Definition 5.1

Let G be a group. A subset $H \subseteq G$ is a *subgroup* of G if it is a group under the operation in G.

Examples.

- $\mathbb{Z}$ and $\mathbb{Q}$ are subgroups of $\mathbb{R}$.
- $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$.
- Let $H \subseteq \mathbb{Z}$ be the set of all odd integers. This is not a subgroup of $\mathbb{Z}$ since e.g. $3, 5 \in H$ but $3 + 5 \notin H$.
- Let $H \subset GL(2, \mathbb{R})$ be a set consisting of all invertible matrices with integer entries. Then H is not not a subgroup of $GL(2, \mathbb{R})$ since, for example,

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \in H \qquad \text{but} \qquad A^{-1} = \begin{bmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{bmatrix} \notin H$$

Theorem 5.2

Let G be a group. A subset $H \subseteq G$ is a subgroup of G if and only if the following conditions are satisfied:

1) The identity element e belongs to H.
2) If $a, b \in H$ then $a \cdot b \in H$.
3) If $a \in H$ then $a^{-1} \in H$.

Exercise. The dihedral group D_4 has the following multiplication table:

$\circ$	I	R_{90}	R_{180}	R_{270}	H	V	D	D'
I	I	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	I	D'	D	H	V
R_{180}	R_{180}	R_{270}	I	R_{90}	V	H	D'	D
R_{270}	R_{270}	I	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	I	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	I	R_{270}	R_{90}
D	D	H	D'	V	R_{270}	R_{90}	I	R_{180}
D'	D'	V	D	H	R_{90}	R_{270}	R_{180}	I

Find all subgroups of D_4.

Definition 5.3

The *center* of a group G is a set $Z(G) \subset G$ consisting of elements that commute with all elements of G:

$$Z(G) = \{g \in G \mid ag = ga \text{ for all } a \in G\}$$

Exercise. Find the center of the dihedral group D_4.

Theorem 5.4

If G is a group then the center $Z(G)$ of G is a subgroup of G.

Proof. 1) For the identity element $e \in G$ we have

$$ea = a = ae$$

for any $a \in G$, so $e \in Z(G)$

2) Assume that $g, h \in Z(G)$. We will show that then $gh \in Z(G)$. Indeed, for any element $a \in G$ we have

$$a(gh) = (ag)h = (ga)h = g(ah) = g(ha) = (gh)a$$

3) Assume that $g \in Z(G)$. We need to show that then $g^{-1} \in Z(G)$. For any $a \in G$ we have

$$ag^{-1} = (ga^{-1})^{-1} = (a^{-1}g)^{-1} = g^{-1}a^{-1}$$

$\square$

Definition 5.5

Let G a group and let $a \in G$. The *centralizer* of a in G is the set $C(a) \subseteq G$, which consists of all elements of G that commute with a:

$$C(a) = \{g \in G \mid ag = ga\}$$

Exercise. Find the centralizer of the element V in D_4.

Theorem 5.6

If G is a group and a then the centralizer $C(a)$ of a in G is a subgroup of G.

Proof. Similar as for Theorem 5.4. $\square$

Definition 5.7

If G is a group and S is a non-empty subset of G, then $\langle S \rangle$ denotes the smallest subgroup of G containing all elements of S:

$$\langle S \rangle = \{a_1^{k_1} \cdot a_2^{k_2} \cdot \dots \cdot a_n^{k_n} \mid n \geq 1 \text{ and for each } i \text{ we have } g_i \in S \text{ and } k_i \in \mathbb{Z}\}$$

We say that $\langle S \rangle$ is the *subgroup of G generated by the set S*.

Note. If $a \in G$ then $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$.

Exercise. Find the subgroup $\langle 2 \rangle$ in $\mathbb{Z}_{10}$

Exercise. Find the subgroup $\langle 2 \rangle$ in $\mathbb{Z}_9$

Exercise. Find the subgroup $\langle V, R_{180} \rangle$ in D_4

Recall:

- The order of a group G is the number of elements of G. It is denoted by $|G|$.

- The order of an element a of a group G is the smallest integer $n > 0$ such that $a^n = e$. It is denoted by $|a|$.

Theorem 5.8

Let G be a group, let $a \in G$ and let $\langle a \rangle$ be the subgroup of G generated by a. Then

$$|a| = |\langle a \rangle|$$

Proof. Assume that $|a| = n$. We will show that the group $\langle a \rangle$ consists of n distinct elements: $e = a^0, a^1, a^2, \dots, a^{n-1}$.

First, we show that all these elements are different. Indeed, if $0 \leq k < l < n$ and $a^k = a^l$ then $0 \leq l - k < n$ and

$$a^{l-k} = a^l \cdot a^{-k} = a^k \cdot a^{-k} = e.$$

This is impossible since $l - k$ is smaller that the order of a.

Next, let take $k \geq n$. Then $k = qn + r$ for some $q, r \in \mathbb{Z}$, $0 \leq r < n$. Then $a^k = a^r$. $\square$