Elements of Algebraic Structures 06.02.24

Lecture 6: Cyclic Groups and Isomorphisms

Lecture: Sujata Ghosh *Scribe: Ritam M Mitra*

1 Cyclic Groups

Cyclic groups are groups in which every element is a power of some fixed element. Here are the relevant definitions.

1.1 Definitions

Definition. Let G be a group, $g \in G$. The *order* of g is the smallest positive integer n such that $g^n = 1$. If there is no positive integer n such that $g^n = 1$, then g has infinite order.

In the case of an abelian group with $+$ as the operation and 0 as the identity, the order of g is the smallest positive integer n such that $ng = 0$.

Definition. If G is a group and $g \in G$, then the subgroup generated by g is

$$\langle g \rangle = \{g^n | n \in Z\}.$$

If the group is abelian and $+$ is used as the operation, then

$$\langle g \rangle = \{ng | n \in Z\}.$$

Definition.A group G is **cyclic** if $G = \langle g \rangle$ for some $g \in G$. g is a **generator** of $\langle g \rangle$.

If a generator g has order n, $G = \langle g \rangle$ is **cyclic of order** n. If a generator g has infinite order, $G = \langle g \rangle$ is **infinite cyclic**.

1.2 Examples

Example. (**The integers and the integers mod n are cyclic**) Show that $\mathbb{Z}$ and $\mathbb{Z}_n$ for $n > 0$ are cyclic.

$\mathbb{Z}$ is an infinite cyclic group, because every element is a multiple of 1 (or of -1). For instance, 117 = 117.1. (Remember that "117.1" is really shorthand for $1 + 1 + \ldots + 1$ —1 added to itself 117 times.)

In fact, it is the only infinite cyclic group up to **isomorphism**. Notice that a cyclic group can have more than one generator. If n is a positive integer, $\mathbb{Z}_n$ is a cyclic group of order n generated by 1. For example, 1 generates $\mathbb{Z}_7$, since

$$1 + 1 = 2$$
$$1 + 1 + 1 = 3$$
$$1 + 1 + 1 + 1 = 4$$
$$1 + 1 + 1 + 1 + 1 = 5$$
$$1 + 1 + 1 + 1 + 1 + 1 = 6$$
$$1 + 1 + 1 + 1 + 1 + 1 + 1 = 0$$

In other words, if you add 1 to itself repeatedly, you eventually cycle back to 0.

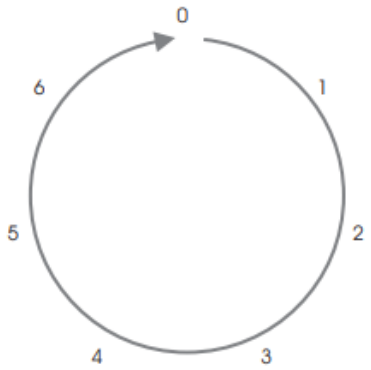

Figure 1: a cyclic group of order 7

Notice that 3 also generates $\mathbb{Z}_7$:

$$3+3=6$$
$$3+3+3=2$$
$$3+3+3+3=5$$
$$3+3+3+3+3=1$$
$$3+3+3+3+3+3=4$$
$$3+3+3+3+3+3+3=0$$

The "same" group can be written using multiplicative notation this way:

$$\mathbb{Z}_7 = \{1, a, a^2, a^3, a^4, a^5, a^6\}.$$

In this form, a is a generator of $\mathbb{Z}_7$. It turns out that in $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, every nonzero element generates the group. On the other hand, in $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, only 1 and 5 generate. □

1.3 Some Lemmas and Proofs

Lemma 1.1 *Let $G = \langle g \rangle$ be a finite cyclic group, where g has order n. Then the powers $\{1, g, \ldots, g^{n-1}\}$ are distinct.*

Proof. Since g has order n, $g, g^2, \ldots, g^{n-1}$ are all different from 1.

Now to show that the powers $\{1, g, \ldots, g^{n-1}\}$ are distinct. Suppose $g^i = g^j$ where $0 \leq j < i < n$. Then $0 < i - j < n$ and $g^{i-j} = 1$, contrary to the preceding observation. Therefore, the powers $g, g^2, \ldots, g^{n-1}$ are distinct. □

Lemma 1.2 *Let $G = \langle g \rangle$ be infinite cyclic. If m and n are integers and $m \neq n$, then $g^m \neq g^n$.*

Proof. Suppose without loss of generality that $m > n$. Now to show that $g^m \neq g^n$; suppose this is false, so $g^m = g^n$. Then $g^{m-n} = 1$, so g has finite order. This contradicts the fact that a generator of an infinite cyclic group has infinite order. Therefore, $g^m \neq g^n$. □

The next result characterizes subgroups of cyclic groups.

Theorem 1.3 *Subgroups of cyclic groups are cyclic.*

Proof. We leave out the proof!! □

Example.[Subgroups of the integers] Describe the subgroups of $\mathbb{Z}$.

Every subgroup of $\mathbb{Z}$ has the form $n\mathbb{Z}$ for $n \in Z$. For example, here is the subgroup generated by 13:

$$13\mathbb{Z} = \langle 13 \rangle = \{\ldots -26, -13, 0, 13, 26, \ldots\}.$$

2 Isomorphism

Groups that are not literally the same may be structurally the same. An example of this idea is the relation between multiplication and addition via exponentiation:

$$e^x e^y = e^{x+y}$$

Every number in $\mathbb{R}_{>0}$ has the form e^x for exactly one $x \in \mathbb{R}$, and the above equation tells us that when we write numbers in $\mathbb{R}_{>0}$ as e^x then multiplying in $\mathbb{R}_{>0}$ corresponds to adding the exponents in $\mathbb{R}$. Going the other way, every real number has the form $\ln x$ for exactly one $x > 0$, and addition of logarithm values corresponds to multiplication inside the logarithm:

$$\ln(x) + \ln(y) = \ln(xy).$$

The functions exp: $\mathbb{R} \to \mathbb{R} > 0$ and $\ln : \mathbb{R}_{>0} \to \mathbb{R}$ make the groups $\mathbb{R}_{>0}$ and $\mathbb{R}$ look the same: they are each a *bijective* way of passing between the two groups that turn the operation in one group into the operation in the other group (e.g. doubling in $\mathbb{R}$ is like squaring in $\mathbb{R}_{>0}$).

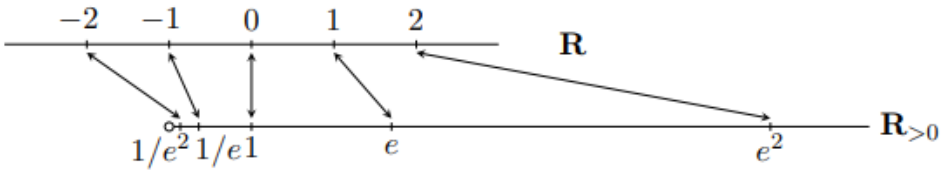

Figure 2: The groups $\mathbb{R}$ and $\mathbb{R}_{>0}$, linked by $x \mapsto e^x$ and $y \mapsto \ln y$.

Definition 2.1 *An isomorphism $f : G \to \tilde{G}$ between two groups G and $\tilde{G}$ is a bijective homomorphism. When there is an isomorphism between G and $\tilde{G}$, the groups are called isomorphic and we write $G \cong \tilde{G}$.*

An isomorphism between two groups is a dictionary that lets us translate elements and operations from one group to the other without losing essential information. For example, we'll see that all cyclic groups of the same size are isomorphic, so if we understand one cyclic group then we can usually transfer that understanding to all the other cyclic groups of the same size. Isomorphisms are the way to express how two groups that are different are nevertheless basically the same.

2.1 Examples of Isomorphisms

Example 1. The exponential function exp: $\mathbb{R} \to \mathbb{R}_{>0}$, sending each $x \in R$ to e^x, is an isomorphism: it is a homomorphism since $e^{x+y} = e^x e^y$ and it is a bijection since it has an inverse function, the natural logarithm.

More generally, for each $b > 0$ with $b \neq 1$ the function $f : \mathbb{R} \to \mathbb{R}_{>0}$ given by $f(x) = b^x$ is an isomorphism: it is a homomorphism since $f(x + y) = b^{x+y} = b^x b^y = f(x)f(y)$, and it is a bijection since it has $\log_b x$ as an inverse function. Figure **??** shows some corresponding elements of $\mathbb{R}$ and $\mathbb{R}_{>0}$ under this isomorphism.

Going the other way, $\log_b : \mathbb{R}_{>0} \to \mathbb{R}$ is an isomorphism: it is a homomorphism since $\log_b(xy) = \log_b x + \log_b y$, and it is a bijection since it has b^x as an inverse function.

Example. 2 The groups D_3 and S_3 are isomorphic. Evidence that they resemble each other is that both groups have order 6, three elements of order 2, and two elements of order 3 (and of course one element of order 1: the identity). To create an isomorphism from D_3 to S_3, label the vertices of an equilateral triangle as 1, 2, and 3 (see Figure **??**) so that each element of D_3 permutes the vertices and thus can be turned into an element of S_3.

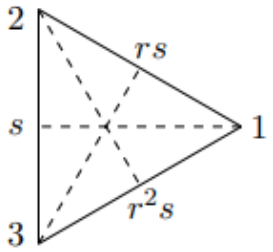

Figure 3:

Let r be a counterclockwise rotation by 120 degrees and s be the reflection across the horizontal dashed line. Then rs and r^2s are reflections across the other dashed lines. The vertex labels in the picture lead to the table below turning elements of D_3 into elements of S_3.

D_3 :	1	r	r^2	s	rs	r^2s
S_3 :	(1)	(123)	(132)	(23)	(12)	(13)

Figure 4:

The correspondence in the table is compatible with the group laws in D_3 and S_3, e.g., r

has order 3 and (123) has order 3, s has order 2 and (23) has order 2, and $sr = r^{-1}s$ while $(23)(123) = (123)^{-1}(23)$. If we let $f : D_3 \to S_3$ by the table above, it is a bijection and a tedious calculation (omitted) can verify that it is a homomorphism. Since f is a bijective homomorphism from D_3 to S_3, it is an isomorphism.