5.1.19 The Group of Invertible Elements. Every monoid contains a special submonoid, the one formed by all invertible elements. And this submonoid is in fact a group that is called the *group of invertible elements*. Let us first prove the following proposition which justifies the definition coming next.

Proposition. Given a monoid $(S, \circ, e)$. Denote by $S^\star$ the set of all its invertible elements. Then $(S^\star, \circ, e)$ is a submonoid of $(S, \circ)$ which is a group. □

Justification. The above proposition immediately follows from 5.1.9. Indeed, $e \in S^\star$, and if $a, b \in S^\star$ then $a \circ b \in S^\star$. So $S^\star$ forms a submonoid.

Moreover, $(S^\star, \circ, e)$ is a group because if $a \in S^\star$ then $a^{-1} \in S^\star$. □

Definition. The group $(S^\star, \circ, e)$ is called the *group of invertible elements* of the monoid S. □

5.1.20 The following theorem is an important fact and is used in a lot of applications. In fact it holds for any finite group but we will state and prove it only for commutative ones now.

Theorem. Let $(G, \circ, e)$ be a finite commutative group. Then for every $a \in G$ we have $a^{|G|} = e$. □

Justification. Assume that the group has n elements and denote $G = \{a_1, a_2, \ldots, a_n\}$. Take any $a \in G$ and form the set $H = \{a \circ a_1, a \circ a_2, \ldots, a \circ a_n\}$. The H has also n elements; indeed, if $a \circ a_i = a \circ a_j$ in a group then $a_i = a_j$ (see 5.1.10).

Therefore, $G = H$ and because G is a commutative group we have

$$a_1 \circ a_2 \circ \ldots \circ a_n = (a \circ a_1) \circ (a \circ a_2) \circ \ldots \circ (a \circ a_n),$$

and also

$$a_1 \circ a_2 \circ \ldots \circ a_n = a^n \circ (a_1 \circ a_2 \circ \ldots \circ a_n).$$

If we multiply the last equality by $(a_1 \circ a_2 \circ \ldots \circ a_n)^{-1}$ we get $a^n = e$. □

5.2 Applications to $(\mathbb{Z}_n, \cdot, 1)$

Let us first introduce the *Euler function*.

5.2.1 Euler function. Given a natural number $n > 1$. Then the value of Euler function $\phi(n)$ equals to the number of all natural numbers i, $0 \leq i < n$, that are relatively prime to n. □

For example $\phi(6) = 2$, since there are only two natural numbers between 0 and 5 that are relatively prime to 6, namely 1 and 5.

5.2.2 Properties of Euler Function.

1. Let p be a prime number, then $\phi(p) = p - 1$.
2. If p is a prime number and $k \geq 1$ then $\phi(n) = p^k - p^{k-1}$.
3. If n and m are relatively prime natural numbers then $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$.

□

It is not difficult to show the first two properties above. The easiest way how to prove the last one is to use the Chinese Remainder Theorem which is beyond the scope of this course.

5.2.3 The Group of Invertible Elements of $(\mathbb{Z}_n, \cdot, 1)$. We will use the facts from 5.1.19 for the commutative monoid $(\mathbb{Z}_n, \cdot, 1)$. We know $(\mathbb{Z}_n, \cdot)$ is a monoid with its neutral element 1. The set of all invertible elements of it is

$$\mathbb{Z}_n^\star = \{i \,|\, 0 \leq i < n, \;\; i \text{ and } n \text{ are relatively prime}\}.$$

Therefore, $(\mathbb{Z}_n^\star, \cdot, 1)$ is a group with $\phi(n)$ elements where $\phi(n)$ is the Euler function of n.

5.2.4 Euler-Fermat Theorem. Applying 5.1.20 we get a theorem which generalizes of the small Fermat theorem:

Theorem (Euler-Fermat). Given a natural number $n > 1$. Then for every integer a relatively prime to n we have

$$a^{\phi(n)} \equiv 1 \,(\mathrm{mod}\, n).$$

□

Justification. Indeed, take any integer a relatively prime to n. Put b to be the remainder when we divide a by n. Then $b \in \mathbb{Z}_n^\star$. Since $(\mathbb{Z}_n^\star, \cdot, 1)$ is a finite group with $\phi(n)$ elements, the Euler-Fermat Theorem is a consequence of 5.1.20. □

Remark. The small Fermat theorem is an immediate consequence of the Euler-Fermat theorem. Indeed, if n is a prime number then $\phi(n) = n - 1$.

5.3 Subgroups

Analogously as we defined subsemigroups and submonoids we can define subgroups. Subgroups are formed by subsets that not only form itself a group but group with the original operations. More precisely:

Definition. Given a group $(G, \circ, e)$. We say that $H \subseteq G$ forms a *subgroup* of $(G, \circ, e)$ if

1. for every $x, y \in H$ it holds that $x \circ y \in H$, (i.e. forms a subsemigroup);
2. $e \in H$, (i.e. forms a submonoid);
3. for every $x \in H$ it holds that $x^{-1} \in H$.

□

Note, that in this case, $(H, \circ, e)$ is also a group.

Remark. Every group $(G, \circ, e)$ with more than one element has at least two subgroups; indeed, one formed by $\{e\}$ and second formed by G. These two subgroups are called *trivial subgroups*.

5.3.1 How Many Elements a Subgroup Can Have? We will show some useful properties of finite groups and their subgroups. The first theorem shows that a subset of a group can form a subgroup only if its number of elements divides the number of elements of the group. Hence, $(\mathbb{Z}_7, +, 0)$ has only trivial subgroups; indeed, 7 is a prime number with divisors 1 and 7. And any subgroup with 1 element consists of 0, a subgroup with 7 elements is $(\mathbb{Z}_7, +, 0)$.

Theorem. Let $(G, \circ, e)$ be a finite group and $H \subseteq G$ its subgroup. Then the number of elements of H divides the number of elements of G. □

Justification. Let us denote $n = |G|$ and $k = |H|$. For every $g \in G$ we form a subset of G: $g \circ H = \{g \circ x \,|\, x \in H\}$.

We show that for every $g_1, g_2 \in G$ the sets $g_1 \circ H$ and $g_2 \circ H$ are either the same or they are disjoint (they do not have a common element).

Assume that $(g_1 \circ H) \cap (g_2 \circ H) \neq \emptyset$. Then there exist $h_1, h_2 \in H$ such that $g_1 \circ h_1 = g_2 \circ h_2$. Since we are in a group, we have

$$g_1 = (g_2 \circ h_2) \circ h_1^{-1} = g_2 \circ (h_2 \circ h_1^{-1}) \;\text{ and }\; g_2 = (g_1 \circ h_1) \circ h_2^{-1} = g_1 \circ (h_1 \circ h_2^{-1}). \qquad (5.5)$$

This means that $g_1 \in g_2 \circ H$ and $q_2 \in g_1 \circ H$, (indeed, H is a subgroup so $h_2 \circ h_1^{-1}, h_1 \circ h_2^{-1} \in H$).

Now, take an arbitrary element $x \in g_1 \circ H$. Then $x = g_1 \circ h$ for some $h \in H$. Substituting form 5.5 we get

$$x = (g_2 \circ (h_2 \circ h_1^{-1})) \circ h = g_2 \circ (h_2 \circ h_1^{-1} \circ h) \;\text{ and so }\; x \in g_2 \circ H.$$

Indeed, H is a subgroup so $h_2 \circ h_1 \circ h$ belongs to H.

Similarly, one gets that any $z \in g_2 \circ H$ belongs to $g_1 \circ H$. So, we have shown that $g_1 \circ H = g_2 \circ H$.

H is a subgroup, so $e \in H$, and therefore $g \in g \circ H$ for every $g \in G$. This means that every element from G belongs to some $g' \circ H$. Hence, the system $\{g \circ H \,|\, g \in G\}$ forms a partition of G.

To finish the argument, we show that all sets $g \circ H$ have the same number of elements which is $k = |H|$. Denote $H = \{h_1, \ldots, h_k\}$. Then

$$g \circ H = \{g \circ h_1, \ldots, g \circ h_k\}.$$

If $g \circ h_i = g \circ h_j$ then $(g^{-1} \circ g) \circ h_i = (g^{-1} \circ g) \circ h_2$, which means that $h_i = h_j$ (see also 5.1.10).

We have shown that the set of n elements is divided into disjoint parts each of them having k elements. Hence n is divisible by k. (Note that there are n/k distinct sets $g \circ H$.) □

5.3.2 Order of a Finite Group. The number of elements of a finite group $(G, \circ, e)$ is often called its *order*. The above theorem can be formulated as follows: The order of any subgroup $(H, \circ, e)$ of a finite group $(G, \circ, e)$ divides the order of $(G, \circ, e)$.

5.3.3 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 $\langle a \rangle$.

5.3.4 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 5.3.1. Indeed, $\langle a \rangle$ is a subgroup of the group $(G, \cdot, e)$ having $r(a)$ elements.

5.3.5 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

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

□

5.3.6 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. □

5.3.7 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,

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

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

5.3.8 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.

5.3.9 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 $r(a) = n$.

5.3.10 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 5.3.9 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 5.3.6: we have

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

The second condition from 5.3.6: 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. □

5.3.11 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 5.3.9 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.

5.3.12 The proposition in 5.3.9 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. □

5.3.13 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 generati+ng elements of the group $\mathcal{G}$. Then the subgroup $\langle a^k \rangle$ where $k = \frac{n}{d}$ had d elements. Indeed, we have

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

5.3.14 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 $i, j \in \{1, 2, \ldots, |G|\}$. 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 $d = \gcd(i, j)$.