Lecture Notes for Abstract Algebra: Lecture 7

1 Cyclic groups

1.1 Cyclic groups, subgroups of a cyclic group and order of elements in a group

Definition 1. let $G = (G, *)$ be a group and $S \subset G$ a set. The subgroup generated by S, denoted $\langle S \rangle$, is the smallest subgroup of G containing S.

Example 2. Let G be a group and $x \in G$. Then, the subgroup $\langle x \rangle$ generated by x is the subgroup consisting of powers $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$.

Definition 3. $G = (G, *)$ be a group and $S \subset G$ a set. We say that G is generated by S when $\langle S \rangle = G$. A group G is cyclic if there exist an element $x \in G$ such that

$$\langle x \rangle = G.$$

The element x is called a generator of the group G.

Definition 4. The order of an element $x \in G$ is the order of the subgroup $\langle x \rangle$ generated by x. It may be finite or infinite.

Remark 5. The order of an element $x \in G$ is the smallest m such that $x^m = e$. If no such m exist, the order of x is infinite.

Example 6. In S_3, the subgroup generated by the permutation $(1\,2)$ is

$$\langle (1\,2) \rangle = \{1, (1\,2)\}.$$

On the other hand $\langle (1\,2\,3) \rangle = \{1, (1\,2\,3), (1\,3\,2)\}$. The order if $(1\,2)$ is two while the order of $(1\,2\,3)$ is three.

Example 7. A cyclic group G of order n can be written as

$$G = \{e, x, x^2, \ldots, x^{n-1}\}.$$

where $x \in G$ is a generator of the group G.

Example 8. $\mathbb{Z}_n = (\mathbb{Z}, + \bmod n)$ is generated by $1 \bmod n$ and is therefore cyclic of order n. The generator of a cyclic group is not unique, see for example how the same group $\mathbb{Z}_n$ could be generated with any number a relatively prime to n.

Example 9. The group $\mathbb{V}_4$ of order 4 is not cyclic. All elements, except the identity, have order 2:

$$\mathbb{V}_4 = \begin{array}{c|cccc} & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array}$$

We can check $a + a = e$, $b + b = e$ and $c + c = e$. There is not element of order 4.

Remark 10. Every cyclic group must be abelian. The group $\mathbb{V}_4$ is an example of an abelian group that is not cyclic.

Proposition 11. *Every subgroup of a cyclic group is cyclic.*

Proof. Let G be a cyclic group generated by x and suppose that H is a subgroup of G. If $H = \{e\}$, we finished. Suppose that H contains some other element g distinct from the identity. Then g can be written as x^n for some integer n. Since g is a subgroup, $g^{-1} = x^{-n}$ must also be in H. Since either n or $-n$ is positive, we can assume that H contains positive powers of x^m with $n > 0$. Let m be the smallest natural number such that $x^m \in H$. Such an m exists by the Principle of Well-Ordering. We claim that $h = x^m$ is a generator for H. We must show that every $h' \in H$ can be written as a power of h. Since $h' \in H$ and H is a subgroup of G, $h' = x^k$ for some integer k. Using the division algorithm, we can find numbers q and r such that $k = mq + r$ where $0 \leq r < m$; hence,

$$x^k = x^{mq+r} = (x^m)^q x^r = h^q x^r.$$

We have that $x^r = x^k h^{-q}$ is also in H. If $r \neq 0$, this will contradict the way we chose m. Hence $r = 0$ and $k = mq \Rightarrow h' = h^q$. □

Remark 12. The dihedral group $\mathbb{D}_3$ cannot be cyclic because is not even abelian! The reflections μ_1, μ_2 and μ_3 are elements of order 2 and the rotations ρ_1 and ρ_2 are elements of order 3. The composition of two reflections $\mu_i \circ \mu_j$ gives a rotation, which is an element of order 3. We can therefore check directly that no element has order 6.

Proposition 13. *Let G be a cyclic group of order n and suppose that $a \in G$ is a generator of the group. If $b = a^k$, then the order of b is n/d, where $d = gcd(k, n)$.*

Proof. We wish to find the smallest integer m such that $e = b^m = a^{mk}$. This is to find, the smallest integer m such that n divides km or, equivalently, n/d divides $m(k/d)$. Since d is the greatest common divisor of n and k, the numbers n/d and k/d are relatively prime and the number n/d must divide m. As a consequence $m \geq n/d$. On the other hand $b^{n/d} = a^{n(k/d)} = e^{k/d} = e$. $\square$

Corollary 14. *A cyclic group G of order n has exactly one subgroup G_d of order d for each $d|n$. If a generates G, then $a^{n/d}$ generates G_d.*

Proposition 15. *An element x has the same order as and any of its conjugates $x_y = yxy^{-1}$.*

Proof. We have the identity $(x_y)^n = yxy^{-1}yxy^{-1} \ldots yxy^{-1} = yx^ny^{-1}$. Hence

$$x^n = e \iff (x_y)^n = e.$$

$\square$

Practice Questions:

1. Let G be a group and x an element of G. Show that the subset of integral powers $\langle x \rangle = \{x^n \,|\, n \in \mathbb{Z}\}$ is a subgroup of G.

2. Let G be a group. Show that the order of the element $x \in G$ is the smallest m such that $x^m = e$. Show that a power $x^k = e$ if and only if k is a multiple of m.

3. Show that any cyclic group is abelian. Find examples of finite abelian groups that are not cyclic.

4. Find the order of the elements in $\mathbb{Z}_6$. What elements generate the whole group?