Cyclic groups (D+F 2.3)

Recall from the homework that a group G is cyclic if $\exists\ x \in G$ s.t. $G = \{x^n \mid n \in \mathbb{Z}\}$.

In this case, we write $G = \langle x \rangle$ and say G is generated by x.

(Note that a cyclic group may have more than one generator.
e.g. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.)

Prop: If $G = \langle x \rangle$, then

- if $|x| = n < \infty$, $1, x, x^2, \ldots, x^{n-1}$ are all the distinct elements of G.
- if $|x| = \infty$, the distinct elements of G are $\{x^n \mid n \in \mathbb{Z}\}$.

Pf: If $|x| = \infty$, then $G = \{x^n \mid n \in \mathbb{Z}\}$ by definition, and all the elements are distinct by HW.

If $|x| = n$, then $\{1, x, \ldots, x^{n-1}\}$ are all distinct by HW #1.

For any $a \in \mathbb{Z}$, we can write $a = bn + r$, $r \in \{0, \ldots, n-1\}$,

so $x^a = \underbrace{x^{bn}}_{=1} x^r = x^r \in \{1, x, \ldots, x^{n-1}\}$, so $\langle x \rangle = G = \{1, \ldots x^{n-1}\}$. □

Cor: If $G = \langle x \rangle$, then $|G| = |x|$.

In fact, any two cyclic groups of the same order are isomorphic:

Thm:

1.) If $n \in \mathbb{Z}^+$ and $\langle x \rangle$ and $\langle y \rangle$ are cyclic groups of order n, then $\varphi : \langle x \rangle \to \langle y \rangle$ defined $x^k \mapsto y^k$ is well-defined and an isomorphism.

2.) If $\langle x \rangle$ is an infinite cyclic group, the map $\varphi : \mathbb{Z} \to \langle x \rangle$ defined $k \mapsto x^k$ is well-defined and an isomorphism.

Pf: 1.) First we need to show φ is well-defined. That is, if $x^r = x^s$, then $\varphi(x^r) = \varphi(x^s)$.

If $x^r = x^s$, then $x^{r-s} = 1$. But $r - s = \ell + mn$, some $\ell \in \{0, \dots, n-1\}$, and $m \in \mathbb{Z}$.

So $x^{r-s} = x^{\ell} \underbrace{x^{mn}}_{(x^n)^m} = x^{\ell} = 1$. Since $1, x, \dots, x^{n-1}$ are all distinct, $\ell = 0$. Thus $n \mid (r-s)$.

So $y^{r-s} = y^{mn} = 1 \Rightarrow y^r = y^s$, so φ is well-defined.

$\varphi(x^a x^b) = \varphi(x^{a+b}) = y^{a+b} = y^a y^b = \varphi(x^a)\varphi(x^b)$, so it's

a homomorphism, w/ obvious inverse $\varphi^{-1}: \langle y \rangle \to \langle x \rangle$ defined $y^k \longmapsto x^k$.

2.) If $\langle x \rangle$ is infinite cyclic, note that $\varphi: \mathbb{Z} \to \langle x \rangle$ is clearly well-defined since there's no ambiguity in the way we express an integer.

If $a, b \in \mathbb{Z}$, then $\varphi(a+b) = x^{a+b} = x^a x^b = \varphi(a)\varphi(b)$, so it's a homomorphism. It's surjective since all elements can be expressed as x^k, $k \in \mathbb{Z}$. It's injective since we already showed $x^a \neq x^b$ if $a \neq b$. □

Notation: Let $\mathbb{Z}_n$ denote the cyclic group of order n, written multiplicatively.

Cor: Up to isomorphism, $\mathbb{Z}_n$ is the unique cyclic group of order n and $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.

In order to determine which elements of a cyclic group generate the whole group, we first determine how the order of a power of an element relates to the order of the original element.

Prop: Let G be a group, $x \in G$, $a \in \mathbb{Z} - \{0\}$.

1.) If $|x| = \infty$ then $|x^a| = \infty$.

2.) If $|x| = n < \infty$, then $|x^a| = \frac{n}{(n,a)}$

((n,a) = gcd of n and a)

Pf: 1.) Follows from definition.

2.) Let $\ell = (n,a)$. Then $n = n'\ell$ and $a = a'\ell$, where n' and a' are relatively prime.

Then $(x^a)^{\frac{n}{\ell}} = (x^n)^{a/\ell} = (x^n)^{a'} = 1$. Thus,

$$|x^a| \,\Big|\, \tfrac{n}{\ell} = n'.$$

But $n \mid a \cdot |x^a| \Rightarrow n' \mid a'|x^a| \Rightarrow n' \mid |x^a|$

$\Rightarrow |x^a| = n' = \frac{n}{(n,a)}$. $\square$

What does this mean?

- If $G = \langle x \rangle$ is finite of order n, then $y \in G$ generates $G \iff |y| = n$.

  So if $y = x^a$, $|y| = n \iff n = \frac{n}{(n,a)} \iff (n,a) = 1 \iff n$ and a are rel. prime.

- If $G = \langle x \rangle$ is infinite, then $y = x^a$ generates $G \iff y^b = x$ for some $b \in \mathbb{Z} \iff ab = 1$ for some $b \iff a = \pm 1$.

  So $G = \langle x^a \rangle \iff a = 1$ or -1.

Subgroups of cyclic groups

It turns out, all the subgroups of a cyclic group are also cyclic:

In the finite case, consider $\mathbb{Z}_n = \langle x \rangle$. Let $H \leq \mathbb{Z}_n$. Let a be the minimum (nonneg) integer s.t. $x^a \in H$.

Then $\langle x^a \rangle \leq H$. Suppose $x^b \in H$. Then $b = qa + r$, some q, and $0 \leq r < a$.

Thus $x^b (x^a)^{-q} = x^{qa} x^r x^{-qa} = x^r \in H$, but by minimality of a, $r = 0$, so $a \mid b$. Thus, $H \leq \langle x^a \rangle$, so $H = \langle x^a \rangle$.
That is, any subgroup of $\mathbb{Z}_n$ is cyclic.

If G is an infinite cyclic group, a nearly identical argument shows that if $H \leq G$, H is generated by x^a, where a is the least positive exponent s.t. $x^a \in H$.

That is, H is also cyclic.

Since all nontrivial elts of an infinite cyclic group have infinite order, all the subgroups must have infinite order.

However, if $G = \langle x \rangle$ is finite, we have the following:

Thm: If $G=\langle x\rangle$ is finite of order n, then for each positive integer a dividing n, there is a unique subgroup of G of order a.

(Note: by Lagrange's Theorem, these are in fact the only subgroups of G.)

Pf: Let a divide n. Then if $d=\frac{n}{a}$, we have $|x^d| = \frac{n}{(n,d)} = \frac{n}{d} = a$

so $|\langle x^d\rangle| = a$, which proves existence.

If $H \leq G$ is another subgroup of order a, we know $H=\langle x^b\rangle$, some b, s.t. $a = |x^b| = \frac{n}{(n,b)}$.

$\Rightarrow (n,b) = \frac{n}{a} = d. \Rightarrow d \mid b \Rightarrow de = b$, some e.

$\Rightarrow x^b = (x^d)^e \in \langle x^d\rangle \Rightarrow \langle x^b\rangle \leq \langle x^d\rangle$, but they have the same order, so they're equal. □

Ex: 1.) The subgroups of $\mathbb{Z}/12\mathbb{Z}$ are of orders $1,2,3,4,6,12$.

They are $\bar{0}=\langle\bar{0}\rangle, \langle\bar{6}\rangle, \langle\bar{4}\rangle, \langle\bar{3}\rangle, \langle\bar{2}\rangle, \langle\bar{1}\rangle = \mathbb{Z}/12\mathbb{Z}$, respectively.

2.) The subgroups of $\mathbb{Z}$ are all of the form $\langle m\rangle$, where m is nonnegative.