13. Orders of group elements and cyclic groups

13.1. **Orders of group elements.**

Definition. Let G be a group.

(a) The order of G, denoted by $|G|$, is the number of elements in G.

(b) Let g be an element of G. The order of g, denoted by $o(g)$, is the smallest POSITIVE integer n such that $g^n = e$, if such n exists. If $g^n \neq e$ for all $n \in \mathbb{N}$, we set $o(g) = \infty$.

Example 1. *Let $G = (\mathbb{R}^\times, \cdot)$, invertible (=nonzero) reals with multiplication.*

We have $o(1) = 1$, $o(-1) = 2$ (since $-1 \neq 1$, but $(-1)^2 = 1$). It is easy to see that $o(x) = \infty$ for any $x \neq \pm 1$.

Example 2. *Let $G = (\mathbb{Z}_{11}^\times, \cdot) = (\mathbb{Z}_{11} \setminus \{0\}, \cdot)$. Find the order of $[4]$.*

We have $[4]^2 = [16] = [5]$, $[4]^3 = [4]^2 \cdot [4] = [5] \cdot [4] = [20] = [9]$, $[4]^4 = [9] \cdot [4] = [36] = [3]$, $[4]^5 = [3] \cdot [4] = [12] = [1]$. Thus $o([4]) = 5$.

Note that a "naive" way to determine the order of $[4]$ in $\mathbb{Z}_{11}$ would have been to compute powers of 4 (in $\mathbb{Z}$) and reduce each of them mod 11 until we get the remainder 1, but this would required computations with four digit numbers. On the other hand, in the above calculation we never had to deal with numbers with more than two digits.

The following theorem shows that the structure of the cyclic subgroup generated by an element a of some group G is completely determined by the order of a.

Theorem 13.1. *Let G be a group and a an element of G.*

(1) *Suppose that $o(a) = \infty$. Then all integer powers of a are distinct, that is, $a^n \neq a^m$ for any $n, m \in \mathbb{Z}$ with $n \neq m$*

(2) *Suppose now that $o(a) < \infty$ and let $n = o(a)$. The following hold:*

  (a) *The elements $e = a^0, a, a^2, \ldots, a^{n-1}$ are distinct*

  (b) *Given any $m \in \mathbb{Z}$, write $m = qn + r$ with $0 \leq r < n$ (that is, r is the remainder of m mod n). Then $a^m = a^r$.*

  (c) $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$.

Proof. We will prove part (2). The proof of part (1) is similar and easier.

(2)(a). We argue by contradiction. Suppose that the elements $a^0, a, \ldots, a^{n-1}$ are not distinct. Then there exist $i, j \in \mathbb{N}$ with $0 \leq i, j \leq n-1$ and $i \neq j$

such that $a^i = a^j$. WOLOG $i < j$. Multiplying both sides of $a^i = a^j$ by a^{-i} and using exponent laws, we get $a^{j-i} = e$. This contradicts the assumption $o(a) = n$ since $0 < j - i < n$ by construction.

(2)(b). This is proved by direct computation: $a^m = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = e^q a^r = a^r$.

Finally, by definition $\langle a \rangle = \{a^m : m \in \mathbb{Z}\}$, so (2)(c) follows directly from (2)(b). □

The following immediate corollary of Theorem 13.1 can be used as an alternative definition of the order of an element.

Corollary 13.2. *Let a be an element of a group G. Then $o(a) = |\langle a \rangle|$, that is, the order of a is equal to the order of the cyclic subgroup generated by a.*

Proof. We consider two cases.

Case 1: $o(a) = \infty$. Then $|\langle a \rangle| = \infty$ as well by Theorem 13.1(1), so $o(a) = |\langle a \rangle|$ in this case.

Case 2: $o(a) < \infty$. Let $n = o(a)$. Then $|\langle a \rangle| \geq n$ by Theorem 13.1(2)(a) and $|\langle a \rangle| \leq n$ by Theorem 13.1(2)(c). Combining the two inequalities, we get that $|\langle a \rangle| = n = o(a)$.

Thus, we proved that $o(a) = |\langle a \rangle|$ in all cases. □

13.2. **Cyclic groups.**

Definition. A group G is called cyclic if there exists $a \in G$ such that $G = \langle a \rangle$. If G is cyclic, any a such that $G = \langle a \rangle$ is called a generator of G.

Example 3. *Let $G = (\mathbb{Z}, +)$.*

For any $a \in G$ we have $\langle a \rangle = \{ak : k \in \mathbb{Z}\} = a\mathbb{Z}$. Clearly, $\langle a \rangle = \mathbb{Z} \iff a = \pm 1$. Thus, G is cyclic and has precisely two generators: 1 and -1.

Example 4. *Let $G = (\mathbb{Z}_n, +)$.*

As in the previous example, G is cyclic, and $\pm[1]$ are generators. However, unlike the case of $\mathbb{Z}$, the group $\mathbb{Z}_n$ has more than two generators for most values of n. For instance, [3] is a generator of $\mathbb{Z}_{10}$, as we saw in the previous lecture; see Proposition 13.3 below for a complete description of generators of $\mathbb{Z}_n$.

Example 5. *Determine whether the group $G = (\mathbb{Z}_n^\times, \cdot)$ is cyclic for $n = 5$ and $n = 8$.*

By definition, to determine whether a finite group is cyclic, it suffices to go over all its elements and for each of them check whether that element generates the entire group (once and if we found a generator, we can stop unless the problem asks to find all the generators). Also note that in some cases it may be clear from the beginning that the group is not cyclic – for instance, cyclic groups are abelian (=commutative), so if we are given a non-abelian group, it cannot be cyclic; however, this observation does not apply in this example.

(i) $G = \mathbb{Z}_5^\times = \{[1], [2], [3], [4]\}$. Clearly, $[1]$ is not a generator; on the other hand, $\langle [2] \rangle = \{[1], [2], [4], [8] = [3]\} = G$, so we proved that $\mathbb{Z}_5^\times$ is cyclic.

(ii) $G = \mathbb{Z}_8^\times = \{[1], [3], [5], [7]\}$. We have $\langle [1] \rangle = \{[1]\}$, $\langle [3] \rangle = \{[1], [3], [9] = [1]\} \neq G$, $\langle [5] \rangle = \{[1], [5], [25] = [1]\} \neq G$, $\langle [7] \rangle = \{[1], [7], [49] = [1]\} \neq G$. Thus, we showed by exhaustion that none of the elements of G is a generator, so G is not cyclic.

Note that in the above computation in $\mathbb{Z}_8^\times$ we used the following "algorithm" for computing the cyclic subgroup generated by an element a of a finite group: compute powers of a one at time starting with exponent zero $(a^0, a, a^2, \ldots)$ and continue until we get the identity element for the second time (that is, until we find the first positive n such that $a^n = e$). Once this happens, we can stop as by that time we have found all elements of $\langle a \rangle$. The justification of this algorithm is provided by Theorem 13.1(2).

We finish the lecture by describing all generators of the groups $(\mathbb{Z}_n, +)$.

Proposition 13.3. *Let $G = (\mathbb{Z}_n, +)$ for some $n \geq 2$. An element $[a] \in G$ is a generator $\iff$ a and n are coprime.*

Proof. First observe that $[a]$ is a generator of $G \iff \langle [a] \rangle$ contains $[1]$. Indeed, the direction $\Rightarrow$ is clear by definition. On the other hand, suppose that $\langle [a] \rangle$ contains $[1]$. Then $\langle [a] \rangle$ is some subgroup containing $[1]$, while $\langle [1] \rangle$ is the smallest subgroup containing $[1]$ (by the original definition of cyclic subgroup – see Lecture 12). Thus $\langle [a] \rangle$ contains $\langle [1] \rangle = G$, and so $\langle [a] \rangle = G$ (since $\langle [a] \rangle$ cannot contain any elements outside of G).

Thus, $[a]$ is a generator of $G \iff [1] \in \langle [a] \rangle \iff [1] = k[a]$ for some $k \in \mathbb{Z}$.

Since $k[a] = \underbrace{[a] + \ldots + [a]}_{k \text{ times}} = [\underbrace{a + \ldots + a}_{k \text{ times}}] = [ka] = [k][a]$, we deduce that $[a]$ is a generator of $G \iff$ there exists $[k] \in \mathbb{Z}_n$ such that $[k][a] = [1]$. But by definition, such $[k]$ exists $\iff$ $[a]$ is an invertible element of the ring $\mathbb{Z}_n$, and we know from Lecture 9 that $[a] \in \mathbb{Z}_n$ is invertible $\iff$ a and n are coprime. $\square$