# Course 4: 15.03.2021

## 1.6 Cyclic groups. Order of an element

Recall that if $(G,\cdot)$ is a group and $x \in G$, then the subgroup generated by $x$ is

$$< x >= \{x^k \mid k \in \mathbb{Z}\}.$$

**Remark 1.6.1** If $(G,+)$ is an additive group and $x \in G$, then

$$< x >= \{kx \mid k \in \mathbb{Z}\}.$$

Throughout this section we will study those groups that are generated by a single element. They are essential tools in Group Theory.

**Definition 1.6.2** A group $(G,\cdot)$ is called *cyclic* if there exists $x \in G$ such that $G =< x >$, that is, $G = \{x^k \mid k \in \mathbb{Z}\}$.

**Remark 1.6.3** Notice that every cyclic group is commutative.

**Example 1.6.4** $(a)$ The group $(\mathbb{Z},+)$ is cyclic, because

$$\mathbb{Z} =< 1 >=< -1 > .$$

$(b)$ The group $(\mathbb{Z}_n,+)$ $(n \in \mathbb{N},\ n \geq 2)$ of residue classes modulo $n$ is cyclic, because

$$\mathbb{Z}_n =< \widehat{1} > .$$

$(c)$ The group $(U_n,\cdot)$ $(n \in \mathbb{N}^*)$ of $n$-th roots of unity is cyclic.

Indeed, $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ has $n$ elements, namely

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = \big(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\big)^k = \varepsilon_1^k, \quad k = 0,1,\ldots,n-1.$$

Then $U_n =< \varepsilon_1 > .$

**Definition 1.6.5** Let $(G,\cdot)$ be a group and let $x \in G$.

Then $x$ is said to have *finite order* if $\exists m \in \mathbb{N}^*$ such that $x^m = 1$ and *infinite order* otherwise.

If $x$ has finite order, then the non-zero natural number

$$\operatorname{ord} x = \min\{m \in \mathbb{N}^* \mid x^m = 1\}$$

is called the *order* of the element $x$.

If $G$ is finite, then the cardinal $|G|$ is called the *order* of the group $G$ and is denoted by $\operatorname{ord} G$.

**Remark 1.6.6** If $(G,+)$ is an additive group and $x$ has finite order, then

$$\operatorname{ord} x = \min\{m \in \mathbb{N}^* \mid mx = 0\}.$$

**Example 1.6.7** $(a)$ Consider the group $(\mathbb{R}^*,\cdot)$. Then $\operatorname{ord} 1 = 1$, $\operatorname{ord}(-1) = 2$ and every $x \in \mathbb{R}^* \setminus \{-1,1\}$ has infinite order.

$(b)$ Consider the group $(\mathbb{Z}_6,+)$. Then $\operatorname{ord}\widehat{0} = 1$, $\operatorname{ord}\widehat{1} = 6$, $\operatorname{ord}\widehat{2} = 3$, $\operatorname{ord}\widehat{3} = 2$, $\operatorname{ord}\widehat{4} = 3$, $\operatorname{ord}\widehat{5} = 6$ and $\operatorname{ord}\mathbb{Z}_6 = 6$.

**Lemma 1.6.8** *Let $(G,\cdot)$ be a group. Then:*

*(i) The unique element in $G$ of order 1 is the identity element 1.*

*(ii) $\forall x \in G$, $\operatorname{ord} x^{-1} = \operatorname{ord} x$.*

*Proof.* $(i)$ Obvious.

$(ii)$ Let $n \in \mathbb{N}^*$. For every $x \in G$, we have $(x^{-1})^n = 1 \iff x^{-n} = 1 \iff x^n = 1$. It follows that $\forall x \in G$, $\operatorname{ord} x^{-1} = \operatorname{ord} x$. Notice that one of the orders is finite iff the other one is finite as well. □

*Remark.* It is worth to emphasize the following idea, just used in Lemma 1.6.8: in order to prove that $\operatorname{ord} x = \operatorname{ord} y$, it is enough to prove that

$$x^n = 1 \iff y^n = 1\,, \qquad \forall n \in \mathbb{N}\,.$$

**Theorem 1.6.9** *Let $(G, \cdot)$ be a group, let $x \in G$ with $\operatorname{ord} x = n$ and let $m \in \mathbb{N}^*$. Then:*

$$x^m = 1 \iff n|m\,.$$

*Proof.* $\Longrightarrow$. Assume that $x^m = 1$. Using the Division Algorithm for $m$ and $n$, there exist unique $q, r \in \mathbb{N}$ such that

$$m = nq + r\,, \quad 0 \leq r < n\,.$$

Then

$$x^r = x^{m-nq} = x^m \cdot (x^n)^{-q} = 1\,,$$

so that $r = 0$, because the order $n$ is the least non-zero natural number $k$ such that $x^k = 1$. But then $m = nq$, i.e., $n|m$.

$\Longleftarrow$. Assume now that $n|m$. Then $\exists q \in \mathbb{N}$ such that $m = nq$. It follows that

$$x^m = x^{nq} = (x^n)^q = 1\,.$$

□

**Theorem 1.6.10** *Let $(G, \cdot)$ be a group and let $x \in G$.*

*(i) If $\operatorname{ord} x = n$, then*

$$< x >= \{1, x, x^2, \ldots, x^{n-1}\}$$

*and consequently $| < x > | = n$.*

*(ii) If $x$ has infinite order, then*

$$i, j \in \mathbb{Z}\,, i \neq j \Longrightarrow x^i \neq x^j\,,$$

*so that $< x >$ is infinite.*

*Proof.* $(i)$ Let $m \in \mathbb{Z}$. By the Division Algorithm, there exist unique $q, r \in \mathbb{Z}$ such that $m = nq + r$, where $0 \leq r < n$. Then we may write

$$x^m = (x^n)^q \cdot x^r = x^r$$

for some $r \in \{0, \ldots, n-1\}$.

Suppose further that $x^i = x^j$ for some $i, j \in \{0, \ldots, n-1\}$, say $j \leq i$. Then $x^{i-j} = 1$ and $0 \leq i - j < n$. Since $\operatorname{ord} x = n$, it follows that $i - j = 0$, hence $i = j$.

Therefore, $< x >= \{x^k \mid k \in \{0, 1, \ldots, n-1\}\}$ and $| < x > | = n$.

$(ii)$ Suppose that $x^i = x^j$ for some $i, j \in \mathbb{Z}$, say $j \leq i$. Then $x^{i-j} = 1$, whence $i = j$, because otherwise $\operatorname{ord} x$ would be finite. □

We have seen that the subgroups of the cyclic group $(\mathbb{Z}, +)$ are of the form $n\mathbb{Z} =< n > (n \in \mathbb{N})$, hence they are cyclic. We have even a more general result.

**Theorem 1.6.11** *Every subgroup of a cyclic group is cyclic.*

*Proof.* Let $(G, \cdot)$ be a cyclic group, say $G =< x >$, and let $H \leq G$.

If $H = \{1\}$, then $H =< 1 >$ is cyclic and we are done.

In the sequel, assume $H \neq \{1\}$. Then $H$ contains positive powers of $x$, since if $x^k \in H$, then $x^{-k} \in H$ for $k \in \mathbb{Z}$.

Choose

$$n = \min\{k \in \mathbb{N}^* \mid x^k \in H\}\,.$$

We will prove that $H =< x^n >$.

Since $x^n \in H$, it follows that $< x^n > \subseteq H$. Conversely, let $x^m \in H$ for some $m \in \mathbb{Z}$. Then by the Division Algorithm, there exist unique $q, r \in \mathbb{Z}$ such that

$$m = nq + r\,, \quad 0 \leq r < n\,.$$

Then

$$x^r = x^{m-nq} = x^m \cdot (x^n)^{-q}\,.$$

But since $x^m$, $x^n \in H$, we have $x^r \in H$. By the choice of $n$, it follows that $r = 0$, so that

$$x^m = (x^n)^q \in < x^n > \ .$$

Hence $H \subseteq < x^n >$ and consequently $H =< x^n >$.

Therefore, $H$ is cyclic. □

We have seen that a cyclic group may have more than one generator. For instance, $(\mathbb{Z}, +)$ is generated by 1, but also by $-1$. We might wonder how could we obtain all the generators of a cyclic group. We are able to give the following result for finite cyclic groups.

**Theorem 1.6.12** *Let $(G, \cdot)$ be a finite cyclic group, say $G =< x >$ and $|G| = n$, and let $k \in \mathbb{N}^*$. Then:*

$$G =< x^k > \iff (n, k) = 1\,.$$

*Proof.* Notice that $\operatorname{ord} x = n$, hence $x^n = 1$.

$\Longrightarrow$. Assume that $G =< x >=< x^k >$. Suppose further that $(n, k) = d \neq 1$. Then $n = dn'$ and $k = dk'$ for some $n', k' \in \mathbb{N}$, where $n' < n$ and $k' < k$. It follows that

$$(x^k)^{n'} = (x^{dk'})^{n'} = (x^{dn'})^{k'} = (x^n)^{k'} = 1\,,$$

hence $\operatorname{ord} x^k \leq n' < n = \operatorname{ord} x$. Then $| < x^k > | \neq | < x > |$, which is a contradiction. Therefore, $(n, k) = 1$.

$\Longleftarrow$. Assume that $(n, k) = 1$. Then $\exists u, v \in \mathbb{Z}$ such that $un + vk = 1$. Then

$$x = x^{un+vk} = (x^n)^u \cdot (x^k)^v = (x^k)^v\,,$$

hence $x \in < x^k >$, so that $G =< x > \subseteq < x^k >$. Obviously, we have $< x^k > \subseteq < x >= G$. Therefore, $G =< x^k >$. □

**Example 1.6.13** $(a)$ Consider the group $(U_8, \cdot)$ of the 8-th roots of unity. Then

$$U_8 = \{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_7\}\,,$$

where

$$\varepsilon_k = (\varepsilon_1)^k = \Big(\cos\frac{2\pi}{8} + i \sin\frac{2\pi}{8}\Big)^k\,, \quad k = 0, 1, \ldots, 7\,.$$

By applying Theorem 1.6.12, we get all the generators of $U_8$, namely $\varepsilon_1$, $\varepsilon_3 = \varepsilon_1^3$, $\varepsilon_5 = \varepsilon_1^5$ and $\varepsilon_7 = \varepsilon_1^7$.

The generators of $(U_n, \cdot)$ are called *primitive roots* of unity. Hence $\varepsilon_1$, $\varepsilon_3$, $\varepsilon_5$ and $\varepsilon_7$ are the primitive roots of unity in $(U_8, \cdot)$.

$(b)$ Consider the group $(\mathbb{Z}_{12}, +)$ of residue classes modulo 12. By applying Theorem 1.6.12, we get all the generators of $\mathbb{Z}_{12}$, namely $\widehat{1}$, $\widehat{5}$, $\widehat{7}$, $\widehat{11}$.

We end the present section with the following extremely important results, telling us that there exist only two cyclic groups up to an isomorphism.

**Theorem 1.6.14** *(i) Any two finite cyclic groups having the same order are isomorphic.*

*(ii) Any two infinite cyclic groups are isomorphic.*

*Proof.* Let $(G,\cdot)$, $(G',\cdot)$ be cyclic groups, say $G =< x >$ and $G' =< y >$.

$(i)$ Suppose first that $G$ and $G'$ are finite, say $|G| = |G'| = n$. Then

$$G = \{1, x, x^2, \ldots, x^{n-1}\}$$

and

$$G' = \{1', y, y^2, \ldots, y^{n-1}\}.$$

Define

$$f : G \to G' \text{ by } f(x^k) = y^k, \quad \forall k \in \{0, \ldots, n-1\}.$$

Then by Theorem 1.6.10, $f$ is injective, hence bijective. Moreover, $f$ is a group homomorphism, since $\forall i, j \in \{0, 1, \ldots, n-1\}$ we have

$$f(x^i \cdot x^j) = f(x^{i+j}) = y^{i+j} = y^i \cdot y^j = f(x^i) \cdot f(x^j).$$

$(ii)$ Suppose now that $G$ and $G'$ are infinite. Define

$$f : G \to G' \text{ by } f(x^k) = y^k, \quad \forall k \in \mathbb{Z}$$

and use the same arguments as for the finite case. □

**Corollary 1.6.15** *Let $(G,\cdot)$ be a cyclic group.*

*(i) If $G$ is finite and $|G| = n$, then*

$$(G,\cdot) \simeq (\mathbb{Z}_n, +).$$

*(ii) If $G$ is infinite, then*

$$(G,\cdot) \simeq (\mathbb{Z}, +).$$

**Remark 1.6.16** Therefore, Corollary 1.6.15 tells us that there exist, up to an isomorphism, only two types of cyclic groups, namely $(\mathbb{Z}_n, +)$ and $(\mathbb{Z}, +)$.