

## §11 Cyclic Groups

Let  $G$  be a group and  $a \in G$ . Consider the set  $\{a^n \in G: n \in \mathbb{Z}\}$  of all integral powers of  $a$ . We designate this subset of  $G$  shortly by  $\langle a \rangle$ . It is not empty and is in fact a subgroup of  $G$ :

(i) if  $a^m, a^n \in \langle a \rangle$ , then  $a^m a^n = a^{m+n} \in \langle a \rangle$ , as  $m+n \in \mathbb{Z}$  when  $m, n \in \mathbb{Z}$ ,

(ii) if  $a^m \in \langle a \rangle$ , then  $(a^m)^{-1} = a^{-m} \in \langle a \rangle$ , as  $-m \in \mathbb{Z}$  when  $m \in \mathbb{Z}$ .

**11.1 Definition:** Let  $G$  be a group and  $a \in G$ . Then  $\langle a \rangle = \{a^n \in G: n \in \mathbb{Z}\}$  is called the *cyclic subgroup of  $G$  generated by  $a$* . If it happens that  $\langle a \rangle = G$ , then  $G$  is called a *cyclic group* and  $a$  is called a *generator of  $G$* .

Any cyclic group is abelian. Indeed, if  $G$  is a cyclic group, generated by  $a$ , then any two elements  $a^m, a^n$  ( $m, n \in \mathbb{Z}$ ) of  $G$  commute:

$$a^m a^n = a^{m+n} = a^{n+m} = a^n a^m.$$

The converse is false. There are abelian groups which are not cyclic. For example, the group  $U$  of Example 9.4(h) is abelian but not cyclic since the cyclic subgroups generated by  $\bar{1}, \bar{3}, \bar{5}, \bar{7}$  are all proper subgroups of  $U$ .

**11.2 Examples: (a)** Consider the subgroup  $\langle i \rangle$  of  $\mathbb{C} \setminus \{0\}$  under multiplication. We have

$$i^0 = 1, i^1 = i, i^2 = -1, i^3 = -i$$

and other powers of  $i$  do not give rise to other complex numbers. To see this, let  $n \in \mathbb{Z}$  and divide  $n$  by 4 to get  $n = 4q + r$ ,  $0 \leq r \leq 3$ ,  $q, r \in \mathbb{Z}$ . Then

$$i^n = i^{4q+r} = i^{4q} i^r = (i^4)^q i^r = 1^q i^r = i^r \in \{1, i, -1, -i\}.$$

Hence  $\langle i \rangle = \{1, i, -1, -i\}$  is a cyclic group of order 4.

**(b)** In §9, Ex.4, the reader proved that  $L = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$  is a group under multiplication (mod 9). Let us find the cyclic subgroup of  $L$  generated by  $\bar{2}$ . We have

$$\bar{2}^0 = \bar{1}, \bar{2}^1 = \bar{2}, \bar{2}^2 = \bar{4}, \bar{2}^3 = \bar{8}, \bar{2}^4 = \bar{7}, \bar{2}^5 = \bar{5},$$

$$L = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\} = \{\bar{2}^n \in L : n = 0, 1, 2, 3, 4, 5\} \subseteq \{\bar{2}^n \in L : n \in \mathbb{Z}\} = \langle \bar{2} \rangle,$$

thus  $L = \langle \bar{2} \rangle$ . So  $L$  is a cyclic group and  $\bar{2}$  is a generator of  $L$ . We see

$$\langle \bar{4} \rangle = \{\bar{1}, \bar{4}, \bar{7}\}, \langle \bar{8} \rangle = \{\bar{1}, \bar{8}\}, \langle \bar{7} \rangle = \{\bar{1}, \bar{7}, \bar{4}\}$$

are proper subgroups of  $L$ . In particular,  $\bar{4}, \bar{7}, \bar{8}$  are not generators of  $L$ . On the other hand,

$$\langle \bar{5} \rangle = \{\bar{1}, \bar{5}, \bar{7}, \bar{8}, \bar{4}, \bar{2}\} = L$$

and  $\bar{5}$  is another generator of  $L$ .

A cyclic group has many generators. The number of generators of a cyclic group will be determined later in this paragraph.

**11.3 Definition:** Let  $G$  be a group and  $a \in G$ . The order  $|\langle a \rangle|$  of the cyclic subgroup of  $G$  generated by  $a$  is called the *order of  $a$*  and is denoted by  $o(a)$ .

Thus  $o(a)$  is either a natural number or  $\infty$ . Of course, if  $G$  is a finite group, then every element  $a$  of  $G$  will have finite order, in fact  $o(a) \mid |G|$  by Lagrange's theorem. An infinite group, on the other hand, has in general, elements of finite order as well as elements of infinite order.

**11.4 Lemma:** *Let  $G$  be a group and  $a \in G$ . Then  $o(a)$  is finite if and only if there is a natural number  $n$  with  $a^n = 1$ . If this is the case, then  $o(a)$  is the smallest natural number  $s$  such that  $a^s = 1$ .*

**Proof:** We put  $A = \{n \in \mathbb{N} : a^n = 1\}$ . The claim is that  $o(a)$  is finite if and only if  $A$  is not empty. First we suppose  $o(a)$  is finite and prove that  $A$  is not empty. If  $o(a)$  is finite, then  $\langle a \rangle$  is a finite subgroup of  $G$  and the infinitely many elements

$$a^1, a^2, a^3, a^4, \dots$$

of  $\langle a \rangle$  cannot be all distinct. So  $a^k = a^m$  for some  $k, m \in \mathbb{N}$  with  $k \neq m$ . Assuming  $k < m$  without loss of generality, we obtain  $a^{m-k} = a^m a^{-k} = a^m (a^k)^{-1} = a^m (a^m)^{-1} = 1$ , so  $m - k \in A$  and  $A \neq \emptyset$ .

Suppose now there are natural numbers  $n$  with  $a^n = 1$ , that is, suppose that  $A \neq \emptyset$ . We prove that  $o(a)$  is finite, and is in fact the smallest natural number in  $A$ . To this end, let  $s$  be the smallest natural number in  $A$ . We show first  $s \leq o(a)$  and then  $o(a) \leq s$ .

Consider the  $s$  elements  $a^0, a^1, a^2, \dots, a^{s-1}$  of  $\langle a \rangle$ . These are all distinct, for if

$$a^i = a^j, i \neq j, 0 \leq i, j \leq s-1$$

say with  $i < j$ , then

$$\begin{aligned} a^{j-i} &= 1, j-i \leq (s-1) - 0, j-i \in \mathbb{N}, \\ j-i &\in A, \quad j-i \leq s-1, \end{aligned}$$

contradicting that  $s$  is the smallest natural number in  $A$ . So there are at least  $s$  distinct elements in  $\langle a \rangle$ . This gives  $s \leq |\langle a \rangle| = o(a)$ .

Next we show that there are at most  $s$  distinct elements in  $\langle a \rangle$ . If  $a^h \in \langle a \rangle$ , where  $h \in \mathbb{Z}$ , we divide  $h$  by  $s$  to get

$$\begin{aligned} h &= qs + r, & q, r &\in \mathbb{Z}, & 0 &\leq r \leq s-1, \\ a^h &= a^{qs+r} = a^{sq}a^r = (a^s)^q a^r = 1^q a^r = a^r, \end{aligned}$$

so

$$\begin{aligned} \langle a \rangle &\subseteq \{a^0, a^1, a^2, \dots, a^{s-1}\}, \\ |\langle a \rangle| &\leq |\{a^0, a^1, a^2, \dots, a^{s-1}\}|, \\ o(a) &\leq s \end{aligned}$$

since the elements  $a^0, a^1, a^2, \dots, a^{s-1}$  are all distinct.

From  $s \leq o(a)$  and  $o(a) \leq s$ , we get  $o(a) = s$ . □

**11.5 Lemma:** *Let  $G$  be a group and  $a \in G$ . Then  $o(a) = \infty$  if and only if powers of  $a$  with distinct exponents are distinct, i.e., if and only if  $a^m \neq a^k$  whenever  $m \neq k$  ( $m, k \in \mathbb{Z}$ ).*

**Proof:** If  $a^m \neq a^k$  whenever  $m \neq k$ , then the infinitely many elements

$$\dots, a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, \dots$$

of  $\langle a \rangle$  are all distinct. So  $\langle a \rangle$  is an infinite group and  $o(a) = \infty$ .

Suppose now the condition in the lemma does not hold. Then there are  $m, k \in \mathbb{Z}$  with  $a^m = a^k$ ,  $m \neq k$ . Assume  $m > k$  without loss of generality. Then  $m - k \in \mathbb{N}$  and  $a^{m-k} = 1$ . There is a natural number  $n$ , namely  $n$

$= m - k$ , with  $a^n = 1$ . Then  $o(a)$  is finite by Lemma 11.4. Hence  $o(a) = \infty$  implies that  $a^m \neq a^k$  whenever  $m \neq k$  ( $m, k \in \mathbb{Z}$ ).  $\square$

**11.6 Lemma:** *Let  $G$  be a group and let  $a \in G$  be of finite order. Let  $n \in \mathbb{Z}$ . Then  $a^n = 1$  if and only if  $o(a) | n$ .*

**Proof:** We put  $s = o(a)$ . If  $s | n$ , then  $n = sq$  for some  $q \in \mathbb{Z}$ , hence  $a^n = a^{sq} = (a^s)^q = 1^q = 1$  since  $a^s = 1$  by Lemma 11.4. Conversely, suppose  $a^n = 1$ . We divide  $n$  by  $s$  and get

$$n = qs + r, \quad q, r \in \mathbb{Z}, \quad 0 \leq r < s,$$

$$1 = a^n = a^{qs+r} = a^{sq}a^r = (a^s)^q a^r = 1^q a^r = a^r.$$

If  $r \neq 0$ , then  $r$  would be a natural number smaller than  $s$  with  $a^r = 1$ , contradicting Lemma 11.4. So  $r = 0$ ,  $n = qs$  and  $s | n$ .

$\square$

**11.7 Lemma:** *If  $G$  is a finite group, then  $a^{|G|} = 1$  for all  $a \in G$ .*

**Proof:** For any  $a \in G$ ,  $o(a) = |\langle a \rangle|$  divides  $|G|$  by Lagrange's theorem. So  $a^{|G|} = 1$  by Lemma 11.6.  $\square$

Next we show that subgroups of cyclic groups are also cyclic.

**11.8 Theorem:** *Let  $G$  be a cyclic group and let  $H \leq G$ . Then  $H$  is cyclic. More informatively, let  $G = \langle a \rangle$ . Then  $\{1\} = \langle 1 \rangle$  and if  $H \neq \{1\}$ , then  $H = \langle a^t \rangle$ , where  $t$  is the smallest natural number in the set  $\{n \in \mathbb{N} : a^n \in H\}$ .*

**Proof:** The subgroup  $\{1\}$  of  $G = \langle a \rangle$  is clearly the cyclic subgroup of  $G$  generated by 1, hence  $\{1\} = \langle 1 \rangle$  is cyclic. Suppose now  $\{1\} \neq H \leq G$ . We prove that  $H$  is cyclic, and in fact  $H = \langle a^t \rangle$  as stated in the theorem. Since  $H \neq \{1\}$  by assumption, there is a nonidentity element in  $H$ , say  $a^m \in H$ , with  $m \in \mathbb{Z} \setminus \{0\}$ . Then  $a^{-m} \in H$  since  $H$  is closed under the forming of inverses. So  $a^m, a^{-m} \in H$ ,  $m \neq 0$ . So there is a natural number  $n$  such that

$a^n \in H$ , for instance  $n = |m|$ . Thus the set  $\{n \in \mathbb{N} : a^n \in H\}$  is not empty. From the natural numbers in this set, we choose the smallest one and call it  $t$ .

Now  $a^t \in H$ . Also  $a^{-t} = (a^t)^{-1} \in H$ . Since  $H$  is closed under multiplication, we obtain  $a^{kt} = (a^t)^k = a^t a^t \dots a^t \in H$  and  $a^{-kt} = (a^{-t})^k = a^{-t} a^{-t} \dots a^{-t} \in H$  for all  $k \in \mathbb{N}$ . Since  $a^{0t} = 1 \in H$ , we see  $a^{mt} = a^{tm} \in H$  for all  $m \in \mathbb{Z}$ . Thus we have  $\langle a^t \rangle = \{a^{tm} \in G : m \in \mathbb{Z}\} \subseteq H$ .

Assume next  $b \in H$ , where  $b \in G = \langle a \rangle$ . We write  $b = a^n$  with a suitable  $n$  in  $\mathbb{Z}$  and divide  $n$  by  $t$ . This gives

$$\begin{aligned} n &= tq + r, \quad q, r \in \mathbb{Z}, \quad 0 \leq r < t, \\ a^r &= a^{n-tq} = a^n (a^{-t})^q \in H, \end{aligned}$$

since  $a^n, a^{-t} \in H$ . If  $r \neq 0$ , then  $r$  would be a natural number smaller than  $t$  such that  $a^r = 1$ , contradicting the definition of  $t$ . So  $r = 0$ ,  $n = tq$ ,  $t|n$  and  $b = a^n = a^{tq} \in \langle a^t \rangle$ . This holds for all  $b \in H$ . Hence  $H \subseteq \langle a^t \rangle$ .

From  $\langle a^t \rangle \subseteq H$  and  $H \subseteq \langle a^t \rangle$ , we get  $H = \langle a^t \rangle$ , as claimed.  $\square$

**11.9 Lemma:** Let  $G$  be a group and  $a \in G$ . Let  $k \in \mathbb{Z}$ ,  $k \neq 0$ .

- (1) If  $o(a) = \infty$ , then  $o(a^k) = \infty$ .
- (2) If  $o(a) = n \in \mathbb{N}$ , then  $o(a^k) = n/(n, k)$ .

**Proof:** (1) Suppose  $o(a) = \infty$ . If  $o(a^k)$  were finite, say  $o(a^k) = m \in \mathbb{N}$ , then  $(a^k)^m = 1$ , so  $a^{km} = 1 = a^0$ , although  $km$  and  $0$  are distinct integers, contrary to Lemma 11.5. So  $o(a) = \infty$  implies  $o(a^k) = \infty$ .

(2) Now let us suppose  $o(a) = n \in \mathbb{N}$ . Then  $\langle a^k \rangle \leq \langle a \rangle$  and so  $o(a^k)$  is finite. By Lemma 11.4,

$$\begin{aligned} o(a^k) &= \text{smallest natural number } s \text{ such that } (a^k)^s = 1 \\ &= \text{smallest natural number } s \text{ such that } a^{ks} = 1 \\ &= \text{smallest natural number } s \text{ such that } n|ks \quad (\text{Lemma 11.6}) \\ &= \text{smallest natural number } s \text{ such that } \frac{n}{(n, k)} \mid \frac{k}{(n, k)} s \end{aligned}$$

= smallest natural number  $s$  such that  $\frac{n}{(n,k)} \mid s$  (Lemma

5.11

and

Theorem 5.12)

$$= \frac{n}{(n,k)}. \quad \square$$

From Lemma 11.9(1), we infer that any nontrivial subgroup of an infinite cyclic group is infinite. Using Lemma 11.9(2), we can find the number of generators of a finite cyclic group. Let  $G = \langle a \rangle$  be a cyclic group of order  $n \in \mathbb{N}$ . Which elements are the generators of  $G$ ? Any element  $a^k$  generates a subgroup  $\langle a^k \rangle$  of  $\langle a \rangle$  and  $a^k$  is a generator of  $\langle a \rangle$  if and only if  $\langle a^k \rangle = \langle a \rangle$ . We know  $\langle a^k \rangle \leq \langle a \rangle$ , so, since  $|\langle a \rangle| = n$  is finite,  $a^k$  is a generator of  $\langle a \rangle$  if and only if  $|\langle a^k \rangle| = |\langle a \rangle|$ . Thus  $a^k$  is a generator of  $\langle a \rangle$  if and only if  $o(a^k) = o(a)$ , that is, if and only if  $n = n/(n,k)$ , and so if and only if  $(n,k) = 1$ . There are  $n$  distinct elements  $a^0, a^1, a^2, \dots, a^{n-1}$  in  $\langle a \rangle$ , and among these,

$$\{a^k : (n,k) = 1, 0 \leq k \leq n-1\} = \{a^k : (n,k) = 1, 1 \leq k \leq n\}$$

is the set of generators of  $\langle a \rangle$ . Hence the number of generators of  $\langle a \rangle$  is the number of positive integers smaller than (or equal to)  $n$  and relatively prime to  $n$ . This number is traditionally denoted by  $\varphi(n)$ . For example

$$\begin{aligned} \varphi(1) = 1, & \quad \varphi(2) = 1, & \quad \varphi(3) = 2, & \quad \varphi(4) = 2, & \quad \varphi(5) = 4, \\ \varphi(6) = 2, & \quad \varphi(7) = 6, & \quad \varphi(8) = 4, & \quad \varphi(9) = 6, & \quad \varphi(10) = 4. \end{aligned}$$

The function  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$  is known as Euler's *phi function* or Euler's *totient function* (L. Euler, a Swiss mathematician (1707-1783)).

Lagrange's theorem asserts that  $m \mid |G|$  when there is a subgroup  $H$  of order  $|H| = m$  (provided  $G$  is a finite group). The converse of Lagrange's theorem is false: if  $G$  is a finite group and  $m \mid |G|$ , then it is not necessarily true that  $G$  has a subgroup of order  $m$  (see §16, Ex.7). However, for cyclic groups, the converse of Lagrange's theorem is true.

**11.10 Lemma:** *Let  $G = \langle a \rangle$  be a cyclic group of order  $|G| = n$ . For any positive divisor  $m$  of  $n$ , there is a unique subgroup  $H$  of order  $|H| = m$ , namely  $\langle a^{n/m} \rangle$ .*

**Proof:**  $o(a) = n$  by hypothesis. We write  $n = mk$ . Consider the subgroup  $\langle a^k \rangle$  of  $\langle a \rangle$ . We observe  $|\langle a^k \rangle| = o(a^k) = n/(n,k) = mk/(mk,k) = mk/k = m$ , so  $\langle a^k \rangle$  is a subgroup of order  $m$ .

We now show that  $\langle a^k \rangle$  is the unique subgroup of  $G$  of order  $m$ . Let  $L$  be a subgroup of order  $m$ . We want to prove  $L = \langle a^k \rangle$ . Since  $|L| = |\langle a^k \rangle| = m$  is finite, it will suffice to prove that  $L \leq \langle a^k \rangle$ . This is certainly true if  $L = \{1\}$ , that is, if  $m = 1$ . When  $m \neq 1$ , we have, by Theorem 11.8,  $L = \langle a^t \rangle$ , where  $t$  is the smallest natural number such that  $a^t \in L$ . In order to show  $\langle a^t \rangle = L \leq \langle a^k \rangle$ , we need only prove  $a^t \in \langle a^k \rangle$ , i.e., we need only prove  $k|t$ . This is easy: since  $o(a^t) = |\langle a^k \rangle| = |L| = m$ , we get  $(a^t)^m = 1$  by Lemma 11.6, so  $a^{tm} = 1$ , so  $n|tm$  by Lemma 11.6 again, which gives  $km|tm$ , hence  $k|t$ .

□

Lemma 11.10 implies that a finite cyclic group  $G$  has, for any positive divisor  $k$  of  $|G|$ , a unique subgroup of index  $k$ . This reformulation of Lemma 11.10 extends immediately to infinite cyclic groups.

**11.11 Lemma:** *Let  $G = \langle a \rangle$  be a cyclic group of infinite order. For any  $m \in \mathbb{N}$ , there is a unique subgroup  $H$  of  $G$  of index  $|G:H| = m$ , namely  $H = \langle a^m \rangle$ . Any nontrivial subgroup of  $G$  has finite index in  $G$ .*

**Proof:** We have  $G = \langle a \rangle$ ,  $o(a) = \infty$ . The elements of  $G$  are the symbols  $a^k$ , where  $k$  runs through the set of integers. By Lemma 11.5,  $a^k \neq a^j$  for  $k \neq j$ . Two symbols are multiplied by adding the exponents:  $a^k \cdot a^j = a^{k+j}$ . Also,  $a^0$  is the identity and  $(a^k)^{-1}$  is the symbol  $a^{-k}$ . Essentially, we have the group of integers under addition, but the integers are written as exponents.

First we prove that a nontrivial subgroup of  $G$  has finite index in  $G$ . Let  $L \leq G = \langle a \rangle$ ,  $L \neq \{1\}$ . From Theorem 11.8, we know  $L = \langle a^t \rangle$ , where  $t$  is the smallest natural number such that  $a^t \in L$ . Any element  $a^n$  of  $G = \langle a \rangle$

can be written as  $a^{tq+r}$ , with some uniquely determined integers  $q, r$ , where  $0 \leq r \leq t - 1$ . Thus any element  $a^n$  of  $G$  belongs to one and only one of the subsets

$$\{a^{tq}: q \in \mathbb{Z}\}, \{a^{tq+1}: q \in \mathbb{Z}\}, \{a^{tq+2}: q \in \mathbb{Z}\}, \dots, \{a^{tq+(t-1)}: q \in \mathbb{Z}\},$$

which are just the right cosets

$$\begin{array}{cccccc} \langle a^t \rangle a^0, & \langle a^t \rangle a^1, & \langle a^t \rangle a^2, & \dots, & \langle a^t \rangle a^{t-1} \\ La^0, & La^1, & La^2, & \dots, & La^{t-1} \end{array}$$

of  $L$ . The uniqueness of  $q$  and  $r$  implies that these cosets are distinct. Alternatively, one can show that these cosets are distinct by noting that  $La^i = La^j$  ( $0 \leq i, j \leq t - 1$ ) implies, when  $i \neq j$ , say when  $i < j$ , that  $L = La^{j-i}$  and thus (Lemma 10.2(2))  $a^{j-i} \in L$ , where  $0 < j - i \leq t - 1$ , contrary to the definition of  $t$  as the smallest natural number such that  $a^t \in L$ . So there are exactly  $t$  distinct right cosets of  $L$  in  $G$  and  $|G:L| = t$  is finite.

We proved in fact that  $|G:\langle a^t \rangle| = t$  when  $t \in \mathbb{N}$ . Thus, for any  $m \in \mathbb{N}$ , there is a subgroup of  $G$  of index  $m$ , namely  $\langle a^m \rangle$ . We proceed to show that  $\langle a^m \rangle$  is the unique subgroup of  $G$  of index  $m$ . Assume  $K \leq G$  with  $|G:K| = m \in \mathbb{N}$ . We are to show  $K = \langle a^m \rangle$ . Now  $K = \langle a^k \rangle$ , where  $k$  is the smallest natural number such that  $a^k \in K$  (as  $|G:K|$  is finite,  $K \neq \{1\}$ ). So  $m = |G:K| = |G:\langle a^k \rangle| = k$  and  $a^m = a^k$ , which yields  $K = \langle a^k \rangle = \langle a^m \rangle$ . Therefore  $\langle a^m \rangle$  is the unique subgroup of  $G$  of index  $m$ .  $\square$

We learned the structure of cyclic groups quite well, but we had only a few examples. We have not seen any cyclic group of order 5 or 7. For all we know about cyclic groups up to now, it is feasible that there is no cyclic group of order 5 or 7. We show next that there is a cyclic group of any order. Incidentally, this shows that there are groups of all orders.

**11.12 Theorem:** *There is a cyclic group of infinite order. Also, for any  $n \in \mathbb{N}$ , there is a cyclic group of order  $n$ .*

**Proof:** We give examples of cyclic groups in additive notation. In this notation,  $\langle a \rangle$  is the group  $\{na: n \in \mathbb{Z}\}$ , the group operation being  $na + ma = (n + m)a$ , the additive counterpart of the rule  $a^n a^m = a^{n+m}$ .

$\mathbb{Z}$  (under addition) is a cyclic group of infinite order as  $\mathbb{Z} = \{m1 : m \in \mathbb{Z}\} = \langle 1 \rangle$  is generated by  $1 \in \mathbb{Z}$ .

$\mathbb{Z}_n$  (under addition) is a cyclic group of order  $n$  as  $\mathbb{Z}_n = \{m\bar{1} : m \in \mathbb{Z}\} = \langle \bar{1} \rangle$  is generated by  $\bar{1} \in \mathbb{Z}_n$ .

□

**11.13 Theorem:** *Let  $p$  be a prime number. If  $G$  is a group of order  $p$ , then  $G$  is cyclic.*

**Proof:** Since  $p$  is prime,  $|G| = p \neq 1$  and so  $G$  does not consist of the identity element only. Let  $a$  be any element of  $G$  distinct from the identity. Then  $1 \neq \langle a \rangle \leq G$  and  $|\langle a \rangle|$  is a positive divisor of  $|G| = p$  by Lagrange's theorem. Since  $\langle a \rangle \neq 1$ , we have  $|\langle a \rangle| \neq 1$ , and so  $|\langle a \rangle| = p = |G|$ . This forces  $G = \langle a \rangle$ . Thus  $G$  is a cyclic group. (In fact, any nonidentity element of  $G$  is a generator of  $G$ .) □

## Exercises

1. Let  $G$  be a group and let  $a$  be an element of finite order  $n$  in  $G$ . Show that, for all  $m, k \in \mathbb{Z}$ , the equality  $a^m = a^k$  holds if and only if  $m \equiv k \pmod{n}$ .
2. Find all subgroups of a cyclic group of order 8, of a cyclic group of order 10, and of a cyclic group of order 12.
3. Let  $G$  be a group,  $a \in G$  and  $o(a) = 36$ . What are the orders of  $a^2, a^3, a^4, a^7, a^{12}, a^{15}, a^{17}$ ?
4. Let  $G$  be a group and  $a \in G$ . Let  $n, k \in \mathbb{N}$  and let  $m = [n, k]$  be the least common multiple of  $n$  and  $k$ . Prove that  $\langle a^n \rangle \cap \langle a^k \rangle = \langle a^m \rangle$ .
5. Let  $G$  be a group and  $a \in G$  with  $o(a) = n_1 n_2 \in \mathbb{N}$ , where  $n_1, n_2$  are relatively prime natural numbers. Show that there are uniquely determined elements  $a_1, a_2$  of  $G$  such that

$$a_1 a_2 = a = a_2 a_1$$

and

$$o(a_1) = n_1, o(a_2) = n_2.$$

6. Let  $G$  be a group and  $a, b \in G$ . Assume that  $o(a) \in \mathbb{N}$ ,  $o(b) \in \mathbb{N}$  and that  $o(a), o(b)$  are relatively prime. Prove: if  $ab = ba$ , then  $o(ab) = o(a)o(b)$ . Prove also that  $o(ab) = o(a)o(b)$  is not necessarily true when the hypothesis  $ab = ba$  is omitted.

7. Show that, if  $p, n \in \mathbb{N}$  and  $p$  is prime, then  $\varphi(p^n) = p^n - p^{n-1}$ .