3.3.3 Subgroup Generated by an Element, Order of an Element. Let $(G, \circ, e)$ be a finite group, choose an element $a \in G$. Consider the set of all powers of a:

$$\{a, a^2, a^3, \ldots, a^k, \ldots\}.$$

Since G is a finite set, there must exist i and j, $i \neq j$, such that $a^i = a^j$. Let us assume that i is the exponent which is smaller than j. We are in a group, so there exists a^{-1}. Therefore

$$a^i = a^j \text{ implies } a^{i-1} = a^{j-1}, \text{ etc. } e = a^0 = a^{j-i}.$$

Hence, we have proved the first part of the following proposition:

Proposition. Let $(G, \circ, e)$ be a finite group, $a \in G$. Then there exists the smallest positive integer r for which $a^r = e$. Moreover, $\{a, a^2, \ldots, a^r\}$ forms a subgroup of $(G, \circ, e)$. □

Justification. The second part follows from the fact that

1. $a^i \circ a^j = a^{i+j} = a^k$ where $k \equiv i + j \bmod r$.
2. $a^r = e \in \{a, a^2, \ldots, a^r\}$.
3. $(a^i)^{-1} = a^{r-i}$.

Definition. The subgroup formed by $\{a, a^2, \ldots, a^r\}$ is called the *subgroup generated by a* and will be denoted by $\langle a \rangle$.

The number of elements of $\langle a \rangle$ (i.e. the smallest positive r for which $a^r = e$) is called the *order of a* and it is denoted by $r(a)$. □

Note that the order of a is in fact the order of the subgroup $\langle a \rangle$.

3.3.4 The fact that $\langle a \rangle$ forms a subgroup of $(G, \circ, e)$ gives us

Corollary. Given a finite group $(G, \circ, n)$ with n elements. Then the order of any element $a \in G$ divides n.

This proposition is a direct consequence of 3.3.1. Indeed, $\langle a \rangle$ is a subgroup of the group $(G, \cdot, e)$ having $r(a)$ elements.

3.3.5 Theorem. Given a finite group $(G, \circ, e)$ with n elements. Then for every $a \in G$ we have

$$a^n = e.$$

Justification. Indeed, since $r(a)$ divides n, we get

$$a^n = a^{k\, r(a)} = (a^{r(a)})^k = e^k = e.$$

□

3.3.6 A Characterization of the Order r(a). The following proposition will help us for example to find the order of of powers of a given element (see **??**) of a finite group.

Proposition. A number r equals to the order $r(a)$ of a in a finite group $(G, \cdot, e)$ if and only if the following two conditions are satisfied:

1) $a^r = e$.
2) If $a^s = e$ for some natural number s then r divides s.

□

Justification. a) Let us assume that r satisfies the two conditions above. Then clearly, r is the smallest positive integer for which $a^r = e$; hence $r = r(a)$.

b) Denote the order $r(a)$ by r. We show that r satisfies the two conditions above. The first condition is obvious. Consider any s for which $a^s = e$. Divide s by r, we get $s = qr + z$ where the remainder z satisfies $0 \leq z < r$. Then

$$e = a^s = a^{qr+z} = (a^r)^q \cdot a^z = e^q \cdot a^z = a^z.$$

Since z is strictly smaller than r, and r is the smallest positive number for which $a^i = e$, we get $z = 0$. And hence r divides s. □

3.3.7 Cyclic Group, a Generating Element of a Group. There is a special type of groups, in fact the "most simple" ones, where the calculation corresponds to the addition in $\mathbb{Z}_r$. More precisely:

Definition. Given a group $\mathcal{G} = (G, \circ, e)$. If there exists an element $a \in G$ for which $\langle a \rangle = G$ we say that the group is *cyclic* and that a is a generating element of $(G, \circ, e)$. □

Remark. Note that a cyclic group does not need to be finite. Even in an infinite group $(G, \circ, e)$ we can form a subgroup generated by $a \in G$, indeed,

$$\langle a \rangle = \{\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots\} = \{a^i \mid i \in \mathbb{Z}\}.$$

If $\langle a \rangle = G$ then the group is cyclic.

3.3.8 Examples.

1. $(\mathbb{Z}_n, +, 0)$ (for any natural number $n > 1$) is a cyclic group with its generating element 1.
2. For every prime number p the group $(\mathbb{Z}_p^\star, \cdot, 1)$ is a cyclic group. It is not straightforward to show it. Moreover, to find a generating element is a difficult task for some primes p.
3. The group $(\mathbb{Z}_8^\star, \cdot, 1)$ **is not** cyclic. We have $\mathbb{Z}_8^\star = \{1, 3, 5, 7\}$ and $3^2 = 1$, $5^2 = 1$ and $7^{-1} = 1$. So, there is no element with order 4.
4. $(\mathbb{Z}, +, 0)$ of all integers together with addition is a cyclic group; its generating element is 1.

3.3.9 Observation. One can reformulate the definition of a finite cyclic group: A finite group $\mathcal{G} = (G, \circ, e)$ of order n is cyclic if and only if there exists $a \in G$ with its order $r(a) = n$.

3.3.10 Order of a Power of a. If we know the order of an element of a in a finite group $(G, \circ, e)$ then we can determine the order of a^i for any $i \in \mathbb{N}$, see the following proposition.

Proposition. Let $\mathcal{G} = (G, \circ, e)$ be a finite group. Let $a \in G$ have order $r(a)$. Then

$$r(a^i) = \frac{r(a)}{\gcd(r(a), i)}.$$

□

Justification. We will show that the number $\frac{r(a)}{\gcd(r(a),i)}$ satisfies the conditions of proposition 3.3.9 and hence it is $r(a^i)$.

Denote $r = r(a)$, and $d = \gcd(i, r)$. Then we can write $i = d\,i'$ and $r = d\,r'$ where i' and r' are relatively prime. With this notation $\frac{r(a)}{\gcd(r(a),i)}$ equals to r'.

We show the first condition from 3.3.6: we have

$$(a^i)^{r'} = a^{i\,r'} = a^{i'\,d\,r'} = (a^{d\,r'})^{i'} = (a^r)^{i'} = e.$$

The second condition from 3.3.6: Assume that $(a^i)^s = a$. Then $a^{i\,s} = e$. Since r is the order of a, necessarily r divides $i\,s$. Further

$$i\,s = k\,r, \text{ i.e. } i'\,d\,s = k\,r'\,d \text{ and } i'\,s = k\,r'.$$

Numbers i' and r' are relatively prime, and r' divides $i'\,s$, hence r' divides s. So r' is the order of a^i as required. □

3.3.11 Observation. The proposition above helps to find orders of all elements b belonging to $\langle a \rangle$. Indeed, we know that the subgroup $\langle a \rangle$ is a cyclic group having a as its generating element. So we can use the proposition from 3.3.9 for every element $b \in \langle a \rangle$. Especially, if we know a generating element of a cyclic group we can find orders of all elements of the group.

3.3.12 The proposition in 3.3.9 can be used to calculate the number of generating elements in any finite cyclic group. Indeed, if a is a generating element of a finite cyclic group $\mathcal{G} = (G, \circ, e)$ with n elements, then $b = a^i$ is also a generating element of $\mathcal{G}$ if and only if $\gcd(i, n) = 1$; and there are $\phi(n)$ such i's. Hence we get the following corollary

Corollary. Given a finite cyclic group $\mathcal{G} = (G, \circ, e)$ with n elements. Then $\mathcal{G}$ has $\phi(n)$ different generating elements. □

3.3.13 Subgroups of a Finite Cyclic Group. Subgroups of a finite cyclic group are easy to describe. The next proposition states that a finite cyclic group with n elements has a subgroup of order d for any divisor d of n. Notice, that it is not true for a finite group which is not cyclic.

Proposition. Given a finite cyclic group $\mathcal{G} = (G, \circ, e)$ with n elements. Then for every natural number d which divides n there exists a subgroup of $\mathcal{G}$ with d elements. □

Justification. Denote by a one of generating elements of the group $\mathcal{G}$. Then the subgroup $\langle a^k \rangle$ where $k = \frac{n}{d}$ had d elements. Indeed, we have

$$\langle a^k \rangle = \{a^k, a^{2k}, \dots, a^{dk} = e\}.$$

3.3.14 Remark. A finite cyclic group has only subgroups that itself are cyclic.

Justification. Let $\mathcal{G} = (G, \circ, e)$ be a finite cyclic group with a generating element a. Consider two elements $b, c \in G$; then $b = a^i$ and $c = a^j$ for some $i, j \in \{1, 2, \dots, |G|\}$. Any subgroup which contains these two elements must contain also all elements of the form a^{ix+jy} where x and y are any integers. From the Bezout's Theorem we know that the equation $ix + jy = k$ has integer solutions if and only if the greatest common divisor of i and j divides k. Therefore the smallest subgroup containing $b = a^i$ and $c = a^j$ is $\langle a^d \rangle$ where $d = \gcd(i, j)$.