27. Cyclic groups

27.1. Definition

A group $\mathfrak{G}$ is called *cyclic* if it contains an element a, called *generator of* $\mathfrak{G}$, such that each element of $\mathfrak{G}$ is a power of a. If $\mathfrak{G}$ is a cyclic group and a its generator, then $\mathfrak{G}$ is denoted by the symbol (a). From the first formula (1) in 19.3 it follows that *every cyclic group is Abelian.*

27.2. The order of a cyclic group

Consider a cyclic group (a). If the powers a^i, a^j of a with any two different exponents i, j are different, then the group (a) has the order 0 because it contains an infinite number of elements

$$\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots \tag{1}$$

As each element of (a) is a power of a, the group (a) does not include any other elements but these so that (a) consists of the elements (1). Now suppose that the powers of a with some different exponents i, j are equal and so $a^i = a^j$, $i \neq j$. Hence $a^{-j} \,.\, a^i = a^{-j} \,.\, a^j$, i.e., $a^{i-j} = \underline{1}$. Since one of the numbers $i - j$, $j - i$ is positive and the powers of a with these exponents equal $\underline{1}$, we observe that there exist positive integers x satisfying the equation $a^x = \underline{1}$. One of them is the least; let us denote it n, thus $a^n = \underline{1}$. Now consider the following elements of (a):

$$\underline{1}, a, a^2, \ldots, a^{n-1}. \tag{2}$$

First, it is easy to verify that every two of them are different: in fact, if for any of them there holds $a^i = a^j$, then one of the numbers $i - j$, $j - i$ is a positive integer smaller than n and satisfies the equation $a^x = \underline{1}$; but that contradicts the definition of n. Consequently, the group (a) comprises at least n elements (2) and has therefore the order 0 or $\geqq n$. Moreover, it is easy to show that (a) does not include any other elements, hence its order is n. To that purpose, consider an element a^x of (a). Dividing x by n, we obtain a quotient q and a remainder r whence $x = qn + r$, $0 \leqq r \leqq n - 1$; consequently, a^r is one of the elements (2). The formulae (1) in 19.3 yield

$$a^x = a^{qn+r} = a^{qn} \,.\, a^r = (a^n)^q \,.\, a^r = \underline{1}^q \,.\, a^r = \underline{1} \,.\, a^r = a^r$$

and we have $a^x = a^r$. Thus we have verified that the group (a) consists of the elements (2) and therefore has the order n. Furthermore, the product $a^i \,.\, a^j$ of an element a^i and an element a^j of (a) is the element a^k, k being the remainder of the division of $i + j$ by n because $a^i \cdot a^j = a^{i+j}$. To sum up, we arrive at the following theorem:

The order n of every cyclic group (a) is either 0, in which case (a) consists of the elements (1), or $n > 0$, and then (a) consists of the elements (2). The product $a^i \cdot a^j$ of the elements a^i and a^j of (a) is, in the first case, the element a^{i+j} whereas, in the second case, it is a^k, k being the remainder of the division of $i + j$ by n. In the latter, n is the least positive integer such that $a^n = \underline{1}$.

Note that in both cases a^{n-i} is the inverse of a^i.

27.3. Subgroups of cyclic groups

Let us now consider a subgroup $\mathfrak{A}$ of a cyclic group (a). If $\mathfrak{A}$ consists of a single element $\underline{1}$, then it is cyclic and its generator is $\underline{1}$. Suppose that $\mathfrak{A}$ contains besides $\underline{1}$ an element a^i where $i \neq 0$. As $\mathfrak{A}$ comprises with a^i simultaneously its inverse a^{-i} and as one of the numbers i, $-i$ is positive, we see that $\mathfrak{A}$ includes powers of a with positive exponents. One of the latter is the least; let us denote it m, hence $a^m \in \mathfrak{A}$. $\mathfrak{A}$ does not contain any powers of a with positive exponents smaller than m. Let a^x be an arbitrary element of $\mathfrak{A}$. Dividing x by m, we obtain a quotient q and a remainder r, hence $x = qm + r$, $0 \leqq r \leqq m - 1$. In accordance with the formulae (1) in 19.3, there follows: $a^x = a^{qm+r} = a^{qm} \cdot a^r$. Consequently, a^r is the product of a^{-qm} and a^x. Since a^{-qm} is the inverse of the element $(a^m)^q$ which is, as the q^{th} power of the element $a^m \in \mathfrak{A}$, also included in $\mathfrak{A}$, we see that a^{-qm} is an element of $\mathfrak{A}$. As even a^x is an element of $\mathfrak{A}$, the product $q^{-qm} \cdot a^x$, namely, the element a^r is included in $\mathfrak{A}$. Consequently, with regard to the inequalities $0 \leqq r \leqq m - 1$ and to the definition of m, there follows $r = 0$. So we have $a^x = (a^m)^q$. Every element of $\mathfrak{A}$ is therefore a power of a^m, hence $\mathfrak{A}$ is cyclic with the generator a^m. Thus we have arrived at the result that *every subgroup of a cyclic group (a) is cyclic.*

Since the cyclic group (a) is Abelian, each of its subgroups is invariant in (a).

27.4. Generators

Do there exist, in the cyclic group (a), any other generators besides a? Let, again, n denote the order of (a) and suppose that some element a^ν of (a) is a generator of (a). Then, in particular, the element a is a power of a^ν, hence $a = a^{\nu q}$, q being an integer. If $n = 0$, then $a = a^{\nu q}$ yields $\nu q = 1$ because, in that case, any two powers of a with different exponents are different; hence $\nu = q = 1$ or $\nu = q = -1$. Consequently, besides a, only a^{-1} can be a generator of (a) and, in fact, each element a^i of (a) is the $-i^{\text{th}}$ power of a^{-1}.

If $n = 0$, then the group (a) has exactly two generators: a, a^{-1}. Note that they are the only two elements of (a) whose exponents are relatively prime to n ($= 0$).

Let us now consider the case when $n > 0$. The cyclic group (a) consists of the elements $\underline{1}, a, a^2, \ldots, a^{n-1}$. If r is the remainder of the division of νq by n so that $\nu q = nq' + r$ where q' is the quotient and $0 \leqq r \leqq n - 1$, then we have $a^{\nu q} = a^r = a$. Consequently, $r = 1$ because a, a^r belong to the sequence $\underline{1}, a, a^2, \ldots, a^{n-1}$ where any two elements with different exponents are different. So we have $\nu q - nq' = 1$ and therefore ν, n are prime to each other. If, conversely, ν is an integer relatively prime to n, then there exist integers q, q' such that $\nu q - nq' = 1$ and there follows, for every integer i, the relation $i = \nu(qi) - n(q'i)$. Consequently, we have $a^i = (a^\nu)^{qi}$ and so a^ν is a generator of the group (a). If $n > 0$, then the generators of (a) are the powers of a whose exponents are relatively prime to n. We saw that the same applies even if $n = 0$ and can therefore sum up the above results in the following theorem:

The generators of the cyclic group (a) of order $n \geqq 0$ are exactly the powers of a with exponents relatively prime to n.

If $n = 0$, then (a) has precisely two generators whereas, if $n > 0$, then the number of the generators equals the number of the positive integers not greater than n and relatively prime to it.

27.5. Determination of all cyclic groups

1. An important example of a cyclic group of order 0 is the group $\mathfrak{Z}$. Evidently, $\mathfrak{Z} = (1)$. All subgroups of $\mathfrak{Z}$ consist, as we know, of all multiples of a non-negative integer n, hence they are cyclic groups (n). Let $n \geqq 0$ and consider the factor group $\mathfrak{Z}/(n)$. We know that, for $n = 0$, $\mathfrak{Z}/(n)$ consists of the sets $\bar{a}_i = \{i\}$ where $i = \ldots, -2, -1, 0, 1, 2, \ldots$, and, for $n > 0$, it consists of the elements $\bar{a}_0, \ldots, \bar{a}_{n-1}$ where $\bar{a}_j$ denotes the set of all the elements of $\mathfrak{Z}$ that differ from j only by a multiple of n; the factor group $\mathfrak{Z}/(n)$ has, in both cases, the order n. It is easy to show that the factor group $\mathfrak{Z}/(n)$ is cyclic with the generator $\bar{a}_1$. In fact, by the definition of the multiplication in $\mathfrak{Z}/(n)$, any i^{th} power of an element $\bar{a}_k \in \mathfrak{Z}/(n)$ is that element of $\mathfrak{Z}/(n)$ which contains the number ik; hence, in particular, $\bar{a}_j = \bar{a}_1{}^j$, which proves the above assertion. Thus we have simultaneously verified that there exist cyclic groups of an arbitrary order $n \geqq 0$.

Now we shall show that, conversely, every cyclic group is isomorphic with a factor group of $\mathfrak{Z}$. Consider a cyclic group (a). To each element $x \in (a)$ there exists at least one integer ξ such that $a^\xi = x$ and, of course, vice versa, for every integer ξ, a^ξ is an element of (a). Associating with each element $\xi \in \mathfrak{Z}$ the element $a^\xi \in (a)$, we obtain a mapping $\boldsymbol{d}$ of $\mathfrak{Z}$ onto (a). If ξ and η are arbitrary elements of $\mathfrak{Z}$ and $\boldsymbol{d}\xi = x$, $\boldsymbol{d}\eta = y$, then we have $x = a^\xi$, $y = a^\eta$ and therefore $xy = a^\xi a^\eta = a^{\xi+\eta}$, hence $\boldsymbol{d}(\xi + \eta) = xy = \boldsymbol{d}\xi\boldsymbol{d}\eta$. Consequently, the mapping $\boldsymbol{d}$ preserves the multiplications in both groups $\mathfrak{Z}$, (a) and therefore is a homomorphism. We observe, first, that (a) is homomorphic with $\mathfrak{Z}$. By the first isomorphism theorem for groups (26.3.1), the set of all $\boldsymbol{d}$-inverse images of the unit of (a) is an invariant subgroup $\mathfrak{A}$ of $\mathfrak{Z}$ and the factor group on $\mathfrak{Z}$, generated by $\mathfrak{A}$, is isomorphic with (a), i. e., $\mathfrak{Z}/\mathfrak{A} \simeq (a)$. Let n ($\geqq 0$) be the order of the cyclic group (a). Then even $\mathfrak{Z}/\mathfrak{A}$ has the order n and so $\mathfrak{A}$ consists of all multiples of n. Consequently, the cyclic group (a) of order n is isomorphic with the factor group $\mathfrak{Z}/(n)$ generated by the subgroup (n) of $\mathfrak{Z}$. In particular, every cyclic group of order 0 is isomorphic with $\mathfrak{Z}/(0)$, hence even with $\mathfrak{Z}$.

It is easy to see that any group isomorphic with a cyclic group of order n ($\geqq 0$) is also cyclic and of order n.

The result:

All cyclic groups of order $n \geqq 0$ are represented by the factor group $\mathfrak{Z}/(n)$ on $\mathfrak{Z}$ in the sense that any cyclic group of order n is isomorphic with $\mathfrak{Z}/(n)$ and, conversely, any group isomorphic with $\mathfrak{Z}/(n)$ is cyclic and of order n.

2. Example. As an example of a cyclic group of order $n > 0$ we may introduce the group consisting of the n^{th} roots of unity with multiplication in the arithmetic sense.

The roots in question are:

$$\varepsilon_0 = 1, \quad \varepsilon_1 = e^{2\pi i/n}, \quad \varepsilon_2 = e^{4\pi i/n}, \ldots, \varepsilon_{n-1} = e^{2(n-1)\pi i/n}$$

and therefore form the cyclic group $(e^{2\pi i/n})$. The points whose coordinates are real and imaginary parts of these roots are the vertices of a regular n-gon. For $n = 6$, for example, we have the vertices of a regular hexagon. The generators of this group of order 6 are $e^{2\pi i/6}$, $e^{10\pi i/6}$.

27.6. Fermat's theorem for groups

The notion of a cyclic group is important even for groups that are not necessarily cyclic. Consider a group $\mathfrak{G}$. Let a be an arbitrary element of $\mathfrak{G}$. The individual powers of a form a cyclic subgroup (a) of $\mathfrak{G}$.

By the *order of the element a* we mean the order of the cyclic subgroup (a). The order n of a is therefore either 0 or the least positive integer x for which $a^x = \underline{1}$; in any case there holds $a^n = \underline{1}$.

Furthermore, it is easy to verify that the order n of each element $a \in \mathfrak{G}$ is a divisor of the order N of $\mathfrak{G}$, i.e., $N = nd$, d integer. For $N = 0$ this statement is obvious. In case of $N > 0$ it is true because the order of any subgroup of $\mathfrak{G}$ is a divisor of the order of $\mathfrak{G}$. From the equality $N = nd$ there follows: $a^N = a^{nd} = (a^n)^d = \underline{1}^d = \underline{1}$. Thus we have arrived at *Fermat's theorem for groups*:

The N^{th} power of any element of a group of order N is the unit of the group.

27.7. The generating of translations on finite groups by pure cyclic permutations

Let us conclude our study with a remark concerning the generating of, for example, the left translations of a finite group by pure cyclic permutations.

Assume $\mathfrak{G}$ to be a finite group and a an element of $\mathfrak{G}$. As we saw in 26.2.1, the left translation $_a\boldsymbol{t}$ of $\mathfrak{G}$ is a permutation of $\mathfrak{G}$ and is therefore generated by a finite number of pure cyclic permutations; that is to say, there exists a decomposition $\overline{G} = \{\bar{a}, \ldots, \overline{m}\}$ of $\mathfrak{G}$ such that each element $\bar{a}, \ldots, \overline{m}$ is invariant under $_a\boldsymbol{t}$ and the partial permutations $_a\boldsymbol{t}_{\bar{a}}, \ldots, {_a\boldsymbol{t}_{\overline{m}}}$ are pure cyclic permutations of the elements $\bar{a}, \ldots, \overline{m}$. Any element $\bar{x}$ of $\overline{G}$ consists of the elements of the cycle: $x, {_a\boldsymbol{t}x}, ({_a\boldsymbol{t}})^2x, \ldots, ({_a\boldsymbol{t}})^{k-1}x$, with x denoting an arbitrary element of $\bar{x}$ and k being the least positive integer such that $({_a\boldsymbol{t}})^kx = x$. Taking account of the definition of the left translation $_a\boldsymbol{t}$, we have

$$_a\boldsymbol{t}x = ax, \; ({_a\boldsymbol{t}})^2x = a^2x, \ldots, ({_a\boldsymbol{t}})^{k-1}x = a^{k-1}x$$

and from $({_a\boldsymbol{t}})^kx = a^kx = x$ there follows $a^k = \underline{1}$. We observe that the cycle in question is $x, ax, a^2x, \ldots, a^{k-1}x$ and, furthermore, that the set $\{\underline{1}, a, a^2, \ldots, a^{k-1}\}$ is the field of the cyclic subgroup (a) of $\mathfrak{G}$. The element $\bar{x}$ is therefore the right coset of x with respect to (a). Consequently, $\overline{G}$ is the right decomposition of $\mathfrak{G}$ generated by (a).

To sum up:

The cycles of pure cyclic permutations generating a left translation $_a\boldsymbol{t}$ of a finite group $\mathfrak{G}$ consist of the same elements as the right cosets with regard to the cyclic subgroup (a) of $\mathfrak{G}$.

27.8. Exercises

1. An element $a \neq \underline{1}$ of a group $\mathfrak{G}$ has the order 2 if and only if it is inverse of itself.
2. In every finite group of an even order there exist elements of the order 2.
3. If an element a of a group $\mathfrak{G}$ is of the order n, then the order of each element of the cyclic subgroup (a) of $\mathfrak{G}$ is a divisor of n.
4. Every group whose order is a prime number is cyclic.
5. The order of each element $\bar{a}$ of any factor group on a finite group $\mathfrak{G}$ is a divisor of the order of each element of $\mathfrak{G}$ contained in $\bar{a}$. If the order of $\bar{a}$ is a power of a prime number p, then there exists in $\bar{a}$ an element a whose order is also a power of p.