Example: Recall $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ is a group with multiplication. Let $H = \{1, -1, i, -i\}$. Then $H < \mathbb{C}^*$ is a subgroup. In fact, it has table:

	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1.

Compare this to $\mathbb{Z}_4$; with $+$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

note these tables are "the same" if we set $0 = 1$, $1 = i$, $2 = -1$, and $3 = -i$. We will make this notion of "sameness" precise later.

Chapter 4 Cyclic groups.

There are times when a single element of a group G can determine an entire subgroup $H \subset G$.

Example: Consider the subgroup $3\mathbb{Z} \subset \mathbb{Z}$. As a set, it's $\{\ldots, -6, -3, 0, 3, 6, \ldots\} = 3\mathbb{Z}$. We can see that in some way, the entire set $3\mathbb{Z}$ is determined by the single element "3". Specifically, every element $m \in 3\mathbb{Z}$ is a multiple of 3, ie

$$m = 3k \text{ for some } k$$
$$= \underbrace{3 + 3 + \ldots + 3}_{k \text{ times}}.$$

Example: If $H = \{2^n \mid n \in \mathbb{Z}\}$, then $H \subset \mathbb{C}^*$ is a subgroup. For example, we can check that

$$a \in H \text{ and } b \in H \Rightarrow ab \in H, \text{ since}$$

$$2^m \in H \text{ and } 2^n \in H \Rightarrow 2^m \cdot 2^n = 2^{m+n} \in H.$$

Then similar to above, every element of H is "determined" by 2, in the sense that for all $a \in H$, a is an iterated product of twos (or an iterated product of inverses of 2).

Theorem: If G is a group and g is any element of G, then the set

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$$

is a subgroup of G. Moreover, $\langle g \rangle$ is the smallest subgroup of G containing g.

Proof: The set $\langle g \rangle$ contains e since $g^0 = e$.
If a, b are elements of $\langle g \rangle$ then $a = g^n$ and $b = g^m$ for some $m, n \in \mathbb{Z}$, so $ab = g^{n+m} \in \langle g \rangle$.
Last, if $g^n \in \langle g \rangle$ then $(g^n)^{-1} = g^{-n} \in \langle g \rangle$ as well, so it is a subgroup.
Finally, if $H \subset G$ is a subgroup containing g, then H must contain every power of g by the fact that it is closed under the group operation. Therefore $\langle g \rangle \subseteq H$, in this sense $\langle g \rangle$ is the smallest subgroup containing g.

Definition: The set $\langle a \rangle$ is called the cyclic subgroup generated by a. In the special case that G contains an element a such that $G = \langle a \rangle$, then G is called a cyclic group. We call ~~g~~ 'a' a generator of G.

Theorem: Every cyclic group is abelian.

Proof: Suppose G is cyclic with generator g, and let $a, b \in G$ be given.
Then $a = g^n$ and $b = g^m$ for some m, n. Therefore

$$ab = g^n \cdot g^m = g^{n+m} = g^{m+n} = g^m \cdot g^n = ba.$$

Corollary: There are many non-cyclic groups, for example the symmetries of a triangle is a non-cyclic group, since that group is nonabelian.

Chapter 4.1 Subgroups of cyclic groups

What are the subgroups of a cyclic group?

Theorem: Every subgroup of a cyclic group is cyclic

Proof: Let G be a cyclic group generated by a, and suppose that H is a subgroup of G.

First, if $H = \{e\}$ then H is trivially cyclic. So suppose that H contains some $g \neq e$. Write g as a power of a, which we can do since G is cyclic: $g = a^n$.

We can assume that $n > 0$, because if $n < 0$ then we can take a^{-1} as a generator of G and then

$a^n = (a^{-1})^{-n} = g$, so g is a positive power of the new generator. Let m be the smallest natural number such that $a^m \in H$ — such a number exists since $a^n = g \in H$, by the Well-Ordering Principle.

Claim: $h = a^m$ is a generator for H, we need to show that every $h' \in H$ can be written as a power of h. Write $h' = a^k$ for some k, this is possible since $h' \in H \subset G$. Since m was chosen to be minimal, $m \leq k$ and we can divide k by m

to get $k = mq + r$ for $0 \le r < m$. Therefore

$$a^k = a^{mq+r} = (a^m)^q a^r = h^q a^r,$$

so that $a^r = a^k h^{-q}$. But then since $a^k \in H$ and $h \in H$, we must have $a^r \in H$; this contradicts minimality of m unless $r = 0$. Consequently $r=0$ and $k = mq$, so

$$h' = a^k = a^{mq} = h^q$$

so that h' is a power of h, and H is cyclic and generated by h.

<u>Corollary</u>: The only subgroups of $\mathbb{Z}$ are $n\mathbb{Z}$ for $n = 0, 1, 2, 3, \ldots$

<u>Proposition</u>: If G is a finite cyclic group, say of order n, then every generator $a \in G$ satisfies $a^k = e$ if and only if n divides k.

<u>Proof</u>: Suppose $\langle a \rangle = G$ and $a^k = e$, and $|G| = n$. Write $k = nq + r$ where $0 \le r < n$, and then write

$$e = a^k = a^{nq+r} = (a^{nq}) a^r = e a^r = a^r,$$

where we know $a^n = e$ since G is cyclic and a is a generator.

The smallest n such that $a^n = e$ is called the <u>order</u> of the element a. If there's no such n, we say a is of infinite order. We write $|a| = n$ and $|a| = \infty$ respectively.

<u>Example</u>: Generators of cyclic subgroups are not unique. For example,

$$\mathbb{Z}_6 = \langle 1 \rangle \quad \text{and} \quad \mathbb{Z}_6 = \langle 5 \rangle, \text{ since}$$

$$5+5 \equiv 4 \bmod 6$$
$$5+5+5 \equiv 3 \bmod 6$$
$$5+5+5+5 \equiv 2 \bmod 6$$
$$5+5+5+5+5 \equiv 1 \bmod 6.$$

On the other hand not every element of a cyclic group is a generator. For example,

$$\langle 2 \rangle = \{0, 2, 4\} \subset \mathbb{Z}_6.$$

<u>Example</u>: $U(9)$ is cyclic. We compute

$$U(9) = \{\cancel{0}, 1, 2, \cancel{3}, 4, 5, \cancel{6}, 7, 8, \cancel{9}\}$$
$$= \{1, 2, 4, 5, 7, 8\}.$$

And then we check:

$$2^0 = 1 \qquad 2^3 = 8$$
$$2^1 = 2 \qquad 2^4 = 7$$
$$2^2 = 4 \qquad 2^5 = 5$$

But $m=n$ is the smallest positive integer s.t. $a^m=e$, so this forces $r=0$. Therefore $k=nq$ and $n|k$.

On the other hand, if $n|k$ then $k=ns$ for some s, and

$$a^k = a^{ns} = (a^n)^s = e.$$

Theorem: Let G be a cyclic group of order n and suppose $a \in G$ is a generator of G. If $b=a^k$, then the order of b is $\dfrac{n}{\gcd(n,k)}$.

Proof: The order of b is the smallest m s.t. $b^m=e$. By the previous proposition, $(a^k)^m = b^m = e$ if and only if km is divisible by n. So, we are seeking the smallest integer km s.t. $n|km$. Equivalently,

$$\frac{n}{\gcd(n,k)} \text{ divides } \frac{km}{\gcd(n,k)}$$ (just take out the biggest factor common to n & k)

But $\dfrac{n}{\gcd(n,k)}$ and $\dfrac{k}{\gcd(n,k)}$ are relatively prime since we have factored the gcd out of each.

So if $\frac{n}{\gcd(n,k)}$ divides $m\left(\frac{k}{\gcd(n,k)}\right)$ then it must divide m. The smallest m divisible by $\frac{n}{\gcd(n,k)}$ is $\frac{n}{\gcd(n,k)}$ itself, which proves the theorem.

<u>Corollary</u>: The generators of $\mathbb{Z}_n$ are exactly the elements $r \in \mathbb{Z}_n$ with $\gcd(r,n)=1$.

<u>Proof</u>: We take $1 \in \mathbb{Z}_n$ as the generator. Then consider $r = \underbrace{1+1+\cdots+1}_{r \text{ times}}$. (or 1^r in multiplicative notation).

The previous theorem says that the order of $r = \underbrace{1+1+\cdots+1}_{r \text{ times}}$ is $\frac{n}{\gcd(n,k)}$. The element r will be a generator if and only if its order is n, this happens exactly when $\gcd(n,r)=1$.

<u>Example</u>: $\mathbb{Z}_8$ has many generators, namely $\{1, 3, 5, 7\}$, each being relatively prime to 8. So a cyclic group can have many generators, and we can list them.

<u>Question</u>: How many generators does a cyclic group have? (Good question for future "research")

Example: The unit circle in $\mathbb{C}^*$ is a subgroup.

It is denoted by

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\},$$

i.e. $S^1 = \{a+ib \in \mathbb{C} \mid a^2+b^2 = 1\}$.

To show that it's a subgroup, observe that:

(i) The identity $1 \in S^1$

(ii) If $z \in S^1$ and $w \in S^1$, then

$$|zw| = |z| \cdot |w| = 1 \cdot 1 = 1,$$

so $zw \in S^1$

(iii) If $z = a+ib \in S^1$, then $z^{-1} = \dfrac{a-ib}{a^2+b^2}$ and

$$|z^{-1}| = \frac{1}{a^2+b^2}|a-ib| = \frac{1}{a^2+b^2} \cdot (a^2+b^2) = 1,$$ so

$z^{-1} \in S^1$.

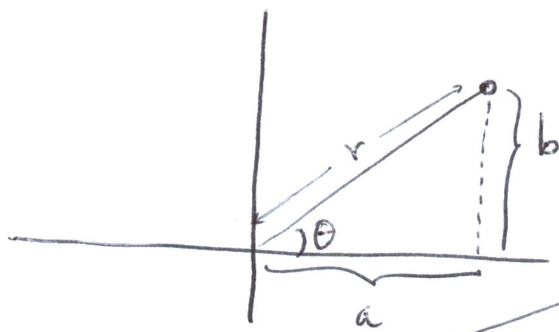
Next day we will examine cyclic subgroups of S^1.

MATH 2020, § 4.2.

<u>Definition</u>: The solutions to $z^n = 1$ are called the <u>n^{th} roots of unity</u>.

<u>Example</u>: Find the solutions to $z^3 = 1$.

<u>Solution</u>: If $z = a + ib$, then thinking in the complex plane:



the book calls this $\mathrm{cis}(\theta)$

we see that $z = r(\cos\theta + i\sin\theta)$, where $r = \sqrt{a^2+b^2}$ and θ is the <u>argument</u> of $z = a+ib$. Then we have the following <u>fact</u>:

If $z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$

and $z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$

then $\quad z_1 z_2 = r_1 r_2(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2))$ i.e., multiplying complex numbers multiplies their lengths and adds their angles. So if $z = r(\cos\theta + i\sin\theta)$ then

$$1 = z^3 \Rightarrow 1 = r^3(\cos(3\theta) + i\sin(3\theta))$$

$\Rightarrow r=1$ and $\theta = \frac{2k\pi}{3}$, for $k=0,1,2$. Since then, for example if $k=1$

$$1\cdot\left(\cos\left(3\cdot\left(\tfrac{2\pi}{3}\right)\right) + i\sin\left(3\cdot\left(\tfrac{2\pi}{3}\right)\right)\right)$$
$$= \cos(2\pi) + i\sin(2\pi) = 1.$$

In this case, the roots are

$k=0$: $\quad \cos(0) + i\sin(0) = 1$

$k=1$ $\quad \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$

$k=2$ $\quad \cos\left(\frac{4\pi}{3}\right) + i\sin\left(\frac{4\pi}{3}\right) = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$

In general, we have De Moivre's theorem.

Theorem: If $z = r(\cos\theta + i\sin\theta)$ then
$$z^n = r^n(\cos(n\theta) + i\sin(n\theta))$$

and as a consequence we get:

Proposition: If $n \geq 1$ then the n^{th} roots of unity (i.e. the solutions to $z^n = 1$) are:

$$z = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right)$$

where $k = 0, 1, 2, \ldots, n-1$. Furthermore, these roots form a cyclic group of order n.

Proof: By de Moivre's theorem,

$$z^n = 1 \Rightarrow 1 = r(\cos(n\theta) + i\sin(n\theta))$$

$$\Rightarrow r = 1 \text{ and } \theta = \frac{2\pi k}{n} \text{ for } k = 0, 1, \ldots, n-1.$$

These solutions are all distinct since the values of $\frac{2\pi k}{n}$ are between 0 and 2π. This set constitutes all of the roots since a polynomial of degree n can have at most n roots (we will actually prove this later).

These roots form a cyclic group since, for $0 \le k < n$ the element

$$\cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right) = \left(\cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)\right)^k, \text{ by}$$

de Moivre's theorem.

A generator for the group of n^{th} roots of unity is called a primitive n^{th} root of unity.

Remark: So, in some cases the solutions to polynomial equations can form a group! This observation forms the backbone of several large fields of study, for example, the study of elliptic curves. (Solutions to $y^2 = x^3 + ax + b$) (The group operation is not multiplication in that case.)

Chapter 4 problems (§4.4)

1, 2, 3 (a)-(d), (g)-(m), 6, 11, 12, 16, 20, 21, 24-31.