**Normal subgroup**:

A subgroup $N$ in a group $G$ is *normal* if the left and right cosets are the same, i.e. $N \leq G$ and $gN = Ng$ for every $g \in G$. Notation: $N \triangleleft G$.

The condition $Ng = gN$ means that (i) $Ng \subseteq gN$ and (ii) $gN \subseteq Ng$, i.e. to every $n \in N$ there exist elements $n_1$ and $n_2$ in $N$ such that (i) $ng = gn_1$ and (ii) $gn = n_2 g$ (and does not mean $ng = gn$!). These two are equivalent to (i) $g^{-1}ng \in N$ and (ii) $gng^{-1} \in N$. If (i) holds for every $g \in G$, then applying it with $g^{-1}$ instead of $g$ we get (ii). Thus we obtained:

$N \triangleleft G \iff N \leq G$ and $g^{-1}ng \in N$ for every $g \in G$ and $n \in N$.

Here $g^{-1}ng$ is called a *conjugate* of $n$.

*Examples*:

If $G$ is commutative, then every subgroup is normal, but the converse is false, see e.g. the *quaternion* group

$$Q = \{\pm 1, \pm i, \pm j, \pm k \mid i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j\}.$$

The trivial subgroups $\{e\}$ and $G$ are always normal.

The subgroups $H$ of index 2 are normal, too, as $H = eH = He$ is both a left and a right coset, and the rest of the group is the other coset, thus it must be both left and right.

In $D_4$, $\langle r^2 \rangle$ is normal, but $\langle t \rangle$ is not.

An important normal subgroup is the center $Z(G)$: this is the set of elements commuting with every element of the group, i.e.

$$Z(G) = \{c \in G \mid cg = gc \text{ for every } g \in G\}.$$

Moreover, every subgroup of the center is normal.

**Factor group** and **group homomorphism**:

The elements in the *factor group* $G/N$ are the cosets of a normal subgroup $N$ and the operation is defined by $(aN)(bN) = abN$.

We show that this is a group. $N = eN$ is the identity, $(aN)^{-1} = a^{-1}N$, and associative law follows from the associative law in $G$:

$$\big((aN)(bN)\big)(cN) = (abN)(cN) = \big((ab)c\big)N = \big(a(bc)\big)N = (aN)(bcN) = (aN)\big((bN)(cN)\big).$$

Similarly to the situation in rings, the only critical point is that the operation is well-defined for the cosets: we defined the operation using arbitrary $a$ and $b$ elements in the two cosets $aN$ and $bN$, so we have to show that the result is independent of the choice of $a$ and $b$, i.e. $aN = a_1N, bN = b_1N \Rightarrow abN = a_1b_1N$. For any subgroup $H$, we have $uH = vH \iff v^{-1}uH = H \iff v^{-1}u \in H$. So we can rewrite the required implication as $a_1^{-1}a \in N, b_1^{-1}b \in N \Rightarrow (a_1b_1)^{-1}ab \in N$. Proof:

$$(a_1b_1)^{-1}ab = b_1^{-1}a_1^{-1}ab = b_1^{-1}n_1b = b_1^{-1}bb^{-1}n_1b = n_2n_3 = n_4$$

where $n_1, n_2 \in N$ due to the assumption, $n_3 \in N$ as $N$ is normal, and $n_4 \in N$ as $N$ is a subgroup.

A map $\varphi : G_1 \to G_2$ (where $G_i$ are groups) is a *group homomorphism* if it preserves the operation, i.e. $\varphi(gh) = \varphi(g)\varphi(h)$ for every $g, h \in G_1$.

It is easy to check the following basic properties for homomorphisms: $\varphi(e_1) = e_2$; $\varphi(g^{-1}) = (\varphi(g))^{-1}$; the kernel $\operatorname{Ker}\varphi = \{g \in G_1 \mid \varphi(g) = e_2\} \lhd G_1$; and the image $\operatorname{Im}\varphi = \{\varphi(g) \mid g \in G_1\} \leq G_2$.

A bijective homomorphism is called an *isomorphism*. A homomorphism $\varphi$ is an isomorphism iff $\operatorname{Ker}\varphi = e_1$ and $\operatorname{Im}\varphi = G_2$. The second condition is equivalent to the surjectivity of $\varphi$, and the first one is equivalent to the injectivity, as

$$\varphi(a) = \varphi(b) \iff \varphi(b)^{-1}\varphi(a) = e_2 \iff \varphi(b^{-1}a) = e_2 \iff b^{-1}a \in \operatorname{Ker}\varphi.$$

*Homomorphism theorem* or *First isomorphism theorem*: If $\varphi : G_1 \to G_2$ is a homomorphism, then $\operatorname{Im}\varphi \cong G_1/\operatorname{Ker}\varphi$.

The idea of the proof is that a coset contains all elements of $G_1$ which are mapped to the same element in $G_2$, hence there is a bijection between the cosets and the elements of $\operatorname{Im}\varphi$, and this bijection preserves the operation.

*Natural homomorphism*: If $N \lhd G$, then $\psi : G \to G/N$ defined by $\psi(g) = gN$ is a homomorphism with $\operatorname{Ker}\psi = N$ and $\operatorname{Im}\psi = G/N$.

Hence, homomorphism theorem and natural homomorphism establish a one-to-one correspondence between factor groups and homomorphisms (and thus also between normal subgroups and homomorphisms) of a group.

**Direct product of groups**

The *direct product* $G_1 \times G_2$ of groups $G_1$ and $G_2$ is the group of all ordered pairs $(g_1, g_2)$ where $g_i \in G_i$, with a multiplication defined by multiplying the "components": $(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2)$.

It is easy to check that this is a group, and the "projection" subsets $G_1^* = \{(g_1, e_2) \mid g_1 \in G_1\}$ and $G_2^* = \{(e_1, g_2) \mid g_2 \in G_2\}$ are isomorphic to $G_1$ and $G_2$, resp.

Further, $G_1^*$ and $G_2^*$ are normal subgroups in the direct product, and every $u \in G_1 \times G_2$ has a unique decomposition $u = u_1u_2$ with $u_i \in G_i^*$.

Also the converse is true: If $N$ and $M$ are normal subgroups in a group $G$ such that every $g \in G$ can be uniquely written as $g = nm$ with $n \in N, m \in M$, then $G \cong N \times M$.

Proof: We show that $\varphi : G \to N \times M$ defined by $\varphi(nm) = (n, m)$ is an isomorphism. It is clearly a bijection, we have to check that it preserves the operation:

$$\varphi\big((n_1m_1)(n_2m_2)\big) = \varphi(n_1m_1)\varphi(n_2m_2). \tag{1}$$

As a preparation, we verify (*) $mn = nm$ for every $m \in M, n \in N$. Multiplying (*) first by $n^{-1}$, and then by $m^{-1}$ from the left, we get the equivalent form $m^{-1}n^{-1}mn = e$. Using normality, the product of the first three factors is in $N$, and since $N$ is a subgroup, the entire product is in $N$. Similarly, it is in $M$, and so in $N \cap M$, too. If $g \in M \cap N$, then $g = ge = eg$, but $g$ has a unique representation as $nm$, $n \in N, m \in M$, therefore $g = e$. This proves (*).

Using (*), the left hand side in (1) is $\varphi\big((n_1n_2)(m_1m_2)\big) = (n_1n_2, m_1m_2)$, and the right hand side is $(n_1, m_1)(n_2, m_2) = (n_1n_2, m_1m_2)$ proving thus (1).

We note that $G_1 \times G_2/G_1^* \cong G_2$ (and similarly, $G_1 \times G_2/G_2^* \cong G_1$). One way to prove it is to check that a coset can be characterized by all elements having the same second component, and this yields a bijection which preserves the operation. An alternative solution is to use the homomorphism theorem for the map $\psi : G_1 \times G_2 \to G_2$ defined as $\psi\big((g_1, g_2)\big) = g_2$.

Direct products of more than two groups can be defined and treated analogously.

Direct product makes possible the construction of groups with various prescribed properties, and in the other direction, it can help to detect the structure of a group by reducing the problem to the investigation of the direct factors. In the latter respect, the *Fundamental Theorem of Finite Abelian Groups* states that every finite Abelian group is the direct product of cyclic groups of prime power size, and the list of the direct factors is uniquely determined. (The cyclic groups of prime power size form one-factor products, and $e$ alone is an empty product.) As an illustration we determine all commutative groups $G$ of size 200. If $G = G_1 \times \ldots \times G_r$, then clearly $|G| = |G_1| \cdot \ldots \cdot |G_r|$. Hence, we have to find all representations of 200 as the product of prime powers:

$$25 \cdot 8; \quad 25 \cdot 4 \cdot 2; \quad 25 \cdot 2 \cdot 2 \cdot 2; \quad 5 \cdot 5 \cdot 8; \quad 5 \cdot 5 \cdot 4 \cdot 2; \quad 5 \cdot 5 \cdot 2 \cdot 2 \cdot 2.$$

Thus all (pairwise non-isomorphic) Abelian groups of size 200 are

$$\mathbf{Z}_{25} \times \mathbf{Z}_8; \mathbf{Z}_{25} \times \mathbf{Z}_4 \times \mathbf{Z}_2; \mathbf{Z}_{25} \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2; \mathbf{Z}_5 \times \mathbf{Z}_5 \times \mathbf{Z}_8; \mathbf{Z}_5 \times \mathbf{Z}_5 \times \mathbf{Z}_4 \times \mathbf{Z}_2; \mathbf{Z}_5 \times \mathbf{Z}_5 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2.$$

freud@caesar.elte.hu freud.web.elte.hu/bsm/index.html