Def. Let G be a group and let H be a subgroup of G. We say H is a normal subgroup of G and write $H \trianglelefteq G$ if $gH = Hg$ for all $g \in G$.

Examples a) For every group G with identity e the subgroups G and $\{e\}$ are normal.

b) For an abelian group every subgroup is normal.

c) In $S_3 = D_3 = \{e, \rho, \rho^2, \alpha, \beta, \gamma\}$ as defined earlier, we have $H = \{e, \rho, \rho^2\}$ is a normal subgroup, whereas $K = \{e, \alpha\}$ is not normal. In fact $\beta K = \{\beta, \rho\} \neq \{\beta, \rho^2\} = K\beta$.

Prop. For a subgroup H of the group G the following are equivalent.

(i) $H \trianglelefteq G$

(ii) $g^{-1}Hg = H$ for all $g \in G$

(iii) $g^{-1}Hg \subseteq H$ for all $g \in G$.

proof: (i) $\Rightarrow$ (ii): $g^{-1}Hg = g^{-1}gH = H$ for all $g \in G$ when we assume $Hg = gH$ for all $g \in G$

(ii) $\Rightarrow$ (iii) ✓

(iii) $\Rightarrow$ (i) Assuming $g^{-1}Hg \subseteq H$ for all $g \in G$ (25)

we compute
$$\begin{array}{c} gg^{-1}Hg \subseteq gH \\ \| \\ Hg \end{array}$$
for all $g \in G$. Then this is also true for g^{-1}, i.e. $g^{-1}H \supseteq Hg^{-1}$ for all $g \in G$. But then we have
$$\begin{array}{c} gg^{-1}Hg \supseteq gHg^{-1}g = gH \\ \| \\ Hg \end{array}$$
for all $g \in G$, which concludes the proof.

Def: A group G is called a simple group if it has no normal subgroups except the trivial ones.

Example a) $\mathbb{Z}_p$ the cyclic groups of prime order

b) $A_n = \{\pi \in S_n \mid \operatorname{sign}(\pi) = 1\}$ where $n \geq 2$ the so called alternating group.

Def: Let G be a group and let N be a normal subgroup. The (left and right) cosets form a set that we denote by $G/N := \{gN \mid g \in G\}$.

We define a binary operation on G/N

$$* : G/N \times G/N \longrightarrow G/N$$
$$(gN, hN) \longmapsto gN * hN := ghN.$$

<u>Lemma</u>: The operation is well defined, ie if $gN = g'N$ and $hN = h'N$, then $ghN = g'h'N$.

<u>proof</u>. $gN = g'N$ implies $n \in N$ with $g = g'n$ also we have ~~...~~ $h = h'm$ for some ~~...~~ $m \in N$. Now we compute $ghN = g'nh'mN = g'nh'N = g'nNh' = g'Nh' = g'h'N$.

<u>prop</u>: The operation $*$ induces a group structure on G/N, which means that
(i) $*$ is associative
(ii) N is the identity
(iii) $g^{-1}N$ is the inverse of gN.

<u>proof</u>: We only check associativity and compute $(aN * bN) * cN = abN * cN = (ab)cN = a(bc)N = aN * bcN = aN * (bN * cN)$, so we see that we have reduced the argument to the associativity of the operation on G.

<u>Example</u>. a) Let $G = \{e, \varrho, \varrho^2, \alpha, \beta, \gamma\}$ our favorite group with 6 elements. We have seen earlier, that $H = \{e, \alpha\}$ is not a normal subgroups, nor are $H = \{e, \beta\}$ nor $H = \{e, \gamma\}$. But as for $H = \{e, \varrho, \varrho^2\}$ we have $[G : H] = 2$, we know that $H = \{e, \varrho, \varrho^2\} = \varrho H = \varrho^2 H$ and $G \setminus H = \{\alpha, \beta, \gamma\} = \alpha H = \beta H = \gamma H$.

For the Cayley table of G/H we find

$\cdot$	H	$G\setminus H$
H	H	$G\setminus H$
$G\setminus H$	$G\setminus H$	H

which is the cyclic group of order 2, that we have met earlier in the form $(\mathbb{Z}_2, +, 0)$ or $(\{1, -1\}, \cdot, 1)$.

Indeed there is a basic similarity in these 3 groups that we will discuss within the next pages.

b) Let $G = (\mathbb{Z}, +, 0)$ and $H = n \cdot \mathbb{Z}$.

Of course H is normal in G because G is abelian. We have

$$G/H = \{ z + n \cdot \mathbb{Z} \mid z \in \mathbb{Z} \}$$

As two cosets $z + n\mathbb{Z}$ and $z' + n\mathbb{Z}$ are the same, if z and z' differ by a multiple of n, in other words if $z \equiv z' \pmod{n}$ we have

$$G/H = \{ z + n\mathbb{Z} \mid z = 0, 1, \ldots n-1 \}.$$

As a matter of fact, the operation on G/H involves integer addition and then reduction $(\bmod\ n)$. This means

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = \underbrace{(a+b)}_{(\bmod\ n)} + n\mathbb{Z}.$$

and the identity is $n\mathbb{Z} = 0 + n\mathbb{Z}$, which suggests, that computing in $\mathbb{Z}_n$ modulo n seems to be the same as using G/H.

More to come!