

Math 71: Algebra

Groups of Small Order

Amittai Siavava

## CONTENTS

1. Groups of Prime Order	3
References	5

## 1. GROUPS OF PRIME ORDER

Next, let's look at groups of prime order through some motivating theorems.

*Theorem 1.1* (Lagrange). If  $G$  is a finite group and  $H$  is a subgroup of  $G$ , then  $|H|$  divides  $|G|$  and the number of left cosets of  $H$  in  $G$  is equal to  $\frac{|H|}{|G|}$ . (I, p.89, Theorem 8)

*Proposition 1.2.* If  $G$  is a finite group of prime order  $p$  then every non-identity element of  $G$  has order  $p$ .

*Proof.* Let  $g$  be a non-identity element of  $G$ , without loss of generality, such that the order of  $g$  is  $x \in \mathbb{Z}_{\geq 0}$ . Then  $g^x = \epsilon$ . This immediately tells us that  $x$  cannot be 1, since  $g$  is clearly not the group identity. Let  $\langle g \rangle$  be the set of all elements  $g^i, i \in \mathbb{Z}$ . Notice that  $\langle g \rangle$  contains *at least* two elements:  $g^x = \epsilon$ , and  $g^1 = g$ . Now, for arbitrary powers  $n \in \mathbb{Z}$ , let  $ax + b = n$ . Then:

$$g^n = g^{ax+b} = (g^x)^a \cdot g^b \epsilon^a \cdot g^b = \epsilon \cdot g^b = g^b$$

This tells us that  $\langle g \rangle$  has at most  $x$  elements. In fact,  $\langle g \rangle$  has exactly  $x$  elements since we took distinct powers of  $g$  and  $g^x = \epsilon$  is the smallest power that cycles back to 0. So;

- (a) The set  $\langle g \rangle$  is finite (it has  $x$  elements).
- (b) The set  $\langle g \rangle$  is closed under the group operation (since the equivalence of every power of  $g$  is in the set).
- (c) The set  $\langle g \rangle$  contains the identity element.

Therefore,  $\langle g \rangle$  is a group. Remember that we picked  $g$  from  $G$ , and  $G$  is itself a group that is closed under the group operation, so  $\langle g \rangle \leq G$ . The first part of Lagrange's theorem tells us that the order of any subgroup  $S \leq G$  *must* divide the order of  $G$ . So  $x$  must divide  $p$ , but  $p$  is prime so  $x = p$ . Therefore, the order of the element  $g$  is  $p$ .  $\square$

*Proposition 1.3.* If a group of order  $n$  contains an element of order  $n$  then the group is cyclic.

*Proof.* Let  $g \in G$  such that the order of  $g$  is  $n$ . Then  $g^n = \epsilon$ . Consider the set  $\langle g \rangle$ . As we saw in Proposition 1.2,  $\langle g \rangle$  is a group of order  $n$ , and it is contained in  $G$ . Therefore,  $\langle g \rangle = G$  since  $G$  has order  $n$ . Therefore,  $G$  is cyclic.  $\square$

*Proposition 1.4.* All cyclic groups of a fixed order  $n$  are isomorphic.

*Proof.* Let  $G$  and  $H$  be cyclic groups of order  $n$ . Let  $g \in G$  and  $h \in H$  be generators. Then the map  $\psi : G \rightarrow H$  defined by  $\psi(g) = h$  is an isomorphism.

$$\begin{aligned} \psi(g) &= h \\ \psi(g^i) &= \psi\left(\prod_{j=0}^{i-1} g\right) = \prod_{j=0}^{i-1} \psi(g) = \prod_{j=0}^{i-1} h = h^i \\ \psi(g^i \cdot g^k) &= \psi(g^{i+k}) = h^{i+k} = h^i \cdot h^k = \psi(g^i) \cdot \psi(g^k) \end{aligned}$$

Therefore, the two groups are isomorphic.  $\square$

*Proposition 1.5.* If  $G$  is a cyclic group then  $G$  is abelian.

*Proof.* Let  $G$  be a cyclic group of order  $p$ , with  $g \in G$  as a generator. Then every element can be expressed as  $g^i$  for some  $i \in \{0, 1, \dots, p-1\}$ , with powers interpreted as repeated application of the group operation. Let  $x \in G$  and  $y \in G$  such that  $x = g^a$  and  $y = g^b$ . Then:

$$xy = g^a \cdot g^b = g^{a+b} = g^b \cdot g^a = yx \quad (1.6)$$

Therefore, for any  $x, y \in G$ ,  $xy = yx$ , and  $G$  is abelian.  $\square$

*Corollary 1.7.* If  $G$  is a finite group of prime order, then  $G$  is abelian.

*Proof.* In combining propositions 1.2, 1.3, 1.4, and 1.5, we see that any group of prime order has a generating element, and by expressing every element in the group as a power of the generating element, we see that the group operation commutes for all elements. We also see that all groups of a given prime order  $p$  are isomorphic. Therefore, every group of prime order is abelian.  $\square$

**Definition 1.8.** The cyclic group of order  $p$  is denoted as  $C_p$  (or  $Z_p$ , in parallel to the integers  $\mathbb{Z} \pmod{p}$ ).

In summary, we have shown that every group of prime order is cyclic and abelian. This tells us that there is only a single structure for any groups of a given prime order  $p$ : the group  $C_p$ . For instance, the only groups of order 2, 3, 5, 7, 11, and 13 are the groups  $C_2, C_3, C_5, C_7, C_{11}$ , and  $C_{13}$  respectively.

Order	Group	Isomorphisms
2	$C_2$	$\mathbb{Z}/2\mathbb{Z}$
3	$C_3$	$\mathbb{Z}/3\mathbb{Z}$
5	$C_5$	$\mathbb{Z}/5\mathbb{Z}$
7	$C_7$	$\mathbb{Z}/7\mathbb{Z}$
11	$C_{11}$	$\mathbb{Z}/11\mathbb{Z}$
13	$C_{13}$	$\mathbb{Z}/13\mathbb{Z}$

TABLE 1. Groups of prime order  $n \leq 15$

## REFERENCES

1. D. S. Dummit, R. M. Foote, *Abstract Algebra* (John Wiley & Sons, ed. 3, 2003).