Course 2

1.3 Subgroups

We turn now our attention to the study of a group inside another group. Recall that the associative law and the commutative law transfer in a stable subset, whereas the identity element and the inverse element do not in general. But we will see that they do transfer in a subgroup.

Definition 1.3.1 Let $(G, \cdot)$ be a group and let $H \subseteq G$. Then H is called a *subgroup of* G if:
(1) H is a stable subset of $(G, \cdot)$, that is, $\forall x, y \in H$, $x \cdot y \in H$;
(2) $(H, \cdot)$ is a group.

We denote by $H \leq G$ the fact that H is a subgroup of G.

The following two characterization theorems provide two easy ways of checking that a subset of a group is a subgroup.

Theorem 1.3.2 *Let $(G, \cdot)$ be a group and let $H \subseteq G$. Then $H \leq G$ if and only if*
(i) $H \neq \emptyset$ ($1 \in H$);
(ii) $x, y \in H \Longrightarrow x \cdot y \in H$;
(iii) $x \in H \Longrightarrow x^{-1} \in H$.

Proof. $\Longrightarrow$. Suppose that $H \leq G$. Then $(H, \cdot)$ is a group, so that $H \neq \emptyset$.
Moreover, there exists an identity element $1' \in H$, hence

$$x \cdot 1' = 1' \cdot x = x, \quad \forall x \in H.$$

By multiplying by x^{-1} on the left or on the right, we get $1' = 1 \in H$. Therefore, a subgroup must contain the identity element of the group.
Condition (ii) holds by the definition of a subgroup.
Now let $x \in H$ and denote by x' its inverse in the group $(H, \cdot)$. Then

$$x \cdot x' = x' \cdot x = 1.$$

But $x \in H \subseteq G$ has an inverse $x^{-1} \in G$. Then by multiplying by x^{-1} on the left or on the right, we get $x' = x^{-1} \in H$.

$\Longleftarrow$. Suppose that the conditions (i), (ii) and (iii) hold. Then H is a stable subset of $(G, \cdot)$. Clearly, the associative law holds also in H. Take $x \in H \neq \emptyset$. Then by (iii), $x^{-1} \in H$ and by (ii), $1 = x \cdot x^{-1} \in H$. Hence 1 is the identity element in H. By (iii), every element of H has an inverse in H. Hence $(H, \cdot)$ is a group. Consequently, H is a subgroup of G. $\square$

Theorem 1.3.3 *Let $(G, \cdot)$ be a group and let $H \subseteq G$. Then $H \leq G$ if and only if*
(i) $H \neq \emptyset$ ($1 \in H$);
(ii) $x, y \in H \Longrightarrow x \cdot y^{-1} \in H$.

Proof. By Theorem 1.3.2. $\square$

Remark 1.3.4 (1) In the case of an additive group $(G, +)$, the conditions (ii) and (iii) in Theorem 1.3.2 become
(ii') $x, y \in H \Longrightarrow x + y \in H$;
(iii') $x \in H \Longrightarrow -x \in H$.

(2) In the case of an additive group $(G, +)$, the condition (ii) in Theorem 1.3.3 becomes
(ii') $x, y \in H \Longrightarrow x - y \in H$.

(3) For subsets X, Y of a group $(G, \cdot)$, we denote

$$X \cdot Y = \{x \cdot y \mid x \in X, y \in Y\},$$
$$X^{-1} = \{x^{-1} \mid x \in X\}.$$

Then the last two conditions from Theorem 1.3.2 are shortly written as $H \cdot H \subseteq H$ and $H^{-1} \subseteq H$, which are in fact equivalent to $H \cdot H = H$ (because $\forall x \in H$, $x = x \cdot 1 \in H \cdot H$, hence $H \subseteq H \cdot H$) and $H^{-1} = H$ (because $\forall x \in H$, $x = (x^{-1})^{-1} \in H^{-1}$, hence $H \subseteq H^{-1}$) respectively. Also, the last condition from Theorem 1.3.3 is shortly written as $H \cdot H^{-1} \subseteq H$, which is in fact equivalent to $H \cdot H^{-1} = H$.

Let us now see some examples of subgroups.

Example 1.3.5 (a) Every non-trivial group $(G,\cdot)$ has two subgroups, namely $\{1\}$ and G, called the *trivial subgroups*.

(b) $\mathbb{Z}$ is a subgroup of $(\mathbb{Q},+)$, $(\mathbb{R},+)$ and $(\mathbb{C},+)$. $\mathbb{Q}$ is a subgroup of $(\mathbb{R},+)$ and $(\mathbb{C},+)$. $\mathbb{R}$ is a subgroup of $(\mathbb{C},+)$.

(c) Consider the group $(\mathbb{Z},+)$. Then

$$H \leq \mathbb{Z} \Longleftrightarrow H = n\mathbb{Z} \text{ for some } n \in \mathbb{N}\,.$$

Indeed, suppose first that $H = n\mathbb{Z}$ for some $n \in \mathbb{N}$. Clearly, $H \neq \emptyset$. For every $x, y \in H$, we have $x = nk$ and $y = nl$ for some $k, l \in \mathbb{Z}$, whence

$$x - y = nk - nl = n(k - l) \in n\mathbb{Z} = H.$$

Then by Theorem 1.3.3, $H = n\mathbb{Z} \leq \mathbb{Z}$.

Conversely, suppose that $H \leq \mathbb{Z}$. If $H = \{0\}$, then $H = 0 \cdot \mathbb{Z}$ and we are done. Assume now that $H \neq \{0\}$. Then H contains a positive element (if $x \in H$ and $x < 0$, then $-x \in H$ and $-x > 0$).

Denote

$$n = \min(H \cap \mathbb{N}^*).$$

We will prove that $H = n\mathbb{Z}$.

Since $n \in H$ and $H \leq \mathbb{Z}$, it follows that $n\mathbb{Z} \subseteq H$. Now if $x \in H$, then by the Division Algorithm, there exist unique $q, r \in \mathbb{Z}$ such that

$$x = nq + r\,, \quad \text{where} \quad 0 \leq r < n\,.$$

But then $r = x - nq \in H$ and $r \geq 0$. By the minimality of n, it follows that $r = 0$, so that $x = nq \in n\mathbb{Z}$, hence $H \subseteq n\mathbb{Z}$. Therefore, $H = n\mathbb{Z}$.

(d) The set

$$H = \{z \in \mathbb{C} \mid |z| = 1\}$$

is a subgroup of the group $(\mathbb{C}^*,\cdot)$, called the *circle group*. But it is not a subgroup of the group $(\mathbb{C},+)$.

(e) The set

$$U_n = \{z \in \mathbb{C} \mid z^n = 1\} \quad (n \in \mathbb{N}^*)$$

is a subgroup of the group $(\mathbb{C}^*,\cdot)$, called the *group of* n^{th} *roots of unity*. Its elements are the following:

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \quad k \in \{0, \ldots, n-1\}.$$

(f) Consider the general linear group $(GL_n(\mathbb{R}),\cdot)$ of rank n, where

$$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$$

$(n \in \mathbb{N}$, $n \geq 2)$ and denote

$$SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) = 1\}.$$

Then $SL_n(\mathbb{R})$ is a subgroup of $(GL_n(\mathbb{R}),\cdot)$, called the *special linear group of rank* n.

(g) Let $(G,\cdot)$ be a group. Then

$$Z(G) = \{x \in G \mid x \cdot g = g \cdot x\,, \forall g \in G\}$$

is a subgroup of G, called *the center of* G. We have $Z(G) = G$ if and only if G is abelian.

1.4 Generated subgroup. Subgroup lattice

For a group $(G,\cdot)$, we denote by $S(G,\cdot)$ the set of all subgroups of G.

We will see that the intersection is compatible with subgroups, whereas the union is not in general.

Theorem 1.4.1 *Let $(G,\cdot)$ be a group and let $(H_i)_{i\in I}$ be a family of subgroups of $(G,\cdot)$. Then $\bigcap_{i\in I} H_i \in S(G,\cdot)$.*

Proof. For each $i\in I$, $H_i \in S(G,\cdot)$, hence $1\in H_i$. Then $1\in \bigcap_{i\in I} H_i \neq \emptyset$. Now let $x,y\in \bigcap_{i\in I} H_i$. Then $x,y\in H_i$, $\forall i\in I$. But $H_i\in S(G,\cdot)$, $\forall i\in I$. It follows that $x\cdot y^{-1}\in H_i$, $\forall i\in I$, hence $x\cdot y^{-1}\in \bigcap_{i\in I} H_i$. Therefore $\bigcap_{i\in I} H_i\in S(G,\cdot)$ by the characterization theorem of subgroups. □

Example 1.4.2 We have seen that $S(\mathbb{Z},+)=\{n\mathbb{Z}\mid n\in\mathbb{N}\}$. Take $H=2\mathbb{Z}$, $K=3\mathbb{Z}\in S(\mathbb{Z},+)$. Then $H\cap K=2\mathbb{Z}\cap 3\mathbb{Z}=6\mathbb{Z}$ is a subgroup of $(\mathbb{Z},+)$. But $H\cup K=2\mathbb{Z}\cup 3\mathbb{Z}$ is not a subgroup of $(\mathbb{Z},+)$, because, for instance, we have $2,3\in H\cup K$, but $2+3=5\notin H\cup K$. Therefore, in general the union of subgroups is not a subgroup.

This leads to the idea of the subgroup generated by a subset of a group.

Definition 1.4.3 Let $(G,\cdot)$ be a group and let $X\subseteq G$. Then we denote

$$<X>=\bigcap\{H\leq G \mid X\subseteq H\}\in S(G,\cdot)$$

and we call it the *subgroup generated by* X.

In fact, $<X>$ is the "least" subgroup of G containing X.

Here X is called the *generating set* of $<X>$.

If $X=\{x\}$, then we denote $<x>=<\{x\}>$.

Remark 1.4.4 Notice that $<\emptyset>=\{1\}$ by Definition 1.4.3.

Let us now determine how the elements of a generated subgroup look like.

Theorem 1.4.5 *Let $(G,\cdot)$ be a group and let $\emptyset\neq X\subseteq G$. Then*

$$<X>=\{x_1\cdot x_2\cdot\ldots\cdot x_n \mid x_i\in X\cup X^{-1}\,, i=1,\ldots,n\,, n\in\mathbb{N}^*\}\,,$$

that is, the set of all finite products of elements or inverses of elements in X.

Proof. Denote by H the right hand side, that is,

$$H=\{x_1\cdot x_2\cdot\ldots\cdot x_n \mid x_i\in X\cup X^{-1}\,, i=1,\ldots,n\,, n\in\mathbb{N}^*\}\,.$$

We are going to prove that H is the least subgroup of G containing X, that is, to show the following 3 properties:

(i) $H\leq G$;

(ii) $X\subseteq H$;

(iii) If $K\leq G$ and $X\subseteq K$, then $H\subseteq K$.

Let us discuss them one by one.

(i) Clearly, we have $H\neq\emptyset$, because $X\neq\emptyset$. Let $x_1\cdot x_2\cdot\ldots\cdot x_m$, $y_1\cdot y_2\cdot\ldots\cdot y_n\in H$. Then

$$(x_1\cdot x_2\cdot\ldots\cdot x_m)\cdot(y_1\cdot y_2\cdot\ldots\cdot y_n)^{-1}=x_1\cdot x_2\cdot\ldots\cdot x_m\cdot y_n^{-1}\cdot\ldots\cdot y_2^{-1}y_1^{-1}\in H\,,$$

so that $H\leq G$ by the characterization theorem of subgroups.

(ii) Clear.

(iii) If $K\leq G$ and $X\subseteq K$, then $X^{-1}\subseteq K$ by by the characterization theorem of subgroups. It follows that $H\subseteq K$. □

Corollary 1.4.6 *Let $(G,\cdot)$ be a group and let $x\in G$. Then $<x>=\{x^k\mid k\in\mathbb{Z}\}$.*

Example 1.4.7 Consider the group $(\mathbb{Z},+)$ and let $n\in\mathbb{Z}$. Then $<n>=\{nk\mid k\in\mathbb{Z}\}=n\mathbb{Z}$.

Theorem 1.4.8 *Let $(G,\cdot)$ be a group. Then $(S(G,\cdot),\subseteq)$ is a complete lattice, in which*

$$\inf(H_i)_{i\in I} = \bigcap_{i\in I} H_i, \quad \sup(H_i)_{i\in I} =< \bigcup_{i\in I} H_i >$$

for every family $(H_i)_{i\in I}$ of subgroups of G.

Theorem 1.4.9 *Let $(G,\cdot)$ be a group and H_1, H_2 subgroups of G. Then*

$$H_1 \cdot H_2 \leq G \Leftrightarrow H_1 \cdot H_2 = H_2 \cdot H_1.$$

Proof. First assume that $H_1 \cdot H_2$ is a subgroup of G. Then $(H_1 \cdot H_2)^{-1} = H_1 \cdot H_2$, whence $H_2^{-1} \cdot H_1^{-1} = H_1 \cdot H_2$. Since H_1, H_2 are subgroups of G, we have $H_1^{-1} = H_1$ and $H_2^{-1} = H_2$. It follows that $H_2 \cdot H_1 = H_1 \cdot H_2$.

Conversely, assume that $H_1 \cdot H_2 = H_2 \cdot H_1$. Since $H_1 \neq \emptyset$ and $H_2 \neq \emptyset$, we have $H_1 \cdot H_2 \neq \emptyset$. Also, we have:

$$(H_1 \cdot H_2) \cdot (H_1 \cdot H_2) = H_1 \cdot (H_2 \cdot H_1) \cdot H_2 = H_1 \cdot (H_1 \cdot H_2) \cdot H_2 = (H_1 \cdot H_1) \cdot (H_2 \cdot H_2) = H_1 \cdot H_2,$$

$$(H_1 \cdot H_2)^{-1} = H_2^{-1} \cdot H_1^{-1} = H_2 \cdot H_1 = H_1 \cdot H_2.$$

Hence $H_1 \cdot H_2$ is a subgroup of G. □

Corollary 1.4.10 *Let $(G,\cdot)$ be a group and H_1, H_2 subgroups of G such that $H_1 \cdot H_2 = H_2 \cdot H_1$. Then:*

$$\sup(H_1, H_2) =< H_1 \cup H_2 >= H_1 \cdot H_2.$$

Proof. First, we have $H_1 \subseteq H_1 \cdot \{1\} \subseteq H_1 \cdot H_2$ and $H_2 \subseteq \{1\} \cdot H_2 \subseteq H_1 \cdot H_2$. Also, if H is a subgroup of G such that $H_1 \subseteq H$ and $H_2 \subseteq H$, then $H_1 \cdot H_2 \subseteq H \cdot H = H$. Hence $\sup(H_1, H_2) = H_1 \cdot H_2$. □

Example 1.4.11 (a) Let us determine the subgroup lattice of Klein's group $(K,\cdot)$. Its subgroups are: $\{e\}$, $\{e,a\}$, $\{e,b\}$, $\{e,c\}$ and K. One may draw its corresponding Hasse diagram.

(b) Let us determine the subgroup lattice of the group $(\mathbb{Z}_6,+)$. Its subgroups are: $\{\widehat{0}\}$, $\{\widehat{0},\widehat{2},\widehat{4}\}$, $\{\widehat{0},\widehat{3}\}$ and $\mathbb{Z}_6$. One may draw its corresponding Hasse diagram.