

Finite Group Theory (WS 2026)

PD Dr. Jürgen Müller, **Lecture 0** (12.10.2026)

Prerequisites

(0.1) Groups. a) A set G together with a **multiplication** $\cdot : G \times G \rightarrow G$ fulfilling the following conditions is called a **group**: **i)** We have **associativity** $(fg)h = f(gh)$ for $f, g, h \in G$; **ii)** there is a **right neutral element** $1 \in G$ such that $g \cdot 1 = g$ for $g \in G$; and **iii)** for any $g \in G$ there is a **right inverse** $g^{-1} \in G$ such that $g \cdot g^{-1} = 1$. If additionally $gh = hg$ holds for $g, h \in G$, then G is called **commutative** or **abelian**.

The product $g_1 g_2 \cdots g_n \in G$ is well-defined independently from the bracketing for $g_1, \dots, g_n \in G$, and if G is abelian then the product $g_1 g_2 \cdots g_n \in G$ is independent from the order of its factors. For $g \in G$ let $g^0 := 1$, and recursively $g^{n+1} := g^n g$, and $g^{-n} := (g^{-1})^n$; then by the statements to be shown below we have $g^m g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$ and $g^{-n} = (g^n)^{-1}$, for $m, n \in \mathbb{Z}$. If $g, h \in G$ **commute**, that is we have $gh = hg$, then we have $(gh)^n = g^n h^n = h^n g^n$ for $n \in \mathbb{Z}$. If G is finite, then its cardinality is called the **order** of G .

b) We collect a few immediate consequences: In particular, we have $G \neq \emptyset$.

We show that the right neutral element is left neutral as well, and that right inverses are left inverses as well: To do so, we first observe that $gg = g$ if and only if $g = 1$: From $gg = g$ we get $g = g \cdot 1 = g(gg^{-1}) = (gg)g^{-1} = gg^{-1} = 1$, and for $g = 1$ we have $1 \cdot 1 = 1$; in particular $1^{-1} = 1$. Now, from $(g^{-1}g)(g^{-1}g) = g^{-1}(gg^{-1})g = (g^{-1} \cdot 1)g = g^{-1}g$ we infer $g^{-1}g = 1$, and we get $g = g \cdot 1 = g(g^{-1}g) = (gg^{-1})g = 1 \cdot g$.

From this we infer that the **neutral** element is uniquely defined: If $1' \in G$ also is a neutral element, then we have $1 = 1 \cdot 1' = 1'$. Moreover, **inverses** are uniquely defined: If $g' \in G$ also is an inverse of $g \in G$, then we have $g' = 1 \cdot g' = (g^{-1}g)g' = g^{-1}(gg') = g^{-1} \cdot 1 = g^{-1}$.

We show the **cancellation law**: For $f, g, h \in G$ we have $f = g$ if and only if $fh = gh$, which holds if and only if $hf = hg$: From $fh = gh$ we deduce $f = f \cdot 1 = f(hh^{-1}) = (fh)h^{-1} = (gh)h^{-1} = g(hh^{-1}) = g \cdot 1 = g$, and from $hf = hg$ we deduce $f = 1 \cdot f = (h^{-1}h)f = h^{-1}(hf) = h^{-1}(hg) = (h^{-1}h)g = 1 \cdot g = g$.

(0.2) Example: Symmetric and alternating groups. a) Let Ω be a set. Then the set $\mathcal{S}_\Omega$ of all permutations of Ω , that is the bijections $\pi : \Omega \rightarrow \Omega$, together with concatenation of maps, becomes a group, being called the **symmetric group** on Ω ; the neutral element is the identity map, and φ^{-1} is given as the inverse map associated with π .

If $\Omega = \{1, \dots, n\}$ for some $n \geq 0$, we write $\mathcal{S}_n := \mathcal{S}_{\{1, \dots, n\}}$. We have $|\mathcal{S}_n| = n!$: For $n = 0$ we have $\mathcal{S}_0 = \{1\}$; for $n \geq 1$ and $\pi \in \mathcal{S}_n$ we have $n\pi = m$ for some

$m \in \{1, \dots, n\}$, hence $\pi: \{1, \dots, n-1\} \rightarrow \{1, \dots, n\} \setminus \{m\}$ is bijective as well, and since there are n choices of m , there are $n \cdot |\mathcal{S}_{n-1}| = n!$ choices of π .

Any permutation can be written uniquely, up to reordering the factors, as a product of **disjoint cycles**, giving rise to **cycle notation**, where often 1-cycles are left out. The lengths of the cycles appearing are collected in a partition of n , called the associated **cycle type**. For example, we have $\mathcal{S}_1 = \{()\}$, $\mathcal{S}_2 = \{(), (1, 2)\}$ 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, from $(1, 2, 3) \cdot (1, 2) = (2, 3) \neq (1, 3) = (1, 2) \cdot (1, 2, 3)$ we deduce that $\mathcal{S}_n$ is not abelian for $n \geq 3$. Note that maps are applied from the right, so that concatenation is to the right as well.

b) For $n \geq 0$, the **sign** map $\text{sgn}: \mathcal{S}_n \rightarrow \{\pm 1\}$ is defined as

$$\text{sgn}(\pi) := \prod_{1 \leq i < j \leq n} \frac{j\pi - i\pi}{j - i} = (-1)^{l(\pi)},$$

where $l(\pi) := |\{\{i, j\} \subseteq \{1, \dots, n\}; i < j, i\pi > j\pi\}|$ is the **inversion number** of $\pi \in \mathcal{S}_n$. Then we have **multiplicativity** $\text{sgn}(\pi\rho) = \text{sgn}(\pi) \cdot \text{sgn}(\rho)$ and $\text{sgn}(\pi) = \text{sgn}(\pi^{-1})$, for $\pi, \rho \in \mathcal{S}_n$. Moreover, writing $\pi \in \mathcal{S}_n$ as a product of r disjoint cycles, we get $\text{sgn}(\pi) = (-1)^{n-r}$: By multiplicativity, it suffices to observe that for the k -cycle we have $l((1, \dots, k)) = k - 1$, for $k \geq 1$.

Let $\mathcal{A}_n := \{\pi \in \mathcal{S}_n; \text{sgn}(\pi) = 1\}$ and $\mathcal{S}_n \setminus \mathcal{A}_n = \{\pi \in \mathcal{S}_n; \text{sgn}(\pi) = -1\}$ be the sets of **even** and **odd** permutations, respectively. By the properties collected above $\mathcal{A}_n$ together with concatenation of maps becomes a group as well, being called the **alternating group** on n letters. We have $\mathcal{A}_0 = \mathcal{S}_0 = \{1\}$ and $\mathcal{A}_1 = \mathcal{S}_1 = \{1\}$, while from $\text{sgn}((1, 2)) = -1$ we infer that $\mathcal{A}_n \neq \mathcal{S}_n$ for $n \geq 2$.

(0.3) Example: General and special linear groups. **a)** Let K be a field. For $n \geq 0$, the set of invertible matrices $\text{GL}_n(K) := \{A \in K^{n \times n}; \det(A) \neq 0\}$, together with matrix multiplication, becomes a group, being called the **general linear group** of degree n over K ; the neutral element is the identity matrix, and A^{-1} is given as the inverse matrix associated with A .

For $n = 0$ we have $\text{GL}_0(K) = \{\emptyset\}$; for $n = 1$ we have $\text{GL}_1(K) = K^* = K \setminus \{0\}$, the multiplicative group of K . While the latter groups are abelian, from

$$\begin{bmatrix} 1 & . \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ . & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \neq \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ . & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & . \\ 1 & 1 \end{bmatrix}$$

we deduce that $\text{GL}_n(K)$ is not abelian for $n \geq 2$. Note again that maps are applied from the right, so that concatenation is to the right as well.

b) For $n \geq 0$, the set of unimodular matrices $\text{SL}_n(K) := \{A \in K^{n \times n}; \det(A) = 1\}$, together with matrix multiplication, becomes a group, being called the **special linear group** of size n over K ; again, the neutral element is the identity matrix, and A^{-1} is given as the inverse matrix associated with A .

For $n = 0$ we have $\text{SL}_0(K) = \{\emptyset\}$; for $n = 1$ we have $\text{SL}_1(K) = \{1\}$. While the latter groups are abelian, from the above computation we deduce that $\text{SL}_n(K)$ is not abelian for $n \geq 2$.

(0.4) Subgroups. a) Let G be a group. A subset $\emptyset \neq H \subseteq G$ is called a **subgroup** of G , if whenever $g, h \in H$ then we have $gh^{-1} \in H$ as well.

Then, assuming that $g, h \in H$, we first get $1 = gg^{-1} \in H$, and from this $g^{-1} = 1 \cdot g^{-1} \in H$, and $gh = g(h^{-1})^{-1} \in H$. Thus H is closed with respect to taking products and inverses, hence again is a group in its own right; we write $H \leq G$. If $H \neq G$ then $H < G$ is called a **proper** subgroup; a proper subgroup $H < G$ is called **maximal**, if $H < U \leq G$ implies $U = G$.

For example, the **trivial group** $\{1\}$ and G always are subgroups of G . Moreover, we have $\mathcal{A}_n \leq \mathcal{S}_n$ and $\text{SL}_n(K) \leq \text{GL}_n(K)$, for $n \geq 0$ and K a field.

b) Let $\{U_i \leq G; i \in \mathcal{I}\}$ where $\mathcal{I}$ is an index set. Then the set-theoretic intersection $\bigcap_{i \in \mathcal{I}} U_i \leq G$ is a subgroup; for $\mathcal{I} = \emptyset$ the empty intersection is defined to be G . But $\bigcup_{i \in \mathcal{I}} U_i \subseteq G$ in general is not a subgroup, hence the set-theoretic union has to be replaced suitably:

Let $\mathcal{S} \subseteq G$ be a subset. Then $\langle \mathcal{S} \rangle := \bigcap \{U \leq G; \mathcal{S} \subseteq U\} \leq G$ is the smallest subgroup of G containing $\mathcal{S}$. It is called the subgroup **generated** by the **generating set** $\mathcal{S}$; if $\mathcal{S}$ is finite then $\langle \mathcal{S} \rangle$ is called **finitely generated**. Letting $\mathcal{S}^{-1} := \{g^{-1} \in G; g \in \mathcal{S}\}$, it is immediate that $\langle \mathcal{S} \rangle$ consists of all finite products of elements of $\mathcal{S} \cup \mathcal{S}^{-1}$. For example, we have $\langle \emptyset \rangle = \langle 1 \rangle = \{1\}$ and $\langle G \rangle = G$.

Example. An element $(i, j) \in \mathcal{S}_n$, for $i \neq j$, is called a **transposition**; if $|i - j| = 1$ then it is called an **adjacent transposition**. Then for $k \geq 1$ we have $(1, \dots, k) = (1, 2)(1, 3) \cdots (1, k-1)(1, k)$, where the empty product is defined to be the identity map. Since any permutation is a product of cycles, we infer that $\mathcal{S}_n$ is generated by its transpositions. Moreover, from

$$(1, k) = (k-1, k)(k-2, k-1) \cdots (2, 3)(1, 2)(2, 3) \cdots (k-2, k-1)(k-1, k)$$

we infer that $\mathcal{S}_n$ is actually generated by its adjacent transpositions.

(0.5) Cyclic groups. a) A group C is called **cyclic**, if it has a singleton generating set. If $C = \langle g \rangle$, then we have $C = \{g^k \in G; k \in \mathbb{Z}\}$; hence C is abelian. If C is finite then its cardinality $|g|$ is also called the **order** of g .

Let $I_g := \{k \in \mathbb{Z}; g^k = 1\}$, which is an ideal of $\mathbb{Z}$. Then C is finite if and only if $I_g \neq \{0\}$; in this case we have $I_g = |g|\mathbb{Z} \trianglelefteq \mathbb{Z}$ and $C = \{1, g, g^2, \dots, g^{|g|-1}\}$:

If C is finite, then there are $i \neq j$ such that $g^i = g^j$, hence $0 \neq i - j \in I_g$. If conversely $I_g = n\mathbb{Z}$, where $n > 0$, then quotient and remainder with respect to n shows that $C = \{1, g, g^2, \dots, g^{n-1}\}$ 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 $\{1, g, g^2, \dots, g^{n-1}\}$ are pairwise distinct, so that $n = |g|$. $\sharp$

b) Any subgroup of C is cyclic; and if C is finite, then there is a subgroup of C of order d if and only if $d \mid |g|$; in this case the latter is uniquely determined:

Let $\{1\} \neq U \leq C$, then $I_U := \{k \in \mathbb{Z}; g^k \in U\}$ is a non-zero ideal of $\mathbb{Z}$, hence there is $m > 0$ such that $I_U = m\mathbb{Z} \trianglelefteq \mathbb{Z}$, thus $U = \langle g^m \rangle$.

Now let C be finite of order n , 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 .

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

(0.6) Cosets. a) Let G be a group, and let $H \leq G$. Then, given $g \in G$, let the associated **(right) coset** of H in G be defined as the subset $Hg := \{hg \in G; h \in H\} \subseteq G$. Hence, by the cancellation law, we conclude that the surjective map $H \rightarrow Hg: h \mapsto hg$ is injective as well, that is bijective; in particular if H is finite this says that $|Hg| = |H|$.

Let $H \backslash G := \{Hg \subseteq G; g \in G\}$ be the set of cosets of H in G . Then two distinct cosets are disjoint: Let $g, g' \in G$ such that $x \in Hg \cap Hg'$, then we have $x = yg = y'g'$ for some $y, y' \in H$, implying that $hg = hy^{-1}y'g' \in Hg'$ for all $h \in H$, that is $gH \subseteq g'H$, and by symmetry $gH = g'H$. Thus, since $g \in gH$ for any $g \in G$, we infer that the cosets of H in G disjointly cover all of G .

A subset $\mathcal{T} \subseteq G$ such that $\mathcal{T} \rightarrow H \backslash G: t \mapsto Ht$ is a bijection, is called a **transversal** of H in G ; note that giving a transversal $\mathcal{T}$ amounts to pick a **representative** out of each coset, hence transversals exist by the Axiom of Choice. Thus we have $G = \coprod_{t \in \mathcal{T}} Ht$, and if $\mathcal{T}$ is finite the cardinality $[G: H] := |H \backslash G| = |\mathcal{T}|$ is called the **index** of H in G .

b) Similarly, given $g \in G$, the set $gH := \{gh \in G; h \in H\} \subseteq G$ is called the associated **left coset**, where again $H \rightarrow gH: h \mapsto gh$ is bijective. Let G/H be the set of left cosets of H in G , and a set of representatives of the latter is called a **left transversal** of H in G .

If $\mathcal{T} \subseteq G$ is a right transversal of H in G , then from $G = \coprod_{t \in \mathcal{T}} Ht$ by inversion we get $G = \coprod_{t \in \mathcal{T}} t^{-1}H$, hence $\mathcal{T}^{-1} \subseteq G$ is a left transversal of H in G . Thus the index $[G: H]$ is independent of whether right or left cosets are considered. But in general left and right cosets do not coincide, and left transversals are not right transversals, leading to the following notion:

c) A subgroup $H \leq G$ is called **normal** if $gH \subseteq Hg$ for all $g \in G$; we write $H \trianglelefteq G$. In this case, inversion yields $Hg^{-1} \subseteq g^{-1}H$, this holding for all $g \in G$ we get $gH = Hg$, saying that left and right cosets coincide. Equivalently, we have $H^g := g^{-1}Hg = H$, for all $g \in G$, that is H equals all its **G -conjugates**. A non-trivial normal subgroup $H \trianglelefteq G$ is called **minimal**, if $U \trianglelefteq G$ such that $U < H$ implies $U = \{1\}$.

Any subgroup of an abelian group is normal. Moreover, any subgroup of index 2 is normal: We have $G = H \cup Hg = H \cup gH$, for any $g \in G \setminus H$. Finally, we always have $\{1\} \trianglelefteq G$ and $G \trianglelefteq G$; a non-trivial group G having only these two normal subgroups is called **simple**.

Example. For $n \geq 2$, using the multiplicativity of the sign map, for any $\pi \in \mathcal{S}_n$ we have either $\text{sgn}(\pi) = 1$ or $\text{sgn}(\pi \cdot (1, 2)) = 1$, thus $\{(), (1, 2)\}$ is a transversal of $\mathcal{A}_n$ in $\mathcal{S}_n$, hence $|\mathcal{A}_n| = \frac{1}{2} \cdot |\mathcal{S}_n| = \frac{n!}{2}$ and $\mathcal{A}_n \trianglelefteq \mathcal{S}_n$.

(0.7) Subgroup orders. a) We derive a few immediate consequences: Let G be a finite group, let $H \leq G$, and let $\mathcal{T}$ be a transversal of H in G . Then we have $|G| = \sum_{t \in \mathcal{T}} |Hg| = \sum_{t \in \mathcal{T}} |H| = |\mathcal{T}| \cdot |H|$, implying **Lagrange's Theorem** saying that $[G : H] = \frac{|G|}{|H|}$. Hence we have $|H| \mid |G|$, so that in order to search for subgroups of G we need only consider subsets of cardinality dividing $|G|$.

Thus for any $g \in G$ we have $|g| \mid |G|$, implying **Euler's Theorem** saying that $g^{|G|} = 1$. Hence, letting $\exp(G) := \text{lcm}\{|g|; g \in G\}$ be the **exponent** of G , we also have $\exp(G) \mid |G|$. In particular, if $|G|$ is a prime, then G is cyclic.

b) This yields a characterisation of cyclic groups: A finite group G is cyclic if and only if G has at most one subgroup of order d , for all $d \geq 1$:

For $n \geq 1$ let $(\mathbb{Z}/n\mathbb{Z})^* := \{k \in \mathbb{Z}/n\mathbb{Z}; \gcd(k, n) = 1\}$, and let $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^*|$ be **Euler's totient function**. Hence a cyclic group of order n has precisely $\varphi(n)$ elements of order n , thus its subgroup structure implies $\sum_{d \in \mathbb{N}, d \mid n} \varphi(d) = n$. (This is well-known from elementary number theory.)

Now let G have the required property. Then G has an element of order d only if $d \mid n := |G|$, and in this case there are at most $\varphi(d)$ of them. Thus by $\sum_{d \in \mathbb{N}, n \neq d \mid n} \varphi(d) < n$ there is an element of order n . $\#$

Example. We determine the subgroups of $\mathcal{S}_3$: 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 $\langle(1, 2)\rangle$, $\langle(1, 3)\rangle$ and $\langle(2, 3)\rangle$ of order 2, and the cyclic subgroup $\mathcal{A}_3 = \langle(1, 2, 3)\rangle = \langle(1, 3, 2)\rangle$ of order 3. Thus the **lattice of subgroups** of $\mathcal{S}_3$ is as depicted in the **Hasse diagram** in Table 1, where the normal subgroups $\{1\}$, $\mathcal{A}_3$ and $\mathcal{S}_3$ are depicted as black vertices.

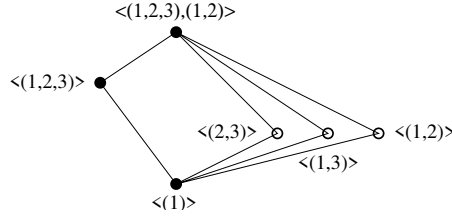
Indeed, $H := \langle(1, 2)\rangle \leq \mathcal{S}_3$, having order 2 and thus index 3, is not normal: We have $\mathcal{S}_3 = \{(), (1, 2)\} \dot{\cup} \{(1, 2, 3), (1, 3)\} \dot{\cup} \{(1, 3, 2), (2, 3)\}$ as right cosets, and $\mathcal{S}_3 = \{(), (1, 2)\} \dot{\cup} \{(1, 2, 3), (2, 3)\} \dot{\cup} \{(1, 3, 2), (1, 3)\}$ as left cosets; the $\mathcal{S}_3$ -conjugates of H are $H = \langle(1, 2)\rangle$, $H^{(1, 2, 3)} = \langle(2, 3)\rangle$ and $H^{(1, 3, 2)} = \langle(1, 3)\rangle$.

(0.8) Homomorphisms. a) Let G and H be groups. Then $\varphi: G \rightarrow H$ is called a **(group) homomorphism**, if $\varphi(gg') = \varphi(g)\varphi(g')$ for all $g, g' \in G$.

Then $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$ yields $\varphi(1) = 1$, and for $g \in G$ we have $1 = \varphi(1) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$, hence $\varphi(g^{-1}) = \varphi(g)^{-1}$.

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 φ^{-1} is an isomorphism as well, and we write $G \cong H$; if $G = H$, then φ is called an **endomorphism**; and a bijective endomorphism is called an **automorphism**.

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



Let $\text{Aut}(G) \subseteq \mathcal{S}_G$ denote the set of all automorphisms of G . It is immediate that the identity $\text{id}_G: G \rightarrow G: g \mapsto g$ is an automorphism, and that for $\varphi, \psi \in \text{Aut}(G)$ we have $\varphi\psi^{-1} \in \text{Aut}(G)$ as well; hence $\text{Aut}(G)$ is a group again, being called the **automorphism group** of G .

b) For any $U \leq G$ we have $\varphi(U) \leq H$, and for any $V \leq H$ we have $\varphi^{-1}(V) \leq G$.

If $U \leq G$, then from $\varphi(U)^{\varphi(g)} = \varphi(U^g) = \varphi(U)$ for all $g \in G$ we infer that $\varphi(U) \trianglelefteq \varphi(G)$. If $V \leq \varphi(G)$, then from $\varphi(\varphi^{-1}(V)^g) = V^{\varphi(g)} = V$ for all $g \in G$ we infer that $\varphi^{-1}(V) \leq G$. In particular, the **kernel** $\ker(\varphi) := \varphi^{-1}(\{1\}) = \{g \in G; \varphi(g) = 1\} \leq G$ of φ is a normal subgroup of G .

For $g \in G$ and $h := \varphi(g) \in H$, we have $\varphi^{-1}(\{h\}) = g\ker(\varphi) \in G/\ker(\varphi)$; in particular, φ is injective if and only if $\ker(\varphi) = \{1\}$: For $u \in \ker(\varphi)$ we have $\varphi(gu) = \varphi(g)\varphi(u) = h$, thus $g\ker(\varphi) \subseteq \varphi^{-1}(\{h\})$, and conversely for $g' \in \varphi^{-1}(\{h\})$ we have $\varphi(g^{-1}g') = 1$, thus $g' = gg^{-1}g' \in g\ker(\varphi)$.

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

b) Conversely, if $\varphi: G \rightarrow H$ is a homomorphism, then the map $\bar{\varphi}: G/\ker(\varphi) \rightarrow \varphi(G): g\ker(\varphi) \mapsto \varphi(g)$ is an isomorphism such that $\varphi = \nu_{\ker(\varphi)} \cdot \bar{\varphi}$.

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 $m, n \in N$, 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 $gN = 1 \cdot N$, that is $g \in N$.

b) It is immediate that $\bar{\varphi}$ is well-defined and surjective, and that φ factors through $\bar{\varphi}$ as asserted. Moreover, writing $\bar{g} := g\ker(\varphi) \in G/\ker(\varphi)$, we have $\bar{g} \in \ker(\bar{\varphi})$ if and only if $\varphi(g) = 1$, in other words $g \in \ker(\varphi)$, that is $\bar{g} = \bar{1}$. $\sharp$

Example. i) We have the **trivial** homomorphism $\varphi: G \rightarrow \{1\}: g \mapsto 1$, with kernel $\ker(\varphi) = G$ and $G/G \cong \{1\}$. For any automorphism $\alpha \in \text{Aut}(G)$ we have

$\ker(\alpha) = \{1\}$ and $G/\{1\} \cong G$, where the latter isomorphism is given by $\bar{\alpha}$.

ii) For $n \geq 0$, the sign map $\text{sgn}: \mathcal{S}_n \rightarrow \{\pm 1\}$ is a homomorphism, where $\{\pm 1\}$ is considered as a multiplicative group, having kernel $\ker(\text{sgn}) = \mathcal{A}_n \trianglelefteq \mathcal{S}_n$; the sign map is surjective if and only if $n \geq 2$, in which case we have $\mathcal{S}_n/\mathcal{A}_n \cong \{\pm 1\}$.

iii) If K is a field, then $\det: \text{GL}_n(K) \rightarrow K^*$ is an epimorphism, and we have $\ker(\det) = \text{SL}_n(K) \trianglelefteq \text{GL}_n(K)$, so that $\text{GL}_n(K)/\text{SL}_n(K) \cong K^*$.

iv) Let $C = \langle g \rangle$ be a cyclic group. Then $\varphi: \mathbb{Z} \rightarrow C: k \mapsto g^k$ is an epimorphism, where $\mathbb{Z}$ is considered as an additive group, such that $\ker(\varphi) = I_g \trianglelefteq \mathbb{Z}$. If C is infinite, then $\ker(\varphi) = \{0\}$, so that $\mathbb{Z} \cong C$; thus up to isomorphism there is only one infinite cyclic group, multiplicatively written C_∞ . If C is finite, then $\ker(\varphi) = |g|\mathbb{Z}$, so that $\mathbb{Z}/|g|\mathbb{Z} \cong C$; thus for any $n \geq 1$ up to isomorphism there is only cyclic group of order n , multiplicatively written C_n .

(0.9) Actions. a) Let G be a group, and let Ω be a set. Then G is said to **act** on Ω , and the latter is called a **G -set**, if there is an **action map** $\Omega \times G \rightarrow \Omega: [x, g] \mapsto xg$ fulfilling the following conditions: We have i) $x \cdot 1 = x$, and ii) $x(gh) = (xg)h$, for $x \in \Omega$ and $g, h \in G$.

If Ω and Ω' are G -sets, then a map $\alpha: \Omega \rightarrow \Omega'$ such that $\alpha(xg) = \alpha(x)g$, for $x \in \Omega$ and $g \in G$, is called a **(G -set) homomorphism**; if α is bijective, then it is called an **isomorphism**, in which case $\Omega \cong \Omega'$ are called **equivalent**.

The connection to group homomorphisms is given as follows: Given an action of G on Ω , for $g \in G$ let $\alpha_g: \Omega \rightarrow \Omega: x \mapsto xg$; hence from $\alpha_g \alpha_{g^{-1}} = \alpha_{g^{-1}} \alpha_g = \alpha_1 = \text{id}_\Omega$ we infer that $\alpha_g \in \mathcal{S}_\Omega$; since $\alpha_g \alpha_h = \alpha_{gh}$ this yields an **action homomorphism** $\alpha: G \rightarrow \mathcal{S}_\Omega: g \mapsto \alpha_g$. Conversely, if $\alpha: G \rightarrow \mathcal{S}_\Omega: g \mapsto \alpha_g$ is a homomorphism, then from $\alpha_1 = \text{id}_\Omega$ and $\alpha_g \alpha_h = \alpha_{gh}$ we infer that letting $\Omega \times G \rightarrow \Omega: [x, g] \mapsto \alpha_g(x)$ defines an action of G on Ω . If the action homomorphism is injective, the action is called **faithful**.

b) The relation $\mathcal{O} := \{[x, y] \in \Omega \times \Omega; y = xg \text{ for some } g \in G\}$ is an equivalence relation on Ω : From $x \cdot 1 = x$ 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 $x \in \Omega$, its equivalence class $x^G := \{xg \in \Omega; g \in G\}$ again is a G -set, called the **(G -)orbit** of x ; its cardinality $|x^G|$ is called its **length**. A subset $\mathcal{T} \subseteq G$, such that $\mathcal{T} \rightarrow x^G: t \mapsto xt$ is a bijection, is called a **transversal** of x^G with respect to x ; transversals exist by the Axiom of Choice.

Let $\Omega/G := \{x^G \subseteq \Omega; x \in \Omega\}$. A subset $\mathcal{S} \subseteq \Omega$, such that $\mathcal{S} \rightarrow \Omega/G: x \mapsto x^G$ is a bijection, is called a set of **orbit representatives** of Ω ; orbit representatives exist by the Axiom of Choice, and we have $\Omega = \coprod_{x \in \mathcal{S}} x^G$. if $\Omega = x^G$ for any and thus all $x \in \Omega$, then Ω is called a **transitive** G -set; in particular $\Omega \neq \emptyset$.

c) For $x \in \Omega$ let $G_x = \text{Stab}_G(x) := \{g \in G; xg = x\}$ be the **stabilizer** of x in G . Then we have $G_x \leq G$: We have $1 \in G_x$, and for $g, h \in G_x$ from $xg = x = xh$ we get $x(gh^{-1}) = (xg)h^{-1} = xh^{-1} = x$, hence $gh^{-1} \in G_x$. Thus or the associated action homomorphism $\alpha: G \rightarrow \mathcal{S}_\Omega$ we have $\ker(\alpha) = \bigcap_{x \in \Omega} G_x \trianglelefteq G$.

For $x \in \Omega$ and $g \in G$ we have $G_{xg} = (G_x)^g$: For $h \in G_x$ we have $(xg)g^{-1}hg = xg$, hence $(G_x)^g \subseteq G_{xg}$; conversely from $(G_{xg})^{g^{-1}} \subseteq G_x$ we get $G_{xg} \subseteq (G_x)^g$. In particular, elements of Ω in the same G -orbit have G -conjugate stabilizers.

(0.10) Example. a) i) Any group G acts **trivially** on any set Ω by $\Omega \rightarrow \Omega: x \mapsto x$, for $g \in G$; the associated action homomorphism is $G \rightarrow \mathcal{S}_\Omega: g \mapsto \text{id}_\Omega$. The orbits are the singleton subsets of Ω , and we have $G_x = G$ for all $x \in \Omega$.

ii) Any group G acts by **conjugation** on itself by $\kappa_g: G \rightarrow G: x \mapsto x^g := g^{-1}xg$, for $g \in G$: We have $\kappa_1 = \text{id}_G$, and $\kappa_g\kappa_h = \kappa_{gh}: x \mapsto h^{-1}(g^{-1}xg)h = (gh)^{-1}x(gh)$. The associated orbits are called the **conjugacy classes** of G , and $C_G(x) := G_x = \{g \in G; x^g = x\} = \{g \in G; xg = gx\} \leq G$ is called the **centraliser** of x in G .

For the associated action homomorphism $\kappa: G \rightarrow \mathcal{S}_G$ we have $Z(G) := \ker(\kappa) = \bigcap_{x \in G} C_G(x) = \{g \in G; xg = gx \text{ for all } x \in G\} \trianglelefteq G$, being called the **centre** of G . From $(xy)^g = g^{-1}(xy)g = g^{-1}xg \cdot g^{-1}yg = x^g y^g$, for $x, y, g \in G$, we infer that $\kappa_g \in \text{Aut}(G)$, being called the **inner** automorphism of G afforded by g . Hence we actually have $\kappa: G \rightarrow \text{Aut}(G)$, whose image $\text{Inn}(G) := \kappa(G) \leq \text{Aut}(G)$ is called the **inner automorphism group** of G ; thus we have $\text{Inn}(G) \cong G/Z(G)$.

iii) Similarly, G acts on the set of its subgroups by conjugation $\kappa_g: U \mapsto U^g$, for $U \leq G$ and $g \in G$. The associated orbits are called the **conjugacy classes** of subgroups of G , and the stabiliser $N_G(U) := \text{Stab}_G(U) = \{g \in G; Ug = gU\}$ is called the **normaliser** of U in G .

Thus $N_G(U)$ is the largest subgroup of G having U as a normal subgroup, in particular $U \leq N_G(U)$, and $N_G(U) = G$ if and only if $U \trianglelefteq G$. Moreover, we have a group homomorphism $\kappa: N_G(U) \rightarrow \text{Aut}(U)$, whose kernel $C_G(U) := \bigcap_{u \in U} C_G(u) \trianglelefteq N_G(U)$ is called the **centraliser** of U in G ; thus $N_G(U)/C_G(U)$ is isomorphic to a subgroup of $\text{Aut}(U)$.

iv) Any group G acts **regularly** on itself by $\rho_g: G \rightarrow G: x \mapsto xg$, for $g \in G$: We have $\rho_1 = \text{id}_G$, and $\rho_g\rho_h = \rho_{gh}$ by associativity. Since $1 \cdot g = g$, for $g \in G$, the action is transitive, and we have $G_x = \{1\}$, for $x \in G$. Moreover, letting $\rho: G \rightarrow \mathcal{S}_G: g \mapsto \rho_g$ be the associated action homomorphism, for $g \in \ker(\rho)$ we have $g = 1 \cdot g = \rho_g(1) = \text{id}_G(1) = 1$, implying that ρ is injective; thus we have **Cayley's Theorem**, saying that G is isomorphic to a subgroup of $\mathcal{S}_G$.

b) i) For $n \geq 0$ the group $\mathcal{S}_n$ acts **naturally** on $\{1, \dots, n\}$, that is with action homomorphism $\text{id}_{\mathcal{S}_n}$. The action is transitive, and we have $\text{Stab}_{\mathcal{S}_n}(n) = \{\pi \in \mathcal{S}_n; n\pi = n\} = \mathcal{S}_{n-1}$. Hence for $\pi \in \mathcal{S}_n$ the subgroup $\langle \pi \rangle \leq \mathcal{S}_n$ also acts on $\{1, \dots, n\}$, its orbits coincide with the cycles of π .

ii) If K is a field, the group $\text{GL}_n(K)$ acts faithfully **naturally** by K -linear maps on the K -vector space K^n . The orbits are given as $\{0\}$ and $K^n \setminus \{0\}$; hence the action is transitive if and only if $n = 0$.

(0.11) Transitive actions. a) Let G be a group and let $U \leq G$. Then U acts on G by **left multiplication** $\lambda_u: G \rightarrow G: g \mapsto u^{-1}g$, for $u \in U$: We

have $\lambda_1(g) = g$ and $\lambda_{uv}(g) = (uv)^{-1}g = v^{-1}u^{-1}g = (\lambda_u\lambda_v)(g)$, for $g \in G$ and $u, v \in U$. Hence the U -orbit of $g \in G$ is the right coset $Ug \subseteq G$, so that the set of U -orbits coincides with $U \backslash G$, and we have $\text{Stab}_U(g) = \{1\}$.

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

b) Let Ω be a transitive G -set, and let $x \in \Omega$. Then the natural map $\alpha: G_x \backslash G \rightarrow \Omega: G_x g \mapsto xg$ is a G -set isomorphism; in other words, the G -sets Ω and $G_x \backslash G$ are equivalent: For $g, h \in G$ and $u \in G_x$ we have $xug = xg$, hence α is well-defined; and $\alpha(G_x hg) = x(hg) = (xh)g = \alpha(G_x h) \cdot g$ shows that α is a G -set homomorphism; since Ω is transitive, α is surjective; and whenever $xh = xg$ then we have $hg^{-1} \in G_x$, hence $h \in G_x g$, thus α is injective as well.

Thus, if G is finite then we have the **orbit-stabilizer theorem**, saying that for any $x \in \Omega$ we have $|\Omega| = |G_x \backslash G| = [G: G_x] = \frac{|G|}{|G_x|}$; in particular $|\Omega| \mid |G|$.

c) Transitive G -sets Ω and Ω' are equivalent if and only if there are $x \in \Omega$ and $y \in \Omega'$ such that $G_y = G_x$: If $\alpha: \Omega \rightarrow \Omega'$ is an isomorphism of G -sets, then for any $x \in \Omega$ and $g \in G_x$ we have $\alpha(x)g = \alpha(xg) = \alpha(x)$, implying $G_x \leq G_{\alpha(x)}$, and hence by symmetry $G_x = G_{\alpha(x)}$; conversely, let $x \in \Omega$ and $y \in \Omega'$ such that $G_y = G_x$, then we have $\Omega \cong G_x \backslash G \cong G_y \backslash G \cong \Omega'$ as G -sets.

Recalling that stabilisers of elements of a transitive G -set are mutually G -conjugate, this yields the following classification of transitive G -sets: Transitive G -sets are equivalent if and only if the associated stabilisers belong to one and the same conjugacy class of subgroups of G .

For the action homomorphism associated with a transitive G -set Ω we have $\ker(\alpha) = \text{core}_G(G_x) := \bigcap_{g \in G} (G_x)^g \trianglelefteq G$, called the **core** of G_x in G , where the latter is the largest normal subgroup of G being contained in G_x : If $N \trianglelefteq G$ such that $N \leq G_x$, then we have $N = N^g \leq (G_x)^g$, for $g \in G$, thus $N \leq \text{core}_G(G_x)$.

(0.12) Counting with groups. We provide a useful tool allowing to determine the number of orbits of a finite group action on a finite set: To this end, for a G -set Ω , and $S \subseteq G$, let $\text{Fix}_\Omega(S) = C_\Omega(S) := \{x \in \Omega; xg = x \text{ for } g \in S\} \subseteq \Omega$ be the set of **fixed points** or the **centraliser** of S in Ω . (Note that for the conjugation action of G on itself, and $H \leq G$, we indeed recover $C_G(H) = \{x \in G; x^h = x \text{ for } h \in H\} = \{x \in G; xh = hx \text{ for } h\} = \{x \in G; h^x = h \text{ for } h\}$.)

Theorem: Orbit Counting Lemma [Cauchy–Frobenius–Burnside].

Let both G and Ω be finite. Then we have $|\Omega/G| = \frac{1}{|G|} \cdot \sum_{g \in G} |\text{Fix}_\Omega(g)|$.

Proof. Letting $\mathcal{O} := \{[x, g] \in \Omega \times G; xg = x\}$, we use **double counting**: On the one hand we get $|\mathcal{O}| = \sum_{g \in G} |\{x \in \Omega; xg = x\}| = \sum_{g \in G} |\text{Fix}_\Omega(g)|$. On the other hand we get $|\mathcal{O}| = \sum_{x \in \Omega} |\{g \in G; xg = x\}| = \sum_{x \in \Omega} |G_x|$. For $y \in x^G$ we have $|G_y| = |G_x|$. Letting $\mathcal{S} \subseteq \Omega$ be orbit representatives, we get $\sum_{x \in \Omega} |G_x| = \sum_{x \in \mathcal{S}} \sum_{y \in x^G} |G_y| = \sum_{x \in \mathcal{S}} |x^G| \cdot |\text{Stab}_G(x)| = \sum_{x \in \mathcal{S}} |G| = |\Omega/G| \cdot |G|$. $\#$

Example: Action on maps. In algebraic combinatorics group actions can be used to count the number of possible ‘configurations’ up to symmetry, where the ‘configurations’ are acted on by a suitable group, so that the equivalence classes with respect to symmetry are just the orbits of the group action. The following typical situation is merely the starting point of so-called **Polya Theory**:

For $n, k \geq 0$ let $\mathcal{M} = \mathcal{M}_{n,k}$ be the set of maps f from $\{1, \dots, n\}$ to $\{1, \dots, k\}$, hence we have $|\mathcal{M}| = k^n$; in combinatorial terms $\mathcal{M}$ can be viewed as the set of all possible **colorings** of n objects with at most k colors. Then $\mathcal{S}_n$ acts on $\mathcal{M}$ by **pre-composition** $\pi: f \mapsto \pi^{-1}f =: f^\pi$: We have $f^{\text{id}} = f$, and $f^{\pi\rho} = (\pi\rho)^{-1}f = \rho^{-1}\pi^{-1}f = (\pi^{-1}f)^\rho = (f^\pi)^\rho$, for $\pi, \rho \in \mathcal{S}_n$. Identifying f with the tuple $[f(1), \dots, f(n)]$, note that $\mathcal{S}_n$ acts by **reordering** the entries.

Depending on the combinatorial interpretation, the relevant symmetry group is a certain subgroup $G \leq \mathcal{S}_n$, so that we have to determine $|\mathcal{M}/G|$. In order to apply the Orbit Counting Lemma, we have to determine $|\text{Fix}_{\mathcal{M}}(\pi)|$: For $f \in \mathcal{M}$ we have $f^\pi = f$, that is $i\pi^{-1}f = if$ for all $i \in \{1, \dots, n\}$, if and only if f is constant on the various cycles of π ; hence if π has r cycles then $|\text{Fix}_{\mathcal{M}}(\pi)| = k^r$.

Example: Chirality. We consider the colorings of the $n = 4$ vertices of the regular tetrahedron with at most $k = 4$ colors, that is the set $\mathcal{M} = \mathcal{M}_{4,4}$, being acted on by the polyhedral groups $\mathcal{S}_4$ and $\mathcal{A}_4$, where the former is the full symmetry group, while the latter is the rotation group.

The cycle types of the elements of $\mathcal{S}_4$ are $\{[4]^6, [2, 1^2]^6, [3, 1]^8, [2^2]^3, [1^4]^1\}$, where exponents denote multiplicities; the latter three types belong to even partitions. Applying the Orbit Counting Lemma we get $|\mathcal{M}/\mathcal{S}_4| = \frac{1}{24} \cdot (6 \cdot 4^1 + 6 \cdot 4^3 + 8 \cdot 4^2 + 3 \cdot 4^2 + 1 \cdot 4^4) = 35$ and $|\mathcal{M}/\mathcal{A}_4| = \frac{1}{12} \cdot (8 \cdot 4^2 + 3 \cdot 4^2 + 1 \cdot 4^4) = 36$.

Since the $\mathcal{S}_4$ -orbits in $\mathcal{M}$ are unions of $\mathcal{A}_4$ -orbits, the above result implies that there is precisely one $\mathcal{S}_4$ -orbit which splits into two $\mathcal{A}_4$ -orbits. Actually, it is given as follows: Let $f = [1, 2, 3, 4] \in \mathcal{M}$, which is a coloring where all 4 colors actually occur. Then we have $\text{Stab}_{\mathcal{S}_4}(f) = \{1\}$. Hence $f^{\mathcal{S}_4}$ has length 24, thus consists of all bijective maps. Hence we have $\text{Stab}_{\mathcal{A}_4}(f) = \{1\}$ as well, implying that $f^{\mathcal{A}_4}$ has length 12. Moreover, letting $f' := f^{(1,2)} = [2, 1, 3, 4]$, from $\mathcal{S}_4 = \mathcal{A}_4 \cup (1, 2) \cdot \mathcal{A}_4$ we get $f^{\mathcal{S}_4} = f^{\mathcal{A}_4} \cup (f')^{\mathcal{A}_4}$,

In chemistry, this phenomenon is known as **chirality** (research into which has won the Nobel prize in chemistry in 2026): A methane molecule, consisting of a central carbon atom and four hydrogen atoms attached to it, carries the symmetry of a regular tetrahedron. If now the hydrogen atoms are replaced by four pairwise distinct ligands, then the resulting molecule exists in a ‘right handed’ and a ‘left handed’ variant. These cannot be transformed into each other by rotations (which exist in reality), but only by reflections (which do not), so that the two variants actually behave differently.