14. The structure of finite cyclic groups. Isomorphisms

14.1. **The structure of finite cyclic groups.** Recall that a group G is called *cyclic* if there exists $x \in G$ such that $\langle x \rangle = G$ and that any such x is called a generator of G. Theorem 13.1(2) from last class implies the following: if $G = \langle x \rangle$ is cyclic of order $n < \infty$, then $G = \{e, x, \dots, x^{n-1}\}$, elements $e, x, \dots, x^{n-1}$ are distinct, and $x^n = e$.

The simplest example of a cyclic group of order n is $G = (\mathbb{Z}_n, +)$, in which case $x = [1]$ is a generator. Last time we obtained a complete characterization of generators for the groups $(\mathbb{Z}_n, +)$:

Proposition 13.3. *Let $G = (\mathbb{Z}_n, +)$. An element $[k] \in G$ is a generator $\iff$ k is coprime to n.*

Let us also recall Example 2 from Lecture 12 where we described (albeit without formal proof) all subgroups of $G = (\mathbb{Z}_{10}, +)$. We found that there are exactly four subgroups: the entire group G, the trivial subgroup $\{e\}$, $\{[0], [2], [4], [6], [8]\} = \langle [2] \rangle$ and $\{[0], [5]\} = \langle [5] \rangle$. Observing that $G = \langle [1] \rangle$ and $\{e\} = \langle [0] \rangle = \langle [10] \rangle$, we see that all subgroups of $(\mathbb{Z}_{10}, +)$ are cyclic and actually bijectively correspond to positive divisors of 10. As you may expect, there is nothing special about 10, and the analogous result remains valid for all n.

The following theorem collects several basic facts about finite cyclic groups; in particular, it generalizes Proposition 14.1 and Example 2 from Lecture 12 to arbitrary cyclic groups. In the statement and proof below we use multiplicative notation.

Theorem 14.1 (Structure of finite cyclic groups)**.** *Let $G = \langle x \rangle$ be a finite cyclic group of order n. The following hold:*

(i) *Every subgroup of G is cyclic and is equal to $\langle x^d \rangle$ where $d > 0$ and $d \mid n$*
(ii) *If d and d' are positive divisors of n and $d \neq d'$, then $\langle x^d \rangle \neq \langle x^{d'} \rangle$*
(iii) *If $k \in \mathbb{Z}$, then x^k is a generator of $G \iff$ k and n are coprime.*
(iv) *For any $k \in \mathbb{Z}$ we have $\langle x^k \rangle = \langle x^d \rangle$ where $d = gcd(n, k)$*
(v) *For any $k \in \mathbb{Z}$ we have $o(x^k) = \frac{n}{gcd(n,k)}$.*

About the proof. A complete proof of Theorem 14.1 is given in [Gilbert, 3.4]. Below we will prove part (iv), part (v) is an exercise in Homework#7, and part (iii) is an easy consequence of (v) since x^k is a generator of $G \iff$

$\langle x^k \rangle = G \iff o(x^k) = |G| = n$. The fact that every subgroup of a cyclic group is cyclic appears as Theorem 2 in [Pinter, Chapter 11]. Part (i) of Theorem 14.1 (which is a slightly stronger statement) follows directly from this result and Theorem 14.1(iv). Finally, part (ii) follows from (v): if d and d' are positive divisors of n and $d \neq d'$, then $o(x^d) = \frac{n}{d}$ and $o(x^{d'}) = \frac{n}{d'}$ by (v), whence $|\langle x^d \rangle| = o(x^d) = \frac{n}{d} \neq \frac{n}{d'} = o(x^{d'}) = |\langle x^{d'} \rangle|$. Thus, subgroups $\langle x^d \rangle$ and $\langle x^{d'} \rangle$ have different orders and in particular must be distinct. □

Before proving Theorem 14.1(iv), we establish two general lemmas.

Lemma 14.2. *If H is a subgroup of some group G, then for any $b \in H$ we have $\langle b \rangle \subseteq H$.*

Proof. Clear since $\langle b \rangle = \{b^k : k \in \mathbb{Z}\}$ and subgroups are closed under taking powers. □

Lemma 14.3. *Let G be a group (not necessarily cyclic), $x \in G$ and $m, n \in \mathbb{Z}$. Let H be a subgroup of G. If $x^m \in H$ and $x^n \in H$, then $x^{gcd(n,m)} \in H$.*

Proof. By GCD theorem, there exist $u, v \in \mathbb{Z}$ such that $gcd(n, m) = nu+mv$. Since $x^n, x^m \in H$ and H is closed under taking powers, we have $x^{nu} = (x^n)^u \in H$ and $x^{mv} = (x^m)^v \in H$. Therefore, $x^{gcd(m,n)} = x^{nu+mv} = x^{nu}x^{mv} \in H$. □

Proof of Theorem 14.1(iv). It suffices to prove two inclusions:

$$\text{(a) } \langle x^k \rangle \subseteq \langle x^d \rangle \qquad \text{(b) } \langle x^d \rangle \subseteq \langle x^k \rangle$$

We start with (a). Since $d = gcd(n, k)$, we have $k = dl$ for some $l \in \mathbb{Z}$ whence $x^k = x^{dl} = (x^d)^l \in \langle x^d \rangle$. Hence by Lemma 14.2 applied to $H = \langle x^d \rangle$, we have $\langle x^k \rangle \subseteq \langle x^d \rangle$.

To prove (b) note that $\langle x^k \rangle$ contains x^k and also $x^n = e$. Hence applying Lemma 14.3 to $H = \langle x^k \rangle$, we conclude that $\langle x^k \rangle$ contains $x^{gcd(n,k)} = x^d$. Applying Lemma 14.2 again, we get that $\langle x^k \rangle \supseteq \langle x^d \rangle$, which proves (b). □

14.2. **Isomorphisms.** We start by motivating the notions of isomorphism isomorphic groups. Informally speaking, groups G and G' are called isomorphic if their multiplication tables can be obtained from each other by relabeling of elements.

Example 1. *Let $G = (\mathbb{Z}_5^\times, \cdot)$ and $G' = \{r_0, r_1, r_2, r_3\}$, the rotation subgroup of the group of isometries of a square (recall that r_k denotes the counter-clockwise rotation by $90k$ degrees for $k = 0, 1, 2, 3$).*

The multiplication tables of G and G' are given below:

$\cdot$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

$\circ$	r_0	r_1	r_2	r_3
r_0	r_0	r_1	r_2	r_3
r_1	r_1	r_2	r_3	r_0
r_2	r_2	r_3	r_0	r_1
r_3	r_3	r_0	r_1	r_2

(To compute the multiplication table of G' we simply observed that $r_i \circ r_j$ is the rotation by $90i + 90j = 90(i + j)$ degrees, so $r_i \circ r_j = r_{i+j}$ if $i + j < 4$ and $r_i \circ r_j = r_{i+j-4}$ if $i + j \geq 4$, where the latter holds since the rotation by $90 \cdot 4 = 360$ degrees is the identity map).

Let us now relabel elements of G using formal symbols r_0, r_1, r_2, r_3 as follows: $[1] \mapsto r_0, [2] \mapsto r_1, [3] \mapsto r_3, [4] \mapsto r_2$. Here is how the multiplication table of G will look like after this relabeling:

$\circ$	r_0	r_1	r_3	r_2
r_0	r_0	r_1	r_3	r_2
r_1	r_1	r_2	r_0	r_3
r_3	r_3	r_0	r_2	r_1
r_2	r_2	r_3	r_1	r_0

It is easy to check that this multiplication table is the same as the multiplication table of G' up to swapping the third and fourth rows and the third and fourth columns. Note that we are definitely not changing the group by changing the order of rows and columns in the multiplication table as there is no predetermined order in which group elements should be listed; the only thing we require is that rows labels and column labels appear in the same order. So, according to our informal definition, the groups G and G' are isomorphic.

The idea behind the notion of isomorphic groups is that all "abstract" properties of a group (that is, properties which do not pertain to specific nature of its elements) are completely determined by its multiplication table. Thus, based on our informal definition, isomorphic groups should have the same abstract properties. For instance, the property of being abelian (=commutative) is definitely abstract as it is clearly determined by the multiplication table: G is abelian $\iff$ the multiplication table of G is symmetric with respect to the main diagonal. Below are other examples of abstract properties, although it is not as transparent that these properties are determined by the multiplication table:

(i) G is cyclic
(ii) G has an element of order k for some fixed k.

Our next goal is to translate the informal definition of isomorphic groups into more formal language which will give us formal definitions of the notion of isomorphic groups and the notion of an isomorphism. So, what does it mean that multiplication tables of two groups G and G' differ only by relabeling of elements? First note that a relabeling is just a bijective map $\varphi : G \to G'$. In the above example the "relabeling" map φ was given by $\varphi([1]) = r_0, \varphi([2]) = r_1, \varphi([3]) = r_3$ and $\varphi([4]) = r_2$.

Next, what does it mean that the relabeling φ transforms the multiplication table of G into the multiplication table of G'? Take any two elements $g, h \in G$. In the initial multiplication table for G the element located at the intersection of g-row and h-column is gh. After the relabeling, the element located at the intersection of $\varphi(g)$-row and $\varphi(h)$-column is $\varphi(gh)$. At the same time, in the multiplication table for G', the element located at the intersection of $\varphi(g)$-row and $\varphi(h)$-column is $\varphi(g)\varphi(h)$. Thus, the multiplication table for G' coincides with the relabeled multiplication table for G $\iff$ $\varphi(gh) = \varphi(g)\varphi(h)$ for all $g, h \in G$.

The above analysis motivates the following formal definition:

Definition. *Let G and G' be groups.*

(a) *A map $\varphi : G \to G'$ is called an <u>isomorphism</u> if*
   (i) *φ is bijective*
   (ii) *φ preserves group operation: $\varphi(gh) = \varphi(g)\varphi(h)$ for all $g, h \in G$*

(b) *We say that G is <u>isomorphic</u> to G' if there exists an isomorphism $\varphi : G \to G'$.*

Note that in the equation in (a)(ii), the product gh on the left-hand side is a product in G, while the product $\varphi(g)\varphi(h)$ on the right-hand side is a product in G'.

14.3. **Book references.** The general references for the first part of this lecture are [Pinter, Chapter 11] and [Gilbert, 3.4]. The general references for the second part are the beginning of [Pinter, Chapter 9] and the beginning of [Gilbert, 3.5]