and thus $[G, G] \leq N$.

b) Letting $G^{(0)} := G$, for $i \in \mathbb{N}$ let successively $G^{(i)} := [G^{(i-1)}, G^{(i-1)}] \leq G^{(i-1)}$; hence $G^{(i)} \trianglelefteq G$ is characteristic. The characteristic series $G = G^{(0)} \geq [G, G] = G^{(1)} \geq \cdots \geq G^{(i)} \geq \cdots$ is called the **derived series** of G. It is immediate that if $G^{(i)} = G^{(i+1)}$ for some $i \in \mathbb{N}_0$ then we have $G^{(i)} = G^{(i+j)}$ for all $j \in \mathbb{N}_0$.

G is called **soluble** if there is $l \in \mathbb{N}_0$ such that $G^{(l)} = \{1\}$; if l is chosen minimal, then G is called to have **derived length** l. The group G has derived length 0 if and only if $G = \{1\}$; the groups of derived length ≤ 1 are the abelian groups; and groups of derived length 2 are called **metabelian**.

(7.4) Theorem. a) Let G be a group. If G is soluble, then so is any subgroup of G, and so is any factor group of G. If there is $N \trianglelefteq G$ such that both N and G/N are soluble, then so is G. Moreover, the following are equivalent:

i) G is soluble. **ii)** G has a normal series with abelian sections.

b) Let G be a finite group. Then the following are equivalent:
i) G is soluble. **ii)** G has a chief series with elementary abelian sections.
iii) G has a composition series with cyclic sections of prime order.

Proof. a) For any $U \leq G$ and all $i \in \mathbb{N}_0$ we have $U^{(i)} \leq G^{(i)}$: By induction we for $i \in \mathbb{N}$ have $U^{(i)} = [U^{(i-1)}, U^{(i-1)}] \leq [G^{(i-1)}, G^{(i-1)}] = G^{(i)}$.

Letting $N \trianglelefteq G$, we for all $g, h \in G$ have $[gN, hN] = [g, h]N \in G/N$, and hence for all $i \in \mathbb{N}_0$ we have $(G/N)^{(i)} = G^{(i)}N/N$: By induction we for $i \in \mathbb{N}$ have $(G/N)^{(i)} = [(G/N)^{(i-1)}, (G/N)^{(i-1)}] = [G^{(i-1)}N/N, G^{(i-1)}N/N] = [G^{(i-1)}N, G^{(i-1)}N]N/N = G^{(i)}N/N$.

Let $N \trianglelefteq G$ such that both N and G/N are soluble, then there is $l \in \mathbb{N}_0$ such that $G^{(l)}N/N = (G/N)^{(l)} = N$ and thus $G^{(l+i)} \leq N^{(i)}$ for all $i \in \mathbb{N}_0$.

Finally, **(i)⇒(ii)** is trivial. And for **(ii)⇒(i)** let $G = N_0 > \cdots > N_k = \{1\}$, for some $k \in \mathbb{N}_0$, be a normal series with abelian sections, then for all $i \in \{0, \ldots, k\}$ we have $G^{(i)} \leq N_i$: We have $G^{(0)} = N_0$, and by induction we for $i \geq 1$ have $G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \leq [N_{i-1}, N_{i-1}] \leq N_i$.

b) (i)⇒(ii): Let $\mathcal{G}\colon G = N_0 > \cdots > N_k = \{1\}$, for some $k \in \mathbb{N}_0$, be a normal series with abelian sections. Hence for $i \in \{0, \ldots, k-1\}$ we have $S := N_i/N_{i+1} = \prod_{p \mid |S|} O_p(S)$, where $O_p(S) \trianglelefteq S$ is characteristic. Thus $\mathcal{G}$ can be refined to a normal series with sections T consisting of abelian p-groups. Then $\Omega(T) := \langle g \in T; g^p = 1 \rangle = \{g \in T; g^p = 1\} \trianglelefteq T$ is a characteristic subgroup, hence $\mathcal{G}$ can be refined further to a normal series with elementary abelian sections.

(ii)⇒(iii): Let $\mathcal{G}\colon G = N_0 > \cdots > N_k = \{1\}$, for some $k \in \mathbb{N}_0$, be a normal series with elementary abelian sections. Hence for $i \in \{0, \ldots, k-1\}$ picking $1 \neq g \in S := N_i/N_{i+1}$ we get $C_p \cong \langle g \rangle \trianglelefteq S$ for some prime p, and hence $\mathcal{G}$ can be refined to a subnormal series with cyclic sections of prime order.

(iii)⇒(i): Let $G = N_0 > \cdots > N_k = \{1\}$, for some $k \in \mathbb{N}_0$, be a subnormal series with cyclic sections of prime order. Since any abelian group is soluble, we for $i \in \{k, k-1, \ldots, 0\}$ by induction infer that N_i is soluble. ♯

(7.5) Definition and Remark. A group is called **supersoluble** if it has a normal series with cyclic sections. Since any subgroup of a cyclic group is characteristic, a finite group is supersoluble if and only if it has a chief series with cyclic sections of prime order.

A supersoluble group is soluble; e. g. $\mathcal{S}_4$ is soluble but not supersoluble.

(7.6) Definition. a) Let G be a group. A normal series $G = N_1 \geq N_2 \geq \cdots \geq N_i \geq \cdots$ such that $[N_i, G] \leq N_{i+1}$ for all $i \in \mathbb{N}$ is called a **central series**; the condition $[N_i, G] \leq N_{i+1}$ is equivalent to $N_i/N_{i+1} \leq Z(G/N_{i+1})$.

G is called **nilpotent** if it has a central series $G = N_1 \geq \cdots \geq N_l = \{1\}$ for some $l \in \mathbb{N}$; in this case the minimal length $c = l - 1 \in \mathbb{N}_0$ of all central series $G = N_1 > \cdots > N_l = \{1\}$ is called the **nilpotency class** of G.

The group G has nilpotency class 0 if and only if $G = \{1\}$, and the groups of nilpotency class ≤ 1 are the abelian groups. Since for any group G all subgroups of $Z(G)$ are normal subgroups of G, we by induction infer that a nilpotent group is supersoluble; e. g. $\mathcal{S}_3$ is supersoluble but not nilpotent.

b) Letting $K_1(G) := G$, for $i \in \mathbb{N}$ let successively $K_{i+1}(G) := [K_i(G), G] \leq G$. Hence $K_i(G) \trianglelefteq G$ is characteristic, and we have $K_{i+1}(G) \trianglelefteq K_i(G)$ and $K_i(G)/K_{i+1}(G) \leq Z(G/K_{i+1}(G))$ for all $i \in \mathbb{N}$. The series $G = K_1(G) \geq [G,G] = K_2(G) \geq \cdots \geq K_i(G) \geq \cdots$ is called the **lower central series** of G.

It is immediate that if $K_i(G) = K_{i+1}(G)$ for some $i \in \mathbb{N}$ then we have $K_i(G) = K_{i+j}(G)$ for all $j \in \mathbb{N}_0$. We let $K_\infty(G) := \bigcap_{i \in \mathbb{N}} K_i(G) \trianglelefteq G$ characteristic.

c) The **upper central series** $\{1\} = Z_0(G) \leq Z_1(G) \leq \cdots \leq Z_i(G) \leq \cdots$ of G is for $i \in \mathbb{N}$ successively defined by $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$; hence $Z_i(G) \trianglelefteq G$ is characteristic for all $i \in \mathbb{N}_0$.

It is immediate that if $Z_i(G) = Z_{i+1}(G)$ for some $i \in \mathbb{N}_0$ then we have $Z_i(G) = Z_{i+j}(G)$ for all $j \in \mathbb{N}_0$. We let $Z_\infty(G) := \bigcup_{i \in \mathbb{N}_0} Z_i(G) \trianglelefteq G$ characteristic be the **hypercentre** of G.

(7.7) Theorem. a) Let G be a group. Then the following are equivalent:
i) G is nilpotent of class $c \in \mathbb{N}_0$. **ii)** There is $r \in \mathbb{N}_0$ such that $K_{r+1}(G) = \{1\}$.
iii) There is $s \in \mathbb{N}_0$ such that $Z_s(G) = G$.

If $G = N_1 \geq \cdots \geq N_l = \{1\}$ is a central series, we have $K_i(G) \leq N_i \leq Z_{l-i}(G)$ for all $i \in \{1, \ldots, l\}$. Thus if r and s are chosen minimal, we have $r = c = s$.

Hence, if G is nilpotent then so is any subgroup, and so is any factor group.

b) Let G be a finite group. Then the following are equivalent:
i) G is nilpotent. **ii)** For any $U < G$ we have $U < N_G(U)$.
iii) Any maximal subgroup of G is normal. **iv)** We have $G = \prod_{p \mid |G|} O_p(G)$.

In particular, if G has order p^n, where p is a prime and $n \in \mathbb{N}_0$, then G is nilpotent of class $c \leq n$; the number $n - c \in \mathbb{N}_0$ is called the **coclass** of G.

Proof. a) (iii)⇒(i) and **(ii)⇒(i)** are trivial. **(i)⇒(ii):** Let $G = N_1 \geq \cdots \geq N_l = \{1\}$ be a central series for some $l \in \mathbb{N}$. Then for all $i \in \{1, \ldots, l\}$ we have $K_i(G) \leq N_i$: By induction we get $K_{i+1}(G) = [K_i(G), G] \leq [N_i, G] \leq N_{i+1}$.

(i)⇒(iii): Let $G = N_1 \geq \cdots \geq N_l = \{1\}$ be a central series for some $l \in \mathbb{N}$. Then for all $i \in \{1, \ldots, l\}$ we have $N_i \leq Z_{l-i}(G)$: We have $N_l = \{1\} = Z_0(G)$, and for $i \in \{2, \ldots, l\}$ we by induction get $[N_{i-1}, G] \leq N_i \leq Z_{l-i}(G)$, implying $N_{i-1} \leq Z_{l-i+1}(G)$. Thus in particular we infer $Z_{l-1}(G) = G$.

b) (i)⇒(ii): Let $U < G$, and let $i \in \mathbb{N}$ maximal such that $K_i(G) \not\leq U$ and $K_{i+1}(G) \leq U$. Hence we have $[K_i(G), U] \leq [K_i(G), G] \leq K_{i+1}(G) \leq U$, thus

$U < UK_i(G) \leq N_G(U)$.

(ii)⇒(iii) is trivial. **(iii)⇒(iv):** We show that any $P \in \mathrm{Syl}_p(G)$ is normal: Assume that $N_G(P) < G$, then there is $U < G$ maximal such that $N_G(P) \leq U$. By the Frattini argument we have $N_G(U) = U$, a contradiction.

(iv)⇒(i): We may assume that G is a p-group. Since $Z(G) \neq \{1\}$ whenever $G \neq \{1\}$ we by induction on $|G|$ infer that G is nilpotent. ♯

(7.8) Theorem. Let $p \neq q$ be primes, let $a \in \mathbb{N}$, and let G be a group such that $|G| = p^a q$. Then G is soluble.

Proof. Let $P \in \mathrm{Syl}_p(G)$, hence we have $[G\colon N_G(P)] \in \{1, q\}$. If $N_G(P) = G$ then we have $P \lhd G$, and both P and $G/P \cong C_q$ are soluble, thus G is as well. Hence we may assume that $[G\colon N_G(P)] = q$. Letting $P_1 \neq P_2 \in \mathrm{Syl}_p(G)$ be chosen such that $S := P_1 \cap P_2$ has maximal order, we distinguish two cases:

i) Let $S = \{1\}$, i. e. P is a trivial intersection subgroup. Hence G has precisely $1 + (|P| - 1) \cdot [G\colon N_G(P)] = 1 + (p^a - 1)q = |G| - (q - 1)$ elements of p-power order, implying that there is a unique Sylow q-subgroup $Q \trianglelefteq G$, where both Q and G/Q are soluble, and thus G is as well.

ii) Let $S \neq \{1\}$. Since P_i is nilpotent we have $S < N_{P_i}(S) \leq P_i$ for $i \in \{1, 2\}$, and thus $S \lhd \langle N_{P_1}(S), N_{P_2}(S)\rangle := T \leq N_G(S) \leq G$. Assume T is a p-group, then there is $P \in \mathrm{Syl}_p(G)$ such that $T \leq P$, implying $S < N_{P_i}(S) \leq P_i \cap T \leq P_i \cap P$. Thus by the maximality of S we conclude $P_1 = P = P_2$, a contradiction.

Hence we have $|T| = p^b q$ for some $b \leq a$, and let $Q \in \mathrm{Syl}_q(T)$. Since $P_1 \cap Q = \{1\}$ it is immediate that for the complex product $QP_1 \subseteq G$ we have $|QP_1| = qp^a = |G|$, thus any $g \in G$ can be written as $g = g'h$ where $g' \in Q$ and $h \in P_1$. Letting $N := \langle S^g; g \in G\rangle \trianglelefteq G$, since $Q \leq T \leq N_G(S)$ we get $N = \langle S^h; h \in P_1\rangle \leq P_1 < G$, implying that $\{1\} \neq N \lhd G$. Hence by induction on $a \in \mathbb{N}$ both N and G/N are soluble, thus G is as well. ♯

(7.9) Remark. a) By the **Hölder-Zassenhaus Theorem** any finite group having only cyclic Sylow subgroups is metabelian; in particular any group of squarefree order is soluble.
b) By **Burnside's Theorem** (1904) any finite group G such that $|G| = p^a q^b$, where $p \neq q$ are primes and $a, b \in \mathbb{N}$, is soluble.
c) By the **Feit-Thompson Theorem** (1963) any group of odd order is soluble.

(7.10) Theorem: Schmidt (1924).
Any finite group all of whose maximal subgroups are nilpotent is soluble.

Proof. Let G be a counterexample of minimal order. Assume there is $\{1\} \leq N \lhd G$, then both N and G/N are soluble, hence G is soluble as well, a contradiction. Hence G is simple.

Let $U_1 \neq U_2 < G$ maximal such that $S := U_1 \cap U_2 < G$ has maximal order. Assume that $S \neq \{1\}$, then we for $i \in \{1,2\}$ have $\{1\} \neq S < N_G(S) \cap U_i =: H_i \leq U_i < G$. Since G is simple we have $N_G(S) < G$, thus there is $U < G$ maximal such that $S \lhd \langle H_1, H_2 \rangle \leq N_G(S) \leq U < G$. Since $S < H_i \leq U_i \cap U$ the maximality of S implies $U_1 = U = U_2$, a contradiction.

Hence any pair of maximal subgroups has trivial intersection. Moreover, since G is simple for any $U < G$ maximal we have $U = N_G(U)$ and thus $|\{U^g < U; g \in G\}| = [G \colon U]$. Let $\{U_j < G; j \in \mathcal{J}\}$ be a set of representatives of the conjugacy classes of maximal subgroups, where $\mathcal{J} \neq \emptyset$ is a finite index set. Then we have $|G| = 1 + \sum_{j \in \mathcal{J}}(|U_j| - 1) \cdot [G \colon U_j] = 1 + |\mathcal{J}| \cdot |G| - \sum_{j \in \mathcal{J}}[G \colon U_j] \geq 1 + |\mathcal{J}| \cdot |G| - |\mathcal{J}| \cdot \frac{|G|}{2} = 1 + |\mathcal{J}| \cdot \frac{|G|}{2}$. This implies $|\mathcal{J}| = 1$, hence $|G| = 1 + |G| - [G \colon U]$, and thus $[G \colon U] = 1$, a contradiction. ♯

(7.11) Remark. a) Let G be a minimal non-nilpotent finite group, i. e. all its maximal subgroups are nilpotent. Then we have:
i) $|G| = p^a q^b$, where $p \neq q$ are primes and $a, b \in \mathbb{N}$; **ii)** G has a normal Sylow p-subgroup $P \lhd G$, where $\Phi(P) \leq Z(G)$, for $p = 2$ we have $\exp(P) \leq 4$ and for $p > 2$ we have $\exp(P) = p$; **iii)** the Sylow q-subgroups $Q < G$ are cyclic such that $\Phi(Q) \leq Z(G)$.

b) The simple groups all of whose maximal subgroups are soluble are given as follows (**Thompson**, 1968):
i) $\mathrm{PSL}_2(\mathbb{F}_p)$, where $p \geq 5$ is a prime such that $5 \not| \, p^2 - 1$; **ii)** $\mathrm{PSL}_2(\mathbb{F}_{2^p})$, where p is a prime; **iii)** $\mathrm{PSL}_2(\mathbb{F}_{3^p})$, where $p \geq 3$ is a prime; **iv)** $\mathrm{PSL}_3(\mathbb{F}_3)$; **v)** the **Suzuki groups** $Sz(\mathbb{F}_{2^p}) = {}^2B_2(\mathbb{F}_{2^p})$, where $p \geq 3$ is a prime.

c) We have the following characterisation of soluble finite groups (**Bandman-Greuel-Grunewald-Kunyavskii-Pfister-Plotkin**, 2003): Let $w_1(X,Y) := X^{-2}Y^{-1}X$ and $w_{n+1}(X,Y) := [Xw_n(X,Y)X^{-1}, Yw_n(X,Y)Y^{-1}]$ for $n \in \mathbb{N}$. Then a finite group G is soluble if and only if for some $n \in \mathbb{N}$ the identity $w_n(g,h) = 1$ holds for all $g, h \in G$.

If G is soluble then it is immediate that the identity w_n is fulfilled for all $n \geq l+1$, where $l \in \mathbb{N}_0$ is the derived length of G. To prove the converse, it can be shown that the minimal non-soluble finite groups do not fulfill any of the identities.

8 Frattini and Fitting subgroups

(8.1) Definition and Remark. a) Let G be a finite group group. If $G \neq \{1\}$ then $\Phi(G) := \bigcap\{U < G \text{ maximal}\}$ is called the **Frattini subgroup** of G; we let $\Phi(\{1\}) := \{1\}$. Hence we have $\Phi(G) \trianglelefteq G$ characteristic.

b) For $g \in G$ we have $g \in \Phi(G)$ if and only if g can be discarded from any generating set of G, i. e. for any $S \subseteq G$ such that $\langle S, g \rangle = G$ we have $\langle S \rangle = G$:

Let $g \in \Phi(G)$ and assume there is $S \subseteq G$ such that $\langle S, g \rangle = G$ and $\langle S \rangle \leq U < G$, for some $U < G$ maximal, then since $\Phi(G) \leq U$ this is a contradiction.

Conversely, let g be discardable from any generating set of G and assume that $g \notin \Phi(G)$, then there is $U < G$ maximal such that $g \notin U$, hence we have $G = \langle U, g\rangle = \langle U\rangle = U$, a contradiction. $\sharp$

c) Let $N \trianglelefteq G$, then it is immediate that the natural map induces a bijection from $\{N \leq U < G \text{ maximal}\}$ to the set of maximal subgroups of G/N. This implies $\Phi(G)N/N \leq \Phi(G/N)$, and $\Phi(G)N/N = \Phi(G/N)$ whenever $N \leq \Phi(G)$.

We show that in general $\Phi(G)N/N \neq \Phi(G/N)$, and $\Phi(H) \not\leq \Phi(G)$ for $H \leq G$:

E. g. let $H := \langle h\rangle \cong C_4$ and $G := H \ltimes N$, where $N := \langle n\rangle \cong C_5$ and h acts by $\alpha\colon N \rightarrow N\colon n \mapsto n^2$, hence $\langle\alpha\rangle = \mathrm{Aut}(N) \cong \mathrm{Aut}(C_5) \cong (\mathbb{Z}/5\mathbb{Z})^* \cong C_4$. We have $[G\colon H] = 5$, hence $H < G$ is maximal, and thus to show that $\Phi(G) = \{1\}$ it suffices to show that $H \cap H^n = \{1\}$: Assume that $H^n = H$, then $H \trianglelefteq G$, and thus $H \cap N = \{1\}$ implies $H \leq C_G(N)$, a contradiction; assume that $\{1\} \neq U := H \cap H^n < H$, then we have $U \trianglelefteq \langle H, H^n\rangle = G$, and $U \cap N = \{1\}$ implies $\langle h^2\rangle = U \leq C_G(N)$, a contradiction. Thus we have $\Phi(H) = \langle h^2\rangle \cong C_2$ and $\{1\} = \Phi(G)N/N \neq \Phi(G/N) \cong \Phi(H) \cong C_2$. $\sharp$

(8.2) Proposition. Let G be a finite group and $N \trianglelefteq G$. If there is $H \leq G$ such that $N \leq \Phi(H)$, then we have $N \leq \Phi(G)$. In particular, we have $\Phi(N) \leq \Phi(G)$.

Proof. Assume that $N \not\leq \Phi(G)$, then there is $U < G$ maximal such that $N \not\leq U$, and hence $UN = G$. Since $N \leq H$ we conclude $H = H \cap UN = (H \cap U)N$. Since $N \leq \Phi(H)$ we infer $H = H \cap U$, hence $N \leq H \leq U$, a contradiction.

Since we have $\Phi(N) \trianglelefteq G$, letting $H := N$ yields $\Phi(N) \leq \Phi(G)$. $\sharp$

(8.3) Theorem: Gaschütz (1953).
Let G be a finite group, let $N, M \trianglelefteq G$ such that $M \leq N \cap \Phi(G)$ and such that N/M is nilpotent. Then N is nilpotent.

Proof. Let $P \in \mathrm{Syl}_p(N)$. Hence $PM/M \in \mathrm{Syl}_p(N/M)$, and since N/M is nilpotent we conclude that $PM/M \trianglelefteq N/M$ is characteristic, and thus we have $PM/M \trianglelefteq G/M$. Since $P \in \mathrm{Syl}_p(PM)$, the Frattini argument implies $G = N_G(P) \cdot PM = N_G(P)M$. Since $M \leq \Phi(G)$ this yields $N_G(P) = G$, thus $P \trianglelefteq G$ and hence N is nilpotent. $\sharp$

(8.4) Corollary: Frattini (1885).
Let G be a finite group.
a) Then $\Phi(G)$ is nilpotent.
b) Then G is nilpotent if and only if $G/\Phi(G)$ is.

Proof. a) Let $N := M := \Phi(G)$. **b)** Let $N := G$ and $M := \Phi(G)$. $\sharp$

(8.5) Theorem: Gaschütz (1953), Wielandt (1937).
Let G be a finite group.
a) Then we have $[G,G] \cap Z(G) \leq \Phi(G)$.
b) Let $N \trianglelefteq G$. Then N is nilpotent if and only if $[N,N] \leq \Phi(G)$. In particular, G is nilpotent if and only if $[G,G] \leq \Phi(G)$.

Proof. a) Let $N := [G,G] \cap Z(G) \trianglelefteq G$, and assume that $N \not\leq \Phi(G)$. Then there is $U < G$ maximal such that $N \not\leq U$, hence we have $G = NU$ and any $g \in G$ can be written as $g = nu$, where $u \in U$ and $n \in N$. Since $n \in N \leq Z(G)$ we have $U^g = U^{nu} = U$, implying that $U \trianglelefteq G$. Since $U < G$ is maximal we infer $G/U \cong C_p$, for some prime p, and thus $N \leq [G,G] \leq U$, a contradiction.

b) Let $[N,N] \leq \Phi(G)$. Since $N/[N,N]$ is abelian and thus nilpotent, and $[N,N] \trianglelefteq G$, we by (8.3) conclude that N is nilpotent.

Conversely, let N be nilpotent; we may assume that $N \neq \{1\}$. Since any maximal subgroup $U < N$ is normal, we conclude that $N/U \cong C_p$, for some prime p, and thus $[N,N] \leq \Phi(N) = \bigcap\{U < N \text{ maximal}\}$. Hence from $\Phi(N) \leq \Phi(G)$ we get $[N,N] \leq \Phi(G)$. ♯

(8.6) Theorem: Burnside's basis theorem (1912).
Let G be a p-group, where p is a prime.
a) Then we have $\Phi(G) = [G,G]G^p$, where $G^p := \langle g^p; g \in G\rangle \trianglelefteq G$; if $p = 2$ then we have $\Phi(G) = G^2$.

Hence $\Phi(G) \trianglelefteq G$ is the smallest normal subgroup having p-elementary abelian factor group. Moreover, for $H \leq G$ we have $\Phi(H) \leq \Phi(G)$, and for $N \trianglelefteq G$ we have $\Phi(G)N/N = \Phi(G/N)$.

b) Let $|G/\Phi(G)| = p^d$, where $d \in \mathbb{N}_0$. Then any minimal generating set of G has cardinality d, and any element of $G \setminus \Phi(G)$ is in a minimal generating set.

Proof: Hall (1933).
a) Let $U < G$ be maximal. Since G is nilpotent, we have $U \triangleleft G$ and thus $G/U \cong C_p$, implying $[G,G]G^p \leq U$ and thus $N := [G,G]G^p \leq \Phi(G)$. Conversely, G/N is p-elementary abelian, thus we have $G/N \cong \mathbb{F}_p^d$ for some $d \in \mathbb{N}_0$. Let $g \in G \setminus N$, then there is an $\mathbb{F}_p$-basis $\{gN, g_2N, \ldots, g_dN\} \subseteq G/N$. Since $G = \langle g, g_2, \ldots, g_d, N\rangle > \langle g_2, \ldots, g_d, N\rangle$ we conclude $g \notin \Phi(G)$.

If $p = 2$, then for all $g, h \in G$ we have $[g,h] = g^{-1}h^{-1}gh = g^{-1}\cdot h^{-2}gg^{-2}gh\cdot gh = (h^g)^{-2}g^{-2}(gh)^2$, implying that $[G,G] \leq G^2$.

b) Let $N := \Phi(G)$, and let $S = \{g_1, \ldots, g_n\} \subseteq G$ for some $n \in \mathbb{N}_0$, then we have $\langle S\rangle = G$ if and only if $\langle g_1N, \ldots, g_nN\rangle = G/N$. We have $G/N \cong \mathbb{F}_p^d$, and thus the minimal generating sets of G/N are precisely its $\mathbb{F}_p$-bases. ♯

(8.7) Definition and Remark. a) Let G be a finite group. Since for any $N \trianglelefteq G$ we have $O_p(N) \trianglelefteq N$ characteristic, we infer $O_p(N) \trianglelefteq O_p(G)$. Thus for any

$N \trianglelefteq G$ nilpotent we have $N = \prod_{p \mid |N|} O_p(N) \leq \prod_{p \mid |G|} O_p(G) =: F(G)$. Hence $F(G) = \langle N \trianglelefteq G \text{ nilpotent} \rangle \trianglelefteq G$ is characteristic, and is the largest nilpotent normal subgroup of G, being called its **Fitting subgroup** (1938).

Moreover, for any $N \trianglelefteq G$ we have $F(N) \leq F(G)$, implying $F(N) = N \cap F(G)$. Thus for any $N \trianglelefteq\trianglelefteq G$ we have $F(N) \leq F(G)$, again implying $F(N) = N \cap F(G)$, and we infer $F(G) = \langle N \trianglelefteq\trianglelefteq G \text{ nilpotent} \rangle$.

b) Since $\Phi(G) \trianglelefteq G$ is nilpotent we have $\Phi(G) \leq F(G)$. Moreover, we have $F(G/\Phi(G)) = F(G)/\Phi(G)$:

Since $F(G)/\Phi(G) \trianglelefteq G/\Phi(G)$ is nilpotent, we have $F(G)/\Phi(G) \leq F(G/\Phi(G))$. Let conversely $\Phi(G) \leq N \trianglelefteq G$ such that $F(G/\Phi(G)) = N/\Phi(G)$, then by (8.3) we infer that N is nilpotent, and thus $N \leq F(G)$. ♯

(8.8) Theorem. Let G be a finite group.
a) Then $C_G(F(G))F(G)/F(G)$ does not have a non-trivial soluble normal subgroup. In particular, if G is soluble then $C_G(F(G)) \leq F(G)$.
b) Let $\{1\} \neq N \trianglelefteq G$ be a minimal normal subgroup. Then we have $F(G) \leq C_G(N)$, and if moreover N is abelian then we have $N \leq Z(F(G))$.
c) Let $G = N_1 > \cdots > N_k = \{1\}$ be a chief series, for some $k \in \mathbb{N}$. Then we have $F(G) = \bigcap_{i=1}^{k-1} C_G(N_i/N_{i+1})$.

Here for any $N, M \trianglelefteq G$ such that $M \leq N$ we let $C_G(N/M) := \{g \in G; [N, g] \subseteq M\} \trianglelefteq G$ be the kernel of the G-conjugation action on N/M.

Proof. a) Let $C := C_G(F(G)) \trianglelefteq G$ characteristic. It is immediate that any minimal characteristic subgroup of a soluble group is elementary abelian. Thus using $CF(G)/F(G) \cong C/(C \cap F(G))$ it suffices to show that $O_p(C/(C \cap F(G))) = \{1\}$ for all primes p:

Let $\nu \colon C \to C/(C \cap F(G))$ be the natural homomorphism, and let $P := \nu^{-1}(O_p(C/(C \cap F(G)))) \trianglelefteq C$. Since $C \cap F(G) \trianglelefteq G$ we conclude that $P \trianglelefteq G$. Since $C \cap F(G) \leq Z(C)$ implies that P is nilpotent, we infer $P \leq F(G)$.

b) If N is abelian, then we have $N \leq F(G)$; conversely, if $N \leq F(G)$ then N is soluble and thus elementary abelian. In this case, since we have $F(G) = \prod_{p \mid |F(G)|} O_p(F(G))$ and thus $Z(F(G)) = \prod_{p \mid |F(G)|} Z(O_p(F(G)))$, we infer $\{1\} \neq N \cap Z(F(G)) \trianglelefteq G$, and thus by minimality we get $N \leq Z(F(G))$.

If N is non-abelian, then by the above we have $N \not\leq F(G)$, hence we have $N \cap F(G) = \{1\}$, and thus it is immediate that $F(G) \leq C_G(N)$.

c) Let $C := \bigcap_{i=1}^{k-1} C_G(N_i/N_{i+1}) \trianglelefteq G$, and for $i \in \{1, \ldots, k\}$ let $C_i := C \cap N_i \trianglelefteq G$. Hence $[C_i, C] \leq C \cap [N_i, C_G(N_i/N_{i+1})] \leq C \cap N_{i+1} = C_{i+1}$, thus $C = C_1 \geq \cdots \geq C_k = \{1\}$ is a central series. Hence $C \trianglelefteq G$ is nilpotent and thus $C \leq F(G)$.

Conversely, $F(G)N_{i+1}/N_{i+1} \trianglelefteq G/N_{i+1}$ is nilpotent for $i \in \{1, \ldots, k-1\}$, and thus $F(G)N_{i+1}/N_{i+1} \leq F(G/N_{i+1})$. Moreover, $\{1\} \neq N_i/N_{i+1} \trianglelefteq G/N_{i+1}$ is a minimal normal subgroup, implying $F(G/N_{i+1}) \leq C_{G/N_{i+1}}(N_i/N_{i+1})$. Hence we infer $F(G) \leq C = \bigcap_{i=1}^{k-1} C_G(N_i/N_{i+1})$. $\sharp$

(8.9) Theorem: Gaschütz (1953).
Let G be a finite group. Then $F(G)/\Phi(G) = F(G/\Phi(G))$ is the direct product of minimal abelian normal subgroups of $G/\Phi(G)$.

Proof. We may assume that $\Phi(G) = \{1\}$. Since $F(G) \trianglelefteq G$ is nilpotent we by (8.5) infer $[F(G), F(G)] \leq \Phi(G) = \{1\}$, hence $F(G)$ is abelian. Let $N \trianglelefteq G$ be a maximal direct product of minimal abelian normal subgroups of G; hence we have $N \leq F(G)$.

We show that N has a **complement** $H \leq G$ in G, i. e. we have $H \cap N = \{1\}$ and $G = HN$: Let $H \leq G$ be a minimal element of $\{U \leq G; UN = G\} \neq \emptyset$. Then we have $H \cap N \trianglelefteq H$, and since N is abelian we also have $H \cap N \trianglelefteq N$, implying that $H \cap N \trianglelefteq HN = G$. Assume that $H \cap N \not\leq \Phi(H)$, then there is $U < H$ maximal such that $H \cap N \not\leq U$, hence $H = U(H \cap N)$ and thus $G = HN = U(H \cap N)N = UN$, a contradiction. Thus we have $H \cap N \leq \Phi(H)$, and hence by (8.2) we get $H \cap N \leq \Phi(G) = \{1\}$.

Since $N \leq F(G)$ abelian, and thus $N \leq C_G(F(G))$, we have $H \cap F(G) \trianglelefteq HN = G$, implying $F(G) = F(G) \cap HN = (H \cap F(G))N = (H \cap F(G)) \times N$. Assume that $N < F(G)$, then there is a minimal abelian normal subgroup $\{1\} \neq M \trianglelefteq G$ such $M \leq H \cap F(G)$, implying $N < N \times M \trianglelefteq G$, a contradiction. $\sharp$

9 Generalised Fitting subgroups

(9.1) Definition and Remark. a) A group G such that $[G, G] = G$ is called **perfect**. A perfect group G such that $G/Z(G)$ is simple is called called **quasi-simple**; in particular we have $G/Z(G) \neq \{1\}$ and thus $G \neq \{1\}$.

In this case $G/Z(G)$ is perfect as well, and thus $G/Z(G)$ is non-abelian simple. Moreover, for any proper subnormal subgroup $N \lhd\lhd G$ we have $N \leq Z(G)$; in particular any non-trivial factor group of G is again quasi-simple:

Assume that $N \not\leq Z(G)$, then since a simple group has only the trivial subgroup as a proper subnormal subgroup, we have $NZ(G) = G$, implying $G = [G, G] = [NZ(G), NZ(G)] = [N, N] \leq N < G$, a contradiction. $\sharp$

b) Let G be a finite group. A quasi-simple subnormal subgroup $K \trianglelefteq\trianglelefteq G$ is called a **component** of G; here, being quasi-simple is a property of K alone, while being subnormal refers to the embedding of K as a subgroup of G.

If $K \leq G$ is a component, it is immediate that if $K \leq H \leq G$ then K also is a component of H, and if $K \not\leq N \trianglelefteq G$ then $KN/N \leq G/N$ is a component of G/N. Moreover, if K is a component of a subnormal subgroup of G then K also is a component of G.

(9.2) Proposition. Let G be a finite group, let $Z \leq Z(G)$, and let $K \leq G$ such that KZ/Z is a component of G/Z. Then $[K,K] \leq G$ is a component.

Proof. From $[K,K] = [KZ,KZ]$ we infer $[K,K] \trianglelefteq KZ \trianglelefteq\trianglelefteq G$. Moreover, from KZ/Z being perfect we get $[K,K]Z = KZ$, implying $[K,K] = [KZ,KZ] = [[K,K]Z,[K,K]Z] = [[K,K],[K,K]]$, thus $[K,K]$ is perfect.

Let $N \trianglelefteq [K,K]$, then since $N \trianglelefteq\trianglelefteq KZ$ we distinguish two cases: If firstly $NZ/Z = KZ/Z = [K,K]Z/Z$ then we get $N \leq [K,K] \leq NZ$, which implies $[K,K] = N(Z \cap [K,K])$. Thus $[K,K] = [[K,K],[K,K]] = [N,N] \leq N$.

If secondly $NZ/Z \leq Z(KZ/Z)$, writing $K^{(1)} = [K,K]$, we get $[K^{(1)},N] \leq Z$, implying $[[K^{(1)},N],K^{(1)}] = \{1\}$ and $[[N,K^{(1)}],K^{(1)}] = \{1\}$. It is immediate that using left normed commutators throughout we have the **Witt identity** (1938; **Hall**, 1934) $[x,y^{-1},z]^y \cdot [y,z^{-1},x]^z \cdot [z,x^{-1},y]^x = 1$ for all $x,y,z \in G$. Hence we have $[[K^{(1)},K^{(1)}],N] = \{1\}$ as well. Since $K^{(1)}$ is perfect we infer $[K^{(1)},N] = \{1\}$, hence $N \leq Z(K^{(1)})$. ♯

(9.3) Theorem. Let G be a finite group, let $H \trianglelefteq\trianglelefteq G$, and let $K \leq G$ be a component of G. Then we have $K \leq H$ or $[K,H] = \{1\}$.

In particular, if $K \neq L \leq G$ is a component of G then we have $[K,L] = \{1\}$.

Proof. We may assume that $H < G$. If $K = G$ then G is quasi-simple, and hence $H \leq Z(G)$, implying $[H,G] = \{1\}$. Hence we may assume that $K < G$ as well, and there are normal subgroups such that $K \leq N \lhd G$ and $H \leq M \lhd G$.

It is immediate that we have $[x,z]^y = [xy,z] \cdot [y,z]^{-1}$ for all $x,y,z \in G$. Hence letting $\widetilde{H} := [K,H] \leq N \cap M$ we infer $K \leq N \cap N_G(\widetilde{H}) = N_N(\widetilde{H}) =: \widetilde{G}$, and thus K is a component of $\widetilde{G}$ and $\widetilde{H} \trianglelefteq \widetilde{G}$. Hence by induction on $|G|$ applied to $\widetilde{G} \leq N < G$ we get $K \leq \widetilde{H}$ or $[K,\widetilde{H}] = \{1\}$.

In the former case we have $K \leq \widetilde{H} \leq M < G$, hence K is a component of M and $H \trianglelefteq\trianglelefteq M$, and by induction on $|G|$ applied to M we get $K \leq H$ or $[K,H] = \{1\}$. In the latter case we have $[[H,K],K] = [[K,H],K] = \{1\}$, hence Witt's identity implies $\{1\} = [[K,K],H] = [K,H]$. ♯

(9.4) Proposition. Let G be a finite group.
a) Let $K \leq G$ be a simple component of G, i. e. we have $Z(K) = \{1\}$. Then $\langle K^G \rangle \trianglelefteq G$ is a non-abelian minimal normal subgroup, being the direct product of the distinct components G-conjugate to K.
b) Let $\{1\} \neq N \trianglelefteq G$ be a non-abelian minimal normal subgroup. Then there is a simple component $K \leq G$ such that $N = \langle K^G \rangle$.

Proof. a) Let $\{t_1,\ldots,t_n\} \subseteq G$ be a transversal of $N_G(K)\backslash G$, and let $K_i := K^{t_i}$ for $i \in \{1,\ldots,n\}$. Hence we have $[K_i,K_j] = \{1\}$ for $i \neq j$, implying that $\langle K^G \rangle = \langle K_1,\ldots,K_n \rangle = K_1 \cdots K_n$ is a **central product**; this does not depend on the order of the factors. Letting $\widehat{K}_i := K_1 \cdots K_{i-1}K_{i+1} \cdots K_n \leq G$ we have $K_i \cap \widehat{K}_i \leq Z(K_i) = \{1\}$, and thus $\langle K^G \rangle \cong \prod_{i=1}^n K_i$.

Let $\{1\} \neq N \trianglelefteq G$ be a normal subgroup such that $N \leq \langle K^G \rangle$. Assume that $N \cap K_i = \{1\}$ for all $i \in \{1, \ldots, n\}$. Then we have $[N, K_i] = \{1\}$, hence $N \leq Z(\langle K^G \rangle) \cong Z(\prod_{i=1}^n K_i) = \{1\}$, a contradiction. Thus we may assume that $\{1\} \neq N \cap K \trianglelefteq K$, hence we infer $K \leq N$ and thus $\langle K^G \rangle \leq N$.

b) If $N = G$ then G is non-abelian simple, and thus we have $K = G$. Hence we may assume that $N < G$. Let $\{1\} \leq M \trianglelefteq N$ be a minimal normal subgroup of N, then we have $\langle M^G \rangle \trianglelefteq G$ and thus $\langle M^G \rangle = N$. Assume that M is abelian, then since there are only finitely many G-conjugates of M we infer that $\langle M^G \rangle = N$ is soluble, which by the minimality of N implies that N is abelian, a contradiction.

Hence M is non-abelian, and by induction on $|G|$ there is a simple component $K \leq N$ such that $M = \langle K^N \rangle$. Since $N \lhd G$ we conclude that K also is a component of G, and we have $N = \langle M^G \rangle = \langle (K^N)^G \rangle = \langle K^G \rangle$. $\sharp$

(9.5) Definition and Remark. a) Let G be a finite group, and $K_1, \ldots, K_n \leq G$ be the components of G, for some $n \in \mathbb{N}_0$; for $i \neq j \in \{1, \ldots, n\}$ we have $[K_i, K_j] = \{1\}$. The **component subgroup** $E(G) := \langle K_1, \ldots, K_n \rangle = K_1 \cdots K_n \trianglelefteq G$ is characteristic; for $n = 0$ we let $E(G) := \{1\}$, which e. g. is the case if G is soluble. We have $[E(G), E(G)] = [K_1, K_1] \cdots [K_n, K_n] = K_1 \cdots K_n = E(G)$.

Letting $\widehat{K}_i := K_1 \cdots K_{i-1}K_{i+1} \cdots K_n \leq G$ yields $[K_i, \widehat{K}_i] = \{1\}$. Let $Z_i := Z(K_i)$ and $Z := Z_1 \cdots Z_n \leq G$, then we have $Z \leq Z(E(G))$, and if conversely $g = g_1 \cdots g_n \in Z(E(G))$, where $g_i \in K_i$, then we infer $gg_i^{-1} \in \widehat{K}_i$ and thus $g_i \in Z_i$, implying $Z \cap K_i = Z_i$ and $Z = Z(E(G)) \trianglelefteq G$ characteristic.

Thus $E_i := K_iZ/Z \cong K_i/(K_i \cap Z) = K_i/Z_i$ is non-abelian simple. The map $\pi \colon \prod_{i=1}^n K_i \to E(G)/Z \colon [g_1, \ldots, g_n] \mapsto g_1 \cdots g_n Z$ is an epimorphism such that $\ker(\pi) = \prod_{i=1}^n Z_i$. Hence we have $E(G)/Z \cong \prod_{i=1}^n K_i/Z_i = \prod_{i=1}^n E_i$.

b) Let $F^*(G) := F(G)E(G) \trianglelefteq G$ characteristic be the **generalised Fitting subgroup** of G. Since $[F(G), E(G)] = \{1\}$ it is a central product. Since $Z \trianglelefteq G$ is abelian we have $Z \leq F(G) \cap E(G) \trianglelefteq E(G)$, and since $F(G) \cap E(G)$ is nilpotent and $E(G)/Z$ has only non-abelian composition factors we infer $Z = F(G) \cap E(G)$.

Then $F^*(G)$ contains any minimal subnormal subgroup $N \trianglelefteq\trianglelefteq G$; hence in particular for $G \neq \{1\}$ we have $F^*(G) \neq \{1\}$: If N is abelian then we have $N \leq F(G)$; and if N is non-abelian, then since N is simple we conclude that N is component of G, and thus $N \leq E(G)$.

Moreover, $F^*(G)$ contains any minimal normal subgroup $N \trianglelefteq G$: If N is abelian then we have $N \leq F(G)$, and if N is non-abelian then there is a component $K \leq G$ such that $N = \langle K^G \rangle$, implying $N \leq E(G)$.

(9.6) Theorem. Let G be a finite group.
a) If $F(G) = \{1\}$ then we have $F^*(G) = E(G) = \langle \{1\} \neq N \trianglelefteq G \text{ minimal} \rangle$.

b) Let $N \trianglelefteq\trianglelefteq G$. Then we have $F^*(N) \leq N \cap F^*(G)$ and $E(N) \cdot C_{E(G)}(E(N)) = E(G)$, implying $E(N) \trianglelefteq E(G)$.
c) We have $C_G(F^*(G)) \leq F^*(G)$, i. e. we have $C_G(F^*(G)) = Z(F^*(G))$.

Proof. a) We have $\langle \{1\} \neq N \trianglelefteq G \text{ minimal} \rangle \leq F^*(G) = E(G)$. Conversely, for any component $K \leq G$ we have $Z(K) \trianglelefteq\trianglelefteq G$, thus $Z(K) \leq F(G) = \{1\}$ implies that K is simple. Hence $\langle K^G \rangle \trianglelefteq G$ is a minimal normal subgroup, where we have $K \leq \langle K^G \rangle \leq E(G) = F^*(G)$.

b) Let $K_1, \ldots, K_m \leq N$ be the components of N, for some $m \in \mathbb{N}_0$. Since the components of N also are components of G, the components of G are given as $K_1, \ldots, K_m, K_{m+1}, \ldots, K_n \leq G$, for some $n \in \mathbb{N}_0$. Since $[K_i, K_j] = \{1\}$ for $i \neq j$ we have $K_{m+1} \cdots K_n \leq C_{E(G)}(K_1 \cdots K_m)$ and thus using $E(N) = K_1 \cdots K_m$ we get $E(G) = K_1 \cdots K_m K_{m+1} \cdots K_n \leq E(N) \cdot C_{E(G)}(E(N)) \leq E(G)$. Thus from $F(N) \leq F(G)$ we get $F^*(N) = F(N)E(N) \leq N \cap F(G)E(G) = N \cap F^*(G)$.

c) Let $C := C_G(F^*(G)) \trianglelefteq G$. We have $Z(C) \leq F(C) \leq F^*(C) \leq C \cap F^*(G) = C_G(F^*(G)) \cap F^*(G) = Z(F^*(G)) \leq Z(C)$, implying $F^*(C) = F(C) = Z(C)$ and $E(C) = \{1\}$. Assume that $E(C/Z(C)) \neq \{1\}$, then there is $K \leq C$ such that $KZ(C)/Z(C)$ is a component of $C/Z(C)$. Hence by (9.2) we infer that $[K, K]$ is a component of C, a contradiction. Thus $F^*(C/Z(C)) = F(C/Z(C))$ is nilpotent, implying that C is nilpotent as well, hence $C \leq F(G) \leq F^*(G)$. $\sharp$

10 Exercises (in German)

(10.1) Aufgabe: Rechnen in Gruppen.
Es sei G eine Gruppe.
a) Man bestimme alle Elemente $g \in G$ mit $g^2 = g$.
b) Für alle $f, g, h \in G$ zeige man die folgenden **Kürzungsregeln**: Es ist $fh = gh$ genau dann, wenn $f = g$ ist, und dies gilt genau dann, wenn $hf = hg$ ist.
c) Man zeige: G ist genau dann abelsch, wenn $g^2h^2 = (gh)^2$ für alle $g, h \in G$.

(10.2) Aufgabe: Untergruppen.
Es sei G eine Gruppe. Man zeige:
a) Eine Teilmenge $\emptyset \neq U \subseteq G$ ist genau dann eine Untergruppe, wenn für alle $g, h \in U$ auch $gh^{-1} \in U$ ist.
b) Eine endliche Teilmenge $\emptyset \neq U \subseteq G$ ist genau dann eine Untergruppe, wenn für alle $g, h \in U$ auch $gh \in U$ ist. Kann auf die Voraussetzung der Endlichkeit verzichtet werden?
c) Sind $U, V \leq G$, so ist $U \cup V$ genau dann eine Untergruppe, wenn $U \subseteq V$ oder $V \subseteq U$ gilt.

(10.3) Aufgabe: Komplexprodukt.
Es seien G eine Gruppe und $A, B \subseteq G$. Dann heißt $AB := \{ab \in G; a \in A, b \in B\} \subseteq G$ das **Komplexprodukt** von A und B. Für Untergruppen $U, V \leq G$ zeige man:
a) Sind U und V endlich, so gilt $|UV| \cdot |U \cap V| = |U| \cdot |V|$.
b) Es ist $UV \subseteq G$ genau dann eine Untergruppe, wenn $VU \subseteq UV$ gilt. Was folgt daraus für abelsche Gruppen?

(10.4) Aufgabe: Multiplikationstafeln.
Man gebe die Multiplikationstafeln der folgenden Gruppen an, und bestimme die Elementordnungen. Welche dieser Gruppen sind abelsch, welche sind zyklisch?
a) Symmetrische Gruppen $\mathcal{S}_2$ und $\mathcal{S}_3$.
b) Alle Gruppen G der Ordnung $|G| \leq 4$.

(10.5) Aufgabe: Matrixgruppen.
Es sei $G := \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in \mathbb{R}^{2\times 2}; a, b \in \mathbb{R} \text{ mit } a^2 + b^2 \neq 0 \right\}$. Man zeige: G ist eine Untergruppe von $\mathrm{GL}_2(\mathbb{R})$.

(10.6) Aufgabe: Symmetrische Gruppen.
Es seien $n \geq 2$ und $\mathcal{S}_n$ die zugehörige symmetrische Gruppe. Man zeige:
a) Es ist $\mathcal{S}_n = \langle (1, 2), (2, 3), \ldots, (n-1, n) \rangle$.
b) Es ist $\mathcal{S}_n = \langle (1, 2), (1, 2, \ldots, n) \rangle$.

(10.7) Aufgabe: Diedergruppen.
Es seien $n \geq 3$ sowie $\tau_n = (1, \ldots, n) \in D_{2n}$ und $T_n := \langle \tau_n \rangle \leq D_{2n}$. Weiter seien $\sigma_n := (1)(2, n)(3, n-1) \cdots (\frac{n+1}{2}, \frac{n+3}{2}) \in D_{2n}$ für ungerades n, und $\sigma_n := (1)(\frac{n+2}{2})(2, n)(3, n-1) \cdots (\frac{n}{2}, \frac{n+4}{2}) \in D_{2n}$ für gerades n.
a) Man zeige: Es ist $D_{2n} = \langle \sigma_n, \tau_n \rangle$, es gilt $\sigma_n^{-1} \tau_n \sigma_n = \tau_n^{-1}$, und es ist $D_{2n} = T_n \dot\cup \sigma_n T_n$ mit $|T_n| = n = |\sigma_n T_n|$. Ist D_{2n} abelsch?
b) Man zeige: Jedes Element $\pi \in D_{2n}$ kann eindeutig in der Form $\pi = \sigma^i \tau^k$, mit $i \in \{0, 1\}$ und $k \in \{0, \ldots, n-1\}$, geschrieben werden. Man beschreibe die Multiplikation in D_{2n} mit Hilfe der Exponenten i und k.
c) Man zeichne Hasse-Diagramme der Untergruppenverbände von D_8 und D_{10}.

(10.8) Aufgabe: Tetraedergruppe.
Man bestimme die Symmetriegruppe eines regulären Tetraeders im Euklidischen Raum $\mathbb{R}^3$ als Gruppe von Permutationen seiner vier Ecken. Wieviele Drehungen und wieviele Spiegelungen gibt es? Man zeige, daß die Menge der Drehungen eine Untergruppe bildet.

(10.9) Aufgabe: Elementordnungen.
Es sei G eine endliche Gruppe. Man zeige:
a) Für alle $g, h \in G$ gilt $|g^{-1}| = |g|$ sowie $|gh| = |hg|$ und $|h^{-1}gh| = |g|$.
b) Sind $g, h \in G$ mit $gh = hg$, so gilt genau dann $|gh| = |g| \cdot |h|$, wenn $\mathrm{ggT}(|g|, |h|) = 1$ ist. Was gilt im Falle $gh \neq hg$?
c) Ist G abelsch, so gibt es ein $g \in G$ mit $|g| = \exp(G)$. Gilt dies auch für nicht-abelsche Gruppen?
d) Ist $\exp(G) \leq 2$, so ist G abelsch.

(10.10) Aufgabe: Index.
Es seien G eine Gruppe und $U, V \leq G$. Man zeige:
a) Sind $|U|$ und $|V|$ endlich mit $\mathrm{ggT}(|U|, |V|) = 1$, so gilt $U \cap V = \{1\}$.
b) Sind $U \leq V \leq G$ mit $[G\colon U]$ endlich, so sind auch $[G\colon V]$ und $[V\colon U]$ endlich, und es gilt $[G\colon U] = [G\colon V] \cdot [V\colon U]$.
c) Man zeige den **Satz von Poincaré**: Sind $[G\colon U]$ und $[G\colon V]$ endlich, so ist auch $[G\colon (U \cap V)]$ endlich und es gilt $[G\colon (U \cap V)] \leq [G\colon U] \cdot [G\colon V]$. Man gebe eine hinreichende Bedingung für Gleichheit an.

(10.11) Aufgabe: Transversalen.
Es seien G eine endliche Gruppe und $U \leq G$. Man zeige: Es gibt eine Rechtstransversale für U in G, die auch eine Linkstransversale ist.

Hinweis. Man benutze den Heiratssatz der Graphentheorie.

(10.12) Aufgabe: Satz von Euler-Fermat.
a) Es sei $n \in \mathbb{N}$. Man zeige: $(\mathbb{Z}/n\mathbb{Z})^* := \{\overline{k} \in \mathbb{Z}/n\mathbb{Z}; \mathrm{ggT}(k, n) = 1\}$ ist eine multiplikative Gruppe; sie heißt Gruppe der **primen Restklassen** modulo n. Wann ist $(\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$ eine multiplikative Gruppe?

b) Für $n \in \mathbb{N}$ und $k \in \mathbb{Z}$ mit $\operatorname{ggT}(k, n) = 1$ zeige man: Es gilt $m^{\varphi(n)} \equiv 1 \pmod{n}$; dabei sei φ die Euler-Funktion.
c) Es seien p eine Primzahl und $k \in \mathbb{Z}$. Man zeige: Es gilt $k^p \equiv k \pmod{p}$.

(10.13) Aufgabe: Satz von Wilson.
a) Es seien G eine endliche abelsche Gruppe und $U := \{g \in G; g^2 = 1\} \subseteq G$. In Unterscheidung der Fälle $|U| = 2$ und $|U| \neq 2$ bestimme man $\prod_{g \in G} g \in G$.
b) Es sei p eine Primzahl. Durch Anwendung von (a) auf $(\mathbb{Z}/p\mathbb{Z})^*$ zeige man den **Satz von Wilson**: Es gilt $(p-1)! \equiv -1 \pmod{p}$.

(10.14) Aufgabe: Einfache abelsche Gruppen.
Man zeige: Die einfachen abelschen Gruppen sind genau die zyklischen Gruppen von Primzahlordnung.

(10.15) Aufgabe: Untergruppen von kleinem Index.
a) Es seien G eine Gruppe und $U \leq G$ mit $[G \colon U] \leq 2$. Man zeige: Es ist $U \trianglelefteq G$. Kann man das auf den Fall $[G \colon U] > 2$ verallgemeinern?
b) Welche Untergruppen der symmetrischen Gruppe $\mathcal{S}_3$ und der Diedergruppen D_8 und D_{10} sind normal?

(10.16) Aufgabe: Gruppenhomomorphismen.
Man gebe einen Gruppenisomorphismus $(\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ an.

(10.17) Aufgabe: Symmetrische Gruppen.
Es seien $X \neq \emptyset \neq Y$ endliche Mengen. Man zeige: Es gibt genau dann einen Isomorphismus $\mathcal{S}_X \cong \mathcal{S}_Y$, wenn $|X| = |Y|$ gilt. Kann auf die Voraussetzung der Endlichkeit verzichtet werden?

(10.18) Aufgabe: Signum.
Es seien $n \in \mathbb{N}$ und $\operatorname{sgn} \colon \mathcal{S}_n \to \{\pm 1\}$ die Signum-Abbildung. Man zeige:
a) Ist $\pi \in \mathcal{S}_n$ Produkt von $r \in \mathbb{N}$ disjunkten Zykeln der Längen $k_1, \ldots, k_r$, so ist $\operatorname{sgn}(\pi) = \prod_{i=1}^{r} (-1)^{k_i - 1} = (-1)^{n-r}$. Was spricht dagegen, dies als Definition der Signum-Abbildung zu verwenden?
b) Für $\pi \in \mathcal{S}_n$ ist $\operatorname{sgn}(\pi) = \prod_{i,j \in \{1,\ldots,n\}, i>j} \frac{i^\pi - j^\pi}{i-j}$.

(10.19) Aufgabe: Alternierende Gruppen.
a) Man bestimme die Elementordnungen der alternierenden Gruppen $\mathcal{A}_2$, $\mathcal{A}_3$ und $\mathcal{A}_4$. Welche dieser Gruppen sind abelsch, welche zyklisch?
b) Man bestimme die Untergruppen von $\mathcal{A}_2$, $\mathcal{A}_3$ und $\mathcal{A}_4$, und zeiche die Hasse-Diagramme der Untergruppenverbände. Welche Untergruppen sind normal?

(10.20) Aufgabe: Lineare Gruppen.
Es sei $\mathbb{F}_q$ der Körper mit $q \in \mathbb{N}$ Elementen. Für $n \in \mathbb{N}$ bestimme man die Ordnungen der linearen Gruppen $\mathrm{GL}_n(\mathbb{F}_q)$ und $\mathrm{SL}_n(\mathbb{F}_q)$.

(10.21) Aufgabe: Isomorphiesatz.
Es seien G eine Gruppe, $U \leq G$ und $M, N \trianglelefteq G$ mit $M \leq N$. Man zeige:
a) Es ist $UN \leq G$ und $U/(U \cap N) \cong UN/N$.
b) Es gilt $(G/M)/(N/M) \cong G/N$.
c) Der natürliche Epimorphismus $G \to G/N$ induziert eine inklusionserhaltende Bijektion $\{U \leq G; N \leq U\} \to \{V \leq G/N\}$, die Normalität und Indizes erhält.

(10.22) Aufgabe: Automorphismengruppen.
Es seien G eine Gruppe und $\mathrm{Aut}(G)$ die Menge aller Automorphismen von G.
a) Man zeige: $\mathrm{Aut}(G)$ ist eine Gruppe, die **Automorphismengruppe** von G.
b) Für $g \in G$ sei $\kappa_g \colon G \to G \colon h \mapsto h^g := g^{-1}hg$ die zugehörige **Konjugationsabbildung**. Man zeige: Für alle $g \in G$ ist $\kappa_g \in \mathrm{Aut}(G)$, und die Abbildung $\kappa \colon G \to \mathrm{Aut}(G) \colon g \to \kappa_g$ ist ein Homomorphismus.
c) Das Bild $\mathrm{Inn}(G) := \mathrm{im}(\kappa) \leq \mathrm{Aut}(G)$ heißt die Gruppe der **inneren Automorphismen** von G. Man zeige: Es ist $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. Eine Untergruppe $U \leq G$ ist genau dann normal, wenn $U^\alpha \subseteq U$ für alle $\alpha \in \mathrm{Inn}(G)$ gilt.
d) Der Kern $Z(G) := \ker(\kappa) \trianglelefteq G$ heißt das **Zentrum** von G. Man zeige: Es ist $Z(G) = \{g \in G; gh = hg \text{ for all } h \in G\}$ und $G/Z(G) \cong \mathrm{Inn}(G)$. Man gebe eine hinreichende und notwendige Bedingung für $\mathrm{Inn}(G) = \{1\}$ an.

(10.23) Aufgabe: Semidirektes Produkt.
a) Es seien H und N Gruppen, sowie $\alpha \colon H \to \mathrm{Aut}(N) \colon h \mapsto \overline{h}$ ein Homomorphismus. Man zeige, daß das mengentheoretische Produkt $H \times N$ zusammen mit $(h, n) \cdot (h', n') := (hh', n^{\overline{h'}} n')$ eine Gruppe ist; sie heißt das **semidirekt Produkt** von H mit N und wird mit $H \ltimes_\alpha N$ bezeichnet.
b) Man gebe das neutrale Element von $H \ltimes_\alpha N$ und das Inverse zu $(h, n) \in H \ltimes_\alpha N$ an. Man zeige, daß N als Normalteiler und H als Untergruppe von $H \ltimes_\alpha N$ aufgefaßt werden können, so daß $H \cap N = \{1\}$ gilt
c) Das semidirekte Produkt zum trivialen Homomorphismus $H \to \mathrm{Aut}(N)$ heißt das **direkte Produkt** von H und N und wird ebenfalls mit $H \times N$ bezeichnet. Man beschreibe Multiplikation und Inversion in $H \times N$.
d) Es seien $\beta \in \mathrm{Aut}(H)$, $\gamma \in \mathrm{Aut}(N)$ und $\widetilde{\alpha} \colon H \to \mathrm{Aut}(N) \colon h \mapsto (\overline{h\beta^{-1}})^\gamma$. Man zeige: Es ist $H \ltimes_\alpha N \to H \ltimes_{\widetilde{\alpha}} N \colon (h, n) \mapsto (h\beta, n\gamma)$ ein Gruppenisomorphismus.
e) Es seien G eine Gruppe, sowie $N \trianglelefteq G$ und $H \leq G$ mit $G = HN$ und $H \cap N = \{1\}$; dann heißt H ein **Komplement** zu N in G. Man zeige: Es ist $G \cong H \ltimes_\alpha N$ für $\alpha \colon H \to \mathrm{Aut}(N)$ geeignet. Ist zudem $H \trianglelefteq G$, so ist $G \cong H \times N$.

(10.24) Aufgabe: Zyklische Gruppen.
a) Es sei $n = \prod_i p_i^{e_i} \in \mathbb{N}$ die Zerlegung von n in Potenzen paarweise verschiedener Primzahlen $p_i \in \mathbb{N}$, mit $e_i \in \mathbb{N}$. Man zeige: Es ist $\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^*$ und $\mathrm{Aut}(C_n) \cong \prod_i \mathrm{Aut}(C_{p_i^{e_i}})$.
b) Man zeige: Für $e \geq 2$ ist $\mathrm{Aut}(C_{2^e}) \cong C_2 \times C_{2^{e-2}}$. Für eine Primzahl $p \geq 3$ und $e \geq 1$ ist $\mathrm{Aut}(C_{p^e}) \cong C_{(p-1)p^{e-1}} \cong C_{p-1} \times C_{p^{e-1}}$.

Hinweis zu (b). Für $p = 2$ untersuche man die Ordnung von $5 \in \mathbb{Z}/2^e\mathbb{Z})^*$. Für $p \geq 3$ untersuche man die Ordnung von $1 + p \in (\mathbb{Z}/p^e\mathbb{Z})^*$.

(10.25) Aufgabe: Kleinsche Vierergruppe.
Es sei $V_4 := \langle (1,2)(3,4), (1,3)(2,4) \rangle \leq \mathcal{S}_4$ die **Kleinsche Vierergruppe**.
a) Man bestimme die Gruppenordnung, die Elementordnungen, sowie die Untergruppen von V_4 und zeichne das Hasse-Diagramm des Untergruppenverbandes. Welche Untergruppen sind normal? Ist V_4 abelsch?
b) Man bestimme $\mathrm{Inn}(V_4)$ und $\mathrm{Aut}(V_4)$. Zu welcher bekannten Gruppe ist $\mathrm{Aut}(V_4)$ isomorph?

(10.26) Aufgabe: Quaternionengruppe.
Es seien $A, B \in GL_2(\mathbb{C})$ gegeben durch

$$A := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad \text{und} \quad B := \begin{bmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{bmatrix},$$

sowie $Q_8 := \langle A, B \rangle \leq GL_2(\mathbb{C})$ die **Quaternionengruppe**.
a) Man bestimme die Gruppenordnung und die Elementordnungen, sowie die Untergruppen von Q_8 und zeichne das Hasse-Diagramm des Untergruppenverbandes. Welche Untergruppen sind normal? Ist Q_8 abelsch?
b) Man gebe einen Monomorphismus $\varphi\colon Q_8 \to \mathcal{S}_8$ an, und bestimme die φ-Bilder der Untergruppen von Q_8.

(10.27) Aufgabe: Konjugiertenklassen symmetrischer Gruppen.
a) Es sei $n \in \mathbb{N}$. Ist $\pi \in \mathcal{S}_n$ ein Produkt von $r \in \mathbb{N}$ disjunkten Zykeln der Längen $n_1 \geq n_2 \geq \cdots \geq n_r \geq 1$, so heißt die nicht-aufsteigende Folge $[n_1, \ldots, n_r]$ der **Zykeltyp** von π. Man zeige: Elemente von $\mathcal{S}_n$ sind genau dann konjugiert in $\mathcal{S}_n$, wenn sie den gleichen Zykeltyp besitzen.
b) Man zeige: $\mathcal{A}_n$ ist eine Vereinigung von $\mathcal{S}_n$-Konjugiertenklassen, und eine $\mathcal{S}_n$-Konjugiertenklasse in $\mathcal{A}_n$ besteht entweder aus einer $\mathcal{A}_n$-Konjugiertenklasse oder zwei $\mathcal{A}_n$-Konjugiertenklassen gleicher Länge.
c) Man bestimme die Konjugiertenklassen in $\mathcal{S}_n$ und $\mathcal{A}_n$ für $n \in \{3,4,5\}$. Insbesondere folgere man, daß $\mathcal{A}_5$ eine einfache Gruppe ist.

(10.28) Aufgabe: Gruppenoperationen.
Es sei G eine endliche Gruppe.
a) Es sei $H \leq G$ mit $[G\colon H] = n$. Man zeige: G besitzt einen Normalteiler $N \trianglelefteq G$ mit $n \mid [G\colon N] \mid n!$.
b) Es sei $|G| = 2m$ für ein $m \in \mathbb{N}_0$ ungerade. Man zeige: G besitzt einen Normalteiler $N \trianglelefteq G$ mit $[G\colon N] = 2$.

(10.29) Aufgabe: Operationen abelscher Gruppen.
Es sei G eine endliche abelsche Gruppe.
a) Man bestimme die treuen transitiven G-Mengen bis auf Isomorphie.
b) Man zeige: Ist X eine treue transitive G-Menge, so gilt $G \cong C_{\mathcal{S}_X}(G)$.

(10.30) Aufgabe: Riffle-Shuffle und Mongean-Shuffle.
a) Für $k \in \mathbb{N}$ und $n \in \{2k, 2k-1\}$ seien $\alpha_n, \beta_n \in \mathcal{S}_n$ gegeben durch:

	1	2	3	4	$\ldots$	$n-3$	$n-2$	$n-1$	n
α_n	1	$k+1$	2	$k+2$	$\ldots$				
β_n					$\ldots$	$k-3$	$n-2$	$k-1$	n

Man untersuche die Gruppe $\langle \alpha_n, \beta_n \rangle \leq \mathcal{S}_n$.
b) Für $k \in \mathbb{N}$ und $n \in \{2k, 2k+1\}$ seien $\gamma_n, \delta_n \in \mathcal{S}_n$ gegeben durch:

	1	2	$\ldots$	$k-1$	k	$k+1$	$k+2$	$k+3$	$\ldots$	$n-1$	n
γ_n			$\ldots$	4	2	1	3	5	$\ldots$		
δ_n	n	$n-1$	$\ldots$						$\ldots$	2	1

Man untersuche die Gruppe $\langle \gamma_n, \delta_n \rangle \leq \mathcal{S}_n$.

(10.31) Aufgabe: Tetraederfärbungen.
Man bestimme die Anzahl der verschiedenen Färbungen der vier Ecken eines regulären Tetraeders mit bis zu vier Farben, bezüglich seiner vollen Symmetriegruppe und bezüglich seiner Drehsymmetriegruppe. Wie kann man das Ergebnis geometrisch interpretieren?

(10.32) Aufgabe: Echte Untergruppen.
Es seien $|G|$ endlich und $U < G$. Man zeige: Es ist $\bigcup_{g \in G} g^{-1}Ug \neq G$.

(10.33) Aufgabe: Zentrum.
Es sei G eine Gruppe.
a) Man zeige: Ist $G/Z(G)$ zyklisch, so ist G abelsch.
b) Es sei p eine Primzahl. Man zeige: Ist $|G| = p^2$, so ist G abelsch. Ist $|G| = p^3$, so ist G abelsch oder $|Z(G)| = p$.
c) Man bestimme die Zentren der symmetrischen Gruppe $\mathcal{S}_3$, der Diedergruppe D_8 und der Quaternionengruppe Q_8.

(10.34) Aufgabe: Elemente von Primzahlordnung.
Es seien G eine endliche Gruppe und p eine Primzahl. Man zeige: Es ist $|\{g \in G; g^p = 1\}| \equiv 0 \pmod{p}$.

(10.35) Aufgabe: Anzahl von Sylow-Gruppen.
Es seien G eine endliche Gruppe, p eine Primzahl, und $d \in \mathbb{N}$, so daß für alle $P, P' \in \mathrm{Syl}_p(G)$ mit $P \neq P'$ gilt $p^d \mid [P \colon (P \cap P')]$. Man zeige: Es gilt $|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p^d}$.

Hinweis. Man betrachte die P-$N_G(P)$-Doppelnebenklassen in G.

(10.36) Aufgabe: Sylow-Gruppen voller linearer Gruppen.
Es seien p eine Primzahl, $\mathbb{F}_q$ der Körper mit $q = p^f$ Elementen und $G := \mathrm{GL}_n(\mathbb{F}_q)$.
a) Es seien $B := \{[a_{ij}] \in G; a_{ij} = 0$ für alle $1 \leq j < i \leq n\}$ die **Borel-Gruppe** der oberen Dreiecksmatrizen und $U := \{[a_{ij}] \in B; a_{ii} = 1$ für alle $i \in \{1, \ldots, n\}\}$ die **unipotente** Untergruppe. Man zeige: Es ist $U \in \mathrm{Syl}_p(G)$ und es gilt $N_G(U) = B$. Man schreibe B als semidirektes Produkt.
b) Es sei $P \leq G$ eine p-Gruppe. Man zeige: Es gibt ein Element $0 \neq v \in \mathbb{F}_q^n$ mit $vg = v$ für alle $g \in P$.

Hinweis zu (a). Man betrachte **Fahnen** $\{0\} = V_0 < V_1 < \ldots < V_n = \mathbb{F}_q^n$ von $\mathbb{F}_q$-Teilräumen.

(10.37) Aufgabe: Gruppenordnungen.
Es seien $p, q, r \in \mathbb{N}$ paarweise verschieden Primzahlen, und G eine endliche Gruppe. Man zeige:
a) Ist $|G| = pq$ mit $p < q$, so besitzt G eine normale q-Sylow-Gruppe; ist zudem $q \not\equiv 1 \pmod{p}$, so ist G zyklisch. Kann auf die Voraussetzung $q \not\equiv 1 \pmod{p}$ verzichtet werden?
b) Ist $|G| = 2p$, so ist $G \cong C_{2p}$ oder $G \cong D_{2p}$.
c) Ist $|G| \in \{p^2q, p^2q^2, pqr\}$, so ist besitzt G einen Normalteiler $\{1\} \neq N \lhd G$.
d) Ist $|G| \in \{2n, 8k\}$, für $n > 1$ ungerade und $k \in \{1, \ldots, 8\}$, so ist besitzt G einen Normalteiler $\{1\} \neq N \lhd G$.

(10.38) Aufgabe: Gruppen kleiner Ordnung.
Man bestimme bis auf Isomorphie
a) die nicht-abelschen Gruppen G der Ordnung $|G| = 8$,
b) die Gruppen G der Ordnung $|G| = 12$,
c) die Gruppen G der Ordnung $|G| = 21$.

(10.39) Aufgabe: Transitive Operationen.
Es seien G eine endliche Gruppe, X eine transitive G-Menge, $x \in X$ und $P \in \mathrm{Syl}_p(\mathrm{Stab}_G(x))$ für eine Primzahl $p \in \mathbb{N}$. Man zeige: $N_G(P)$ operiert transitiv auf $\mathrm{Fix}_X(P)$.

(10.40) Aufgabe: Unterbahnen.
Es seien G eine endliche Gruppe, X eine transitive G-Menge, $x \in X$ und $H := \mathrm{Stab}_G(x)$. Man zeige: Ist $G = \coprod_{i \in \mathcal{I}} Hg_iH$ die Zerlegung von G in H-H-Doppelnebenklassen, für eine Indexmenge $\mathcal{I} \neq \emptyset$ und $g_i \in G$, so ist $X = \coprod_{i \in \mathcal{I}} xHg_iH$ die Zerlegung von X in H-Bahnen. Wann ist X eine 2-fach transitive G-Menge?

(10.41) Aufgabe: Produktoperation.
Es seien G eine Gruppe, X eine endliche transitive G-Menge, H eine Gruppe und Y eine H-Menge. Man zeige: Das Kranzprodukt $H \wr_X G$ operiert auf $Y^X :=$

$\{p\colon X \to Y\}$ via der **Produktoperation** $p \mapsto p^{(g,f)}\colon X \to Y\colon x \mapsto (xg^{-1}p)^{xf}$. Sind X und Y treu mit $|Y| \geq 2$, so auch Y^X; ist Y transitiv, so auch Y^X.

(10.42) Aufgabe: Kranzprodukt $C_3 \wr C_2$.
Es seien X die reguläre C_2-Menge und $G := C_3 \wr_X C_2$, sowie Y die reguläre C_3-Menge. Man gebe den durch die Standardoperation induzierten Homomorphismus $G \to \mathcal{S}_{X\times Y}$ und den durch die Produktoperation induzierten Homomorphismus $G \to \mathcal{S}_{X^Y}$ an, und zeige $G \cong \mathcal{S}_3 \times C_3$.

(10.43) Aufgabe: Imprimitive Operation.
Es sei $G := \langle (1,6)(2,7,8,5)(3,4), (1,8)(2,3)(4,7,5) \rangle \leq \mathcal{S}_8$. Man gebe ein nichttriviales Blocksystem $\mathcal{B}$ für G und den dadurch induzierten Homomorphismus $G \to \mathcal{S}_B \wr_{\mathcal{B}} \mathcal{S}_{\mathcal{B}}$, wobei $B \in \mathcal{B}$, an.

(10.44) Aufgabe: Imprimitive Operation.
Man gebe ein Blocksystem aus 2-elementigen Blöcken für die Diedergruppe $D_{4n} \leq \mathcal{S}_{2n}$, wobei $n \in \mathbb{N}$, und den dadurch induzierten Homomorphismus $D_{4n} \to \mathcal{S}_2 \wr \mathcal{S}_n$ an. Gibt es solch ein Blocksystem auch für $D_{4n+2} \leq \mathcal{S}_{2n+1}$?

(10.45) Aufgabe: Zentralisatoren in $\mathcal{S}_n$.
Es seien $n \in \mathbb{N}$ und $\pi_\lambda \in \mathcal{S}_n$ vom Zykeltyp $\lambda := [1^{a_1}, 2^{a_2}, \ldots, n^{a_n}]$, wobei $a_i \in \mathbb{N}_0$. Man zeige: Der Zentralisator $C_{\mathcal{S}_n}(\pi_\lambda)$ ist ein direktes Produkt der Form $C_{\mathcal{S}_n}(\pi_\lambda) \cong \prod_{i=1}^n (C_i \wr \mathcal{S}_{a_i})$, wobei die Kranzprodukte mit der natürlichen Operation von $\mathcal{S}_{a_i}$ gebildet seien.

(10.46) Aufgabe: Primitive Gruppen.
Man bestimme alle primitiven Gruppen $G \leq \mathcal{S}_X$ für $|X| \leq 5$.

(10.47) Aufgabe: Scharf 2-fach transitive Operationen.
Es seien $p \in \mathbb{N}$ eine Primzahl und $G := C_{p-1} \ltimes C_p$, wobei $C_{p-1} \cong \mathrm{Aut}(C_p)$ in natürlicher Weise auf C_p operiere. Man zeige: Bis auf Isomorphie gibt es genau eine scharf 2-fach transitive G-Menge.

(10.48) Aufgabe: Projektive lineare Gruppen.
Es seien $\mathbb{F}_q$ der Körper mit q Elementen, sowie $G := \mathrm{GL}_2(\mathbb{F}_q)$ und $H := \mathrm{SL}_2(\mathbb{F}_q)$.
a) Man bestimme $Z(G)$, und zeige $Z(G) \cong C_{q-1}$. Man bestimme $Z(H)$, und zeige $Z(H) = \{1\}$ falls q gerade, und $Z(H) \cong C_2$ falls q ungerade ist. Man bestimme die Ordnung der **projektiven linearen Gruppe** $\mathrm{PGL}_2(\mathbb{F}_q) := G/Z(G)$ und der **projektiven speziellen linearen Gruppe** $\mathrm{PSL}_2(\mathbb{F}_q) := H/Z(H)$. Wie kann $\mathrm{PSL}_2(\mathbb{F}_q)$ als Untergruppe von $\mathrm{PGL}_2(\mathbb{F}_q)$ aufgefaßt werden?
b) Es sei $\mathbb{P}(\mathbb{F}_q^2) := \{\langle v \rangle \leq \mathbb{F}_q^2; v \neq 0\}$ die **projektive Gerade** über $\mathbb{F}_q$. Man zeige: $\mathrm{PGL}_2(\mathbb{F}_q)$ operiert scharf 3-fach transitiv auf $\mathbb{P}(\mathbb{F}_q^2)$. Operiert $\mathrm{PSL}_2(\mathbb{F}_q)$ ebenfalls 3-fach transitiv auf $\mathbb{P}(\mathbb{F}_q^2)$?

(10.49) Aufgabe: Mathieu-Gruppe M_{11}.
Es seien G eine Gruppe, die auf der Menge X mit $|X| = 11$ treu und scharf 4-fach transitiv operiere, und $\{1\} \neq N \trianglelefteq G$ sowie $P \in \mathrm{Syl}_{11}(N)$. Man zeige:
a) Es gilt $[G\colon N] \mid 8$.
b) Es gilt $C_G(P) = P$ und $|N_G(P)| \mid 11 \cdot 10$, sowie $G = N \cdot N_G(P)$.
c) Ist $N \neq G$, so gibt es eine Involution $t \in N_G(P)$, und es gilt $|\mathrm{Fix}_X(t)| = 1$; daraus folgere man, daß es $U < G$ mit $[G\colon U] = 2$ gibt.
d) G ist eine einfache Gruppe.

(10.50) Aufgabe: Reguläre Normalteiler.
Es seien G eine endliche Gruppe, $\{1\} \neq N \trianglelefteq G$, und X eine primitive treue G-Menge, auf der N regulär operiere. Man zeige: Es ist N ein minimaler Normalteiler.

(10.51) Aufgabe: Affine lineare Gruppe.
Es seien $\mathbb{F}_q$ der Körper mit q Elementen, $V := \mathbb{F}_q^n$ für ein $n \in \mathbb{N}$ und $G := \mathrm{AGL}_n(\mathbb{F}_q) := \{V \to V\colon v \mapsto vg + t; g \in \mathrm{GL}_n(\mathbb{F}_q), t \in V\}$ die Gruppe der **affinen linearen Abbildungen** auf V. Man zeige:
a) Es ist $G \cong \mathrm{GL}_n(\mathbb{F}_q) \ltimes V$, wobei das semidirekte Produkt mit der natürlichen Operation von $\mathrm{GL}_n(\mathbb{F}_q)$ auf V gebildet sei. Die Untergruppe $V \lhd G$ wird als **Translationsnormalteiler** bezeichnet.
b) Die Gruppe G operiert 2-fach transitiv auf V, und $V \lhd G$ operiert regulär. Wann operiert G sogar 3-fach transitiv auf V?

(10.52) Aufgabe: Satz von Galois.
Es seien G eine endliche Gruppe, $\{1\} \neq N \trianglelefteq G$ ein abelscher minimaler Normalteiler, X eine primitive treue G-Menge und $x \in X$. Man zeige:
a) N operiert regulär auf X und ist p-elementar-abelsch, für eine Primzahl $p \in \mathbb{N}$, und es gilt $G \cong \mathrm{Stab}_G(x) \ltimes N$. Außerdem ist $C_G(N) = N$, und N ist der einzige minimale Normalteiler von G.
b) G kann als Untergruppe der affinen linearen Gruppe $\mathrm{AGL}_n(\mathbb{F}_p)$ aufgefaßt werden, für ein $n \in \mathbb{N}$. Man beschreibe $\mathrm{Stab}_G(x)$ und N als Untergruppen von $\mathrm{AGL}_n(\mathbb{F}_p)$. Was hat die G-Operation auf X mit der natürlichen Operation von $\mathrm{AGL}_n(\mathbb{F}_p)$ auf $\mathbb{F}_p^n$ zu tun?

(10.53) Aufgabe: Untergruppen von $\mathcal{S}_n$.
Es seien $n \geq 5$ und $U \leq \mathcal{S}_n$ mit $[\mathcal{S}_n\colon U] < n$. Man zeige: Es gilt $U \geq \mathcal{A}_n$.

(10.54) Aufgabe: Kommutatoren.
Es seien G eine Gruppe und $x, y, z \in G$. Man zeige:
a) Es gilt $[x, y]^{-1} = [y, x]$.
b) Es gilt $[x, yz] = [x, z] \cdot [x, y]^z = [x, z] \cdot [x, y] \cdot [x, y, z]$.
c) Es gilt $[xy, z] = [x, z]^y \cdot [y, z] = [x, z] \cdot [x, z, y] \cdot [y, z]$.
d) Es gilt die **Witt-Identität** $[x, y^{-1}, z]^y \cdot [y, z^{-1}, x]^z \cdot [z, x^{-1}, y]^x = 1$.

(10.55) Aufgabe: Auflösbare Gruppen kleiner Ordnung.
Es sei G eine endliche Gruppe. Man zeige:
a) Man zeige: Ist G nicht auflösbar mit $|G| \leq 200$, so $|G| \in \{60, 120, 168, 180\}$.
b) Ist G nicht auflösbar mit $|G| = 60$, so ist $G \cong \mathcal{A}_5$.
c) Ist $|G| \in \{120, 180\}$, so besitzt G einen Normalteiler $\{1\} \neq N \lhd G$.

(10.56) Aufgabe: Auflösbare Gruppen.
Es sei G eine endliche Gruppe. Man zeige:
a) Sind $M, N \trianglelefteq G$ mit G/M und G/N auflösbar, so ist auch $G/(M \cap N)$ auflösbar.
b) G besitzt einen eindeutig bestimmten maximalen auflösbaren Normalteiler.
c) Sind G auflösbar und $\{1\} \neq N \trianglelefteq G$ ein minimaler Normalteiler, so ist N elementar-abelsch.

(10.57) Aufgabe: Nilpotente Gruppen.
Es seien G eine Gruppe und $M, N \trianglelefteq G$. Man zeige:
a) Man zeige: Sind G/M und G/N nilpotent, so ist auch $G/(M \cap N)$ nilpotent. Sind G/N und N nilpotent, ist dann notwendig auch G nilpotent?
b) Sind M und N nilpotent der Klassen c_M bzw. c_N, so ist $M \times N$ nilpotent der Klasse $\max\{c_M, c_N\}$, und $MN \trianglelefteq G$ ist nilpotent der Klasse höchstens $c_M + c_N$.

(10.58) Aufgabe: Nilpotente endliche Gruppen.
Es sei G eine endliche Gruppe.

a) Man zeige die Äquivalenz der folgenden Aussagen:
i) G ist nilpotent.
ii) Für jeden Normalteiler $N \lhd G$ ist $Z(G/N) \neq \{1\}$.
iii) Für jeden Normalteiler $\{1\} \neq N \trianglelefteq G$ ist $[N, G] < N$.
iv) Sind $g, h \in G$ mit $\mathrm{ggT}(|g|, |h|) = 1$, so ist $gh = hg$.
v) Für alle $g, h \in G$ ist $\langle g, h \rangle \leq G$ nilpotent.

b) Man zeige: Es ist $Z_\infty(G) = \bigcap\{N \trianglelefteq G; Z(G/N) = \{1\}\}$ und $K_\infty(G) = \langle N \trianglelefteq G; [N, G] = N \rangle$. Ist $N \trianglelefteq G$, so ist G/N genau dann nilpotent, wenn $K_\infty(G) \leq N$ gilt.

(10.59) Aufgabe: Normalteiler nilpotenter Gruppen.
Es seien G eine nilpotente endliche Gruppe und $\{1\} \neq N \trianglelefteq G$. Man zeige:
a) Es ist $Z(G) \cap N \neq \{1\}$.
b) Ist N ein maximaler abelscher Normalteiler, so gilt $C_G(N) = N$.

(10.60) Aufgabe: Symmetrische Gruppen.
Es sei $n \in \mathbb{N}$. Man bestimme die Normalteiler, die Kommutatorreihe, die obere und untere Zentralreihe, die Hauptfaktoren und die Kompositionsfaktoren der symmetrischen Gruppe $\mathcal{S}_n$. Wann ist $\mathcal{S}_n$ auflösbar? Wann ist $\mathcal{S}_n$ überauflösbar? Wann ist $\mathcal{S}_n$ nilpotent?

(10.61) Aufgabe: Diedergruppen.
Es sei $n \geq 3$. Man bestimme die Kommutatorreihe, die obere und untere Zentralreihe, und die Kompositionsfaktoren der Diedergruppe D_{2n}. Wann ist D_{2n} auflösbar? Wann ist D_{2n} überauflösbar? Wann ist D_{2n} nilpotent?

(10.62) Aufgabe: Frattini-Gruppe.
Es seien G eine endliche Gruppe und $N \trianglelefteq G$. Man zeige:
a) Ist $M \trianglelefteq G$ mit $G = M \times N$, so ist $\Phi(G) = \Phi(M) \times \Phi(N)$.
b) Es gibt genau dann $U < G$ mit $UN = G$, wenn $N \not\leq \Phi(G)$ ist.
c) Ist N abelsch mit $N \cap \Phi(G) = \{1\}$, so besitzt N in G ein Komplement.

(10.63) Aufgabe: Überflüssige Erzeuger.
Es sei G eine endliche Gruppe.

a) Besitzt G ein Erzeugendensystem der Kardinalität $n \in \mathbb{N}$, so zeige man für $g \in G$ die Äquivalenz der folgenden Aussagen:
i) Es ist $g \in \Phi(G)$. **ii)** Ist $\langle g_1, \ldots, g_n \rangle = G$, so ist stets auch $\langle gg_1, \ldots, g_n \rangle = G$.

b) Ist $n \in \mathbb{N}$ die minimale Kardinalität eines Erzeugendensystems von G, so zeige man für $g \in G$ die Äquivalenz der folgenden Aussagen:
i) Es ist $g \in \Phi(G)$. **ii)** Aus $\langle g, g_1, \ldots, g_n \rangle = G$ folgt stets auch $\langle g_1, \ldots, g_n \rangle = G$.

(10.64) Aufgabe: Nilpotente zyklische Gruppen.
Es sei G eine nilpotente endliche Gruppe. Man zeige die Äquivalenz der folgenden Aussagen:
i) G ist zyklisch. **ii)** $G/[G,G]$ ist zyklisch.
iii) Jede Sylow-Gruppe von G ist zyklisch.

(10.65) Aufgabe: Maximale Untergruppen.
Es sei G eine endliche Gruppe, die genau eine maximale Untergruppe besitze. Man zeige: G ist zyklisch von Primzahlpotenzordnung.

(10.66) Aufgabe: Nilpotenzklasse.
Es seien G eine p-Gruppe mit $|G| = p^n$, für ein $n \in \mathbb{N}_0$, und Nilpotenzklasse $c \in \mathbb{N}_0$. Man zeige: Es gilt $c \leq n$ und es ist genau dann $c = n$, wenn $n \leq 1$ gilt.

(10.67) Aufgabe: Satz von Gaschütz.
Es seien G eine endliche Gruppe, und $N \trianglelefteq G$ mit $N \leq \Phi(G)$. Man zeige: Es gilt $\mathrm{Inn}(N) \leq \Phi(\mathrm{Aut}(N))$.

(10.68) Aufgabe: Gruppen der Ordnung 8.
Es sei G eine Gruppe der Ordnung 8. Man bestimme $Z(G)$, die Kommutatorgruppe $[G,G]$, die Frattini-Gruppe $\Phi(G)$ und die Fitting-Gruppe $F(G)$.

(10.69) Aufgabe: Perfekte Gruppen.
Es seien G eine endliche Gruppe, und $N \trianglelefteq G$ abelsch mit G/N perfekt. Man zeige: $[G, G]$ ist perfekt.

(10.70) Aufgabe: Direkte Produkte.
Es seien $G_1, \ldots, G_n$ nicht-abelsche einfache Gruppen, für ein $n \in \mathbb{N}$. Man bestimme alle Normalteiler des direkten Produkts $G_1 \times \cdots \times G_n$. Gilt eine analoge Aussage auch für abelsche einfache Gruppen?

(10.71) Aufgabe: Komponenten.
Es seien G eine endliche Gruppe und $K \leq G$. Man zeige: Genau dann ist K eine Komponente von G, wenn K Komponente von $\langle K, K^g \rangle$ für alle $g \in G$ ist.

(10.72) Aufgabe: Verallgemeinerte Fitting-Gruppe.
Für eine endliche Gruppe G bestimme man $K_\infty(F^*(G))$, sowie $F^*(C_G(E(G)))$ und $F^*(C_G(F(G)))$.

(10.73) Aufgabe: Spezielle lineare Gruppe $\mathbf{SL}_2(\mathbb{F}_5)$.
Es sei $G := \mathrm{SL}_2(\mathbb{F}_5)$.
a) Man bestimme das Zentrum $Z(G)$ und die Kommutatorgruppe $[G, G]$, und zeige $\mathrm{PSL}_2(\mathbb{F}_5) := G/Z(G) \cong \mathcal{A}_5$, und daß $Z(G)$ in G kein Komplement besitzt.
b) Man bestimme die Frattini-Gruppe $\Phi(G)$, die Fitting-Gruppe $F(G)$, die Komponentengruppe $E(G)$ und die verallgemeinerte Fitting-Gruppe $F^*(G)$.

11 References

[1] J. Alperin, R. Bell: Groups and Representations, Springer, 1995.

[2] M. Aschbacher: Finite Group Theory, 2nd ed., Cambridge University Press, 2000.

[3] W. Burnside: Theory of Groups of Finite Order, Cambridge University Press, 1911, Reprint: Dover, 1955.

[4] G. Butler: Fundamental Algorithms for Permutation Groups, Lecture Notes in Computer Science 559, Springer, 1991.

[5] R. Carter: Simple Groups of Lie type, Wiley, London, 1989.

[6] P. Cameron: Permutation groups, Cambridge University Press, 1999.

[7] H. Coxeter, W. Moser: Generators and Relations for Discrete Groups, 4th ed., Springer, 1980.

[8] L. Dickson: Linear Groups, Dover, 1958.

[9] J. Dixon: Problems in Group Theory, Blaisdell Publishing Co., 1967.

[10] K. Doerk, T. Hawkes: Finite Soluble Groups, deGruyter, 1992.

[11] D. Gorenstein: Finite Groups, 2nd ed., Chelsea Publishing Co., 1980.

[12] D. Gorenstein: Finite Simple Groups, Plenum Publishing Corp., 1982.

[13] M. Hall: The Theory of Groups, Macmillan Co., 1959, Reprint: Chelsea Publishing Co., 1976.

[14] B. Huppert: Endliche Gruppen I, Springer, 1967.

[15] B. Huppert, N. Blackburn: Finite Groups II, Springer, 1982.

[16] B. Huppert, N. Blackburn: Finite Groups III, Springer, 1982.

[17] D. Johnson: Presentations of Groups, 2nd ed., Cambridge University Press, 1997.

[18] M. Kargapolov: Fundamentals of the Theory of Groups, Springer, 1979.

[19] R. Kochendörffer: Lehrbuch der Gruppentheorie unter besonderer Berücksichtigung der endlichen Gruppen, Akad. Verlagsgesell. Geest und Portig, 1966.

[20] R. Kochendörffer: Group Theory, McGraw-Hill, 1970.

[21] A. Kurosh: The Theory of Groups I, II, Chelsea Publishing Co., 1960.

[22] H. Kurzweil, B. Stellmacher: Endliche Gruppen, Springer, 1998.

[23] I. MacDonald: The Theory of Groups, Clarendon Press, 1968, Reprint: Krieger, 1988.

[24] D. Robinson: A Course in the Theory of Groups, Springer, 1996.

[25] T. Rose: A Course on Group Theory, Cambridge University Press, 1978, Reprint: Dover, 1994.

[26] J. Rotman: An Introduction to the Theory of Groups, Springer, 1995.

[27] W. Scott: Group Theory, 2nd. ed., Dover 1987.

[28] A. Seress: Permutation Group Algorithms, Cambridge Tracts in Mathematics 152, Cambridge University Press, 2003.

[29] C. Sims: Computation with Finitely Presented Groups, Cambridge University Press, 1994.

[30] R. Schmidt: Subgroup Lattices of Groups, deGruyter, 1994.

[31] M. Suzuki: Group Theory I, Springer, 1982.

[32] M. Suzuki: Group Theory II, Springer, 1986.

[33] M. Weinstein: Examples of Groups, Polygonal Publishing House, 1977.

[34] F. Wielandt: Finite Permutation Groups, Academic Press, 1964.

[35] H. Zassenhaus: The Theory of Groups, 2nd ed., Chelsea Publishing Co., 1958, Reprint: Dover, 1999.