9-21-1993

Cyclic groups.

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**.

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

Examples. $\mathbb{Z}$ is an infinite cyclic group. (In fact, it is the only infinite cyclic group up to **isomorphism**.) Notice that $\mathbb{Z}$ is generated by 1 and by -1 — 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,

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

is cyclic of order 6. 1 generates, since

$$1+1=2, \quad 1+1+1=3, \quad 1+1+1+1=4, \quad 1+1+1+1+1=5, \quad 1+1+1+1+1+1=0. \square$$

Lemma. Let $G = \langle g \rangle$ be a finite cyclic group, where g has order n.

1. n is the smallest positive power of g such that $g^n = 1$.
2. The powers $\{1, g, \ldots, g^{n-1}\}$ are distinct.

Proof. Since g has order n, n is the smallest positive power of g such that $g^n = 1$.

To prove the second statement, note that the first says that $g^m \neq 1$ for $0 < m < n$. Hence, 1 is certainly different from $\{g, \ldots, g^{n-1}\}$.

It remains to show that the powers $\{1, g, \ldots, g^{n-1}\}$ are distinct. Suppose $g^i = g^j$ where $0 \le j < i < n$. Then $g^{i-j} = 1$, making $i - j$ is a positive number smaller than n which kills g. This contradicts statement 1.

Therefore, the powers $\{1, g, \ldots, g^{n-1}\}$ are distinct. $\square$

Lemma. 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. One of m, n is larger — suppose without loss of generality that $m > n$. I want 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, $g^m \neq g^n$. $\square$

Theorem. Every subgroup of a cyclic group is cyclic.

Proof. This proof will make crucial use of the **Division Algorithm**.

Let $G = \langle g \rangle$ be a cyclic group, where $g \in G$. Let $H < G$. If $H = \{1\}$, then H is cyclic with generator 1. So assume $H \neq \{1\}$.

To show H is cyclic, I must produce a generator for H. What is a generator? It is an element whose powers make up the group. *A thing should be smaller than things which are "built from" it.* Since elements of the subgroup are "built from" the generator, the generator should be the "smallest" thing in the subgroup.

What should I mean by "smallest"?

Well, G is cyclic, so everything in G is a power of g. With this discussion as motivation, let m be the smallest positive integer such that $g^m \in H$.

Why is there such an integer m? Well, H contains something other than $1 = g^0$, since $H \neq \{1\}$. That "something other" is either a positive or negative power of g. If H contains a positive power of g, it must contain a *smallest* positive power, by well ordering.

On the other hand, if H contains a negative power of g — say g^{-k}, where $k > 0$ — then $g^k \in H$, since H is closed under inverses. Hence, H again contains positive powers of g, so it contains a *smallest* positive power, by well ordering.

So I have g^m, the smallest positive power of g in H. I claim that g^m generates H. I must show that every $h \in H$ is a power of g^k. Well, $h \in H < G$, so at least I can write $h = g^n$ for some n. But by the Division Algorithm, there are unique integers q and r such that

$$n = mq + r, \quad \text{where} \quad 0 \le r < m.$$

It follows that

$$g^n = g^{mq+r} = (g^m)^q \cdot g^r, \text{ so } h = (g^m)^q \cdot g^r, \text{ or } g^r = (g^m)^{-q} \cdot h.$$

Now $g^m \in H$, so $(g^m)^{-q} \in H$. Hence, $(g^m)^{-q} \cdot h \in H$, so $g^r \in H$. However, g^m was the *smallest positive power of g lying in H*. Since $g^r \in H$ and $r < m$, the only way out is if $r = 0$. Therefore, $n = qm$, and $h = g^n = (g^m)^q \in \langle g^m \rangle$.

This proves that g^m generates H, so H is cyclic. □

Example. What are the subgroups of $\mathbb{Z}_{15}$? Since the order of a subgroup must divide the order of the group, there may be subgroups of order 1, 3, 5, or 15. The first is the identity, and the last is the entire group.

In fact, there is one subgroup of order 3, namely

$$\langle 5 \rangle = \{0, 5, 10\}.$$

Likewise,

$$\langle 3 \rangle = \{0, 3, 6, 9, 12\}$$

is the unique subgroup of order 5. □

Example. In case $G = \mathbb{Z}$, the proof of the theorem shows that every subgroup has the form $n\mathbb{Z}$ for $n \in \mathbb{Z}$.

For example,

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

is a subgroup of $\mathbb{Z}$. □

Lemma. Let G be a group, and let $g \in G$ have order m. Then $g^n = 1$ if and only if $m \mid n$.

Proof. If $m \mid n$, then $n = mq$ for some q, so $g^n = (g^m)^q = 1$.

Conversely, suppose that $g^n = 1$. By the Division Algorithm,

$$n = mq + r \quad \text{where} \quad 0 \le r < n.$$

Hence,

$$g^n = g^{mq+r} = (g^m)^q g^r \text{ so } 1 = g^r.$$

Since m is the smallest positive power of g which equals 1, and since $r < n$, this is only possible if $r = 0$. Therefore, $n = qm$, i.e. $m \mid n$. □

Thus, the order of an element is the smallest power which kills the element in two ways. It is "smallest" in the sense of being numerically smallest, but it is also smallest in the sense that it divides any power which kills the element.

Proposition. Let $G = \langle g \rangle$ be a cyclic group of order n, and let $m < n$. Then $\langle g^m \rangle$ has order $\dfrac{n}{(m,n)}$.

Proof. Since $(m, n) \mid m$, it follows that $\dfrac{m}{(m,n)}$ is an integer. Therefore, $n \mid \dfrac{mn}{(m,n)}$, and

$$(g^m)^{\frac{n}{(m,n)}} = 1$$

by the last lemma. Thus, $\dfrac{n}{(m, n)}$ is a power which kills g^m.

Now suppose that $(g^m)^k = 1$. By the preceding lemma, $n \mid mk$, so

$$\frac{n}{(m, n)} \mid k \cdot \frac{m}{(m, n)}.$$

However, $\left(\dfrac{n}{(m, n)}, \dfrac{m}{(m, n)}\right) = 1$, so $\dfrac{n}{(m, n)} \mid k$. Thus, $\dfrac{n}{(m, n)}$ divides any power of g^m which is 1, so it is the order of g^m. □

Example. Find the order of the element $12 \in \mathbb{Z}_{15}$.

$(12, 15) = 3$, so the order of 12 is $\dfrac{15}{3} = 5$. □

Example. Consider the group

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(m, n) \mid m \in \mathbb{Z}_2, n \in \mathbb{Z}_3\}.$$

The operation is componentwise addition:

$$(m, n) + (m', n') = (m + m', n + n').$$

It is routine to verify that this is a group, the **direct product** of $\mathbb{Z}_2$ and $\mathbb{Z}_3$.

The element $(1, 1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ has order 6:

$$\begin{aligned}
(1, 1) + (1, 1) &= (0, 2), \\
(1, 1) + (0, 2) &= (1, 0), \\
(1, 1) + (1, 0) &= (0, 1), \\
(1, 1) + (0, 1) &= (1, 2), \\
(1, 1) + (1, 2) &= (0, 0).
\end{aligned}$$

Hence, $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic of order 6. More generally, if $(m, n) = 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic of order mn. □