Day 4 June 3, 2024

Cyclic subgroups

Given any element $g \in G$, we denote by $\langle g \rangle$ the smallest subgroup of G which contains g.

Thm Let G be a group. For any $g \in G$,

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

Def. We call $\langle g \rangle$ the cyclic subgroup generated by g. If $G = \langle g \rangle$, we say that G is a cyclic group. In this case, we call g a generator for G.

(Proof.) Note that $g \in \langle g \rangle$ by def'n.

B/c $\langle g \rangle$ is a subgroup, $g^{-1} \in \langle g \rangle$ & $g^0 \in \langle g \rangle$.

Suppose $g^m \in \langle g \rangle$, for some $m \in \mathbb{Z}$.

Then $g^{m+1} = g \cdot g^m \in \langle g \rangle$

& $g^{m-1} = g^{-1} \cdot g^m \in \langle g \rangle$.

So $g^k \in \langle g \rangle$ $\forall k \in \mathbb{Z}$, by induction.

Check: $\{ g^k \mid k \in \mathbb{Z} \}$ is a subgroup of G.

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

Thm. Every cyclic group is abelian.

(Proof.) Exercise. ∎

Thm. Every subgroup of a cyclic group is cyclic.

(Proof.) Let $G = \langle g \rangle$ be a cyclic subgroup and let $H \leq G$ be a subgroup.

If H is trivial, then $H = \langle e \rangle$ and we're done.

Otherwise, pick a nontrivial elt $h \in H$.

Then $h = g^n$, for some $0 \neq n \in \mathbb{Z}$ and $H \supseteq \langle h \rangle$.

Since $g^{-n} = h^{-1} \in \langle h \rangle \subseteq H$, we can assume $n > 0$.

Let m be the smallest pos. int. s.t. $g^m \in H$.

Claim: $H = \langle g^m \rangle$.

To prove this, pick $a \in H$. NTS: $a = (g^m)^q$, for some $q \in \mathbb{Z}$. Since $a \in G$, $\exists\, k \in \mathbb{Z}$ s.t.

$$a = g^k.$$

By the division algorithm, $\exists\, q \in \mathbb{Z}$ & $0 \leq r < m$ s.t. $k = mq + r$. So

$$a = g^k = g^{mq+r} = g^{mq} \cdot g^r = (g^m)^q \cdot g^r.$$

Then $g^r = a(g^m)^{-q} \in H$, since $a \in H$ & $g^m \in H$.

If $r \neq 0$, then it's a pos. int. smaller than m, a contradiction. So $r = 0$.

But then $a = (g^m)^q$, as desired.

So $H = \langle g^m \rangle$. ∎

Corollary. Every subgroup of $\mathbb{Z}$ has the form $n\mathbb{Z}$, for some $n \in \mathbb{Z}$.

Orders of elements

Given $g \in G$, if the subgroup $\langle g \rangle \leq G$ has finite order, then the order of g is $|g| := |\langle g \rangle|$.
Otherwise $|g| := \infty$.

defined to be equal to

Thm. Let G be a cyclic group generated by g with finite order n. For any $1 \leq k \leq n$,

$$|g^k| = n/d,$$

where $d = \gcd(n,k)$.

(Proof.)

Fact: $g^m = e$ iff n divides m.
Proof of fact is very similar to that of previous thm.

Now $|g^k|$ is the smallest integer m such that

$$e = (g^k)^m = g^{km}.$$

Equivalently, m is the smallest pos. int. s.t. n divides km.

$$n \mid (km) \iff (n/d) \mid (k/d)\, m,$$

where $d = \gcd(n,k)$. Now n/d & k/d are coprime, so $(n/d) \mid m$.
The smallest pos. int. divisible by n/d is n/d.
So $|g^k| = m = n/d$. ∎

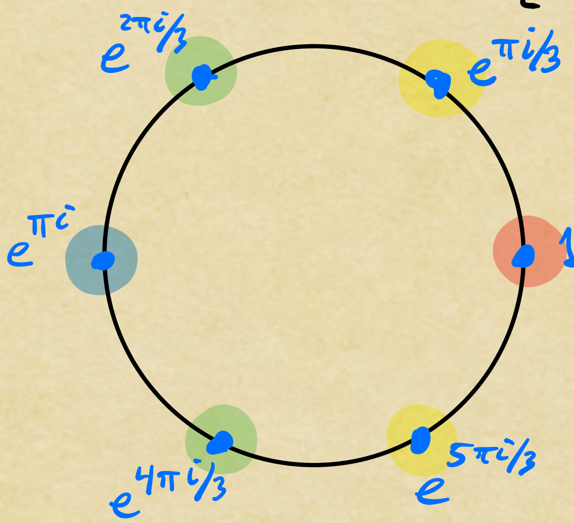
Corollary. The generators of $\mathbb{Z}_n$ are those integers $1 \leq k < n$ s.t. $\gcd(n,k) = 1$.

Cyclic subgroups of $\mathbb{C}^* := \mathbb{C} - \{0\}$

How many elements of finite order are there in $\mathbb{R}^*$, $\mathbb{Q}^*$? Just two: $\{\pm 1\}$.

Solutions to the equation $z^n - 1 = 0$ are called n^{th} roots of unity. These are given by

$$R(n) = \{ e^{2\pi i k/n} \mid 0 \leq k \leq n-1 \}.$$



Check: $R(n)$ is a cyclic subgroup of $\mathbb{C}^*$ gen'd by $e^{2\pi i/n}$.

Not all n^{th} roots of unity have order n. Those which do are called primitive n^{th} roots of unity:

$$P(n) = \{ e^{2\pi i k/n} \mid 0 \leq k \leq n-1, \ \gcd(n,k) = 1 \}.$$

If $\zeta \in R(n)$ has order d, then $\zeta \in P(d)$. Then

$$R(n) = \bigsqcup_{d \mid n} P(d)$$

$\boxed{\operatorname{cis}(\theta) = e^{i\theta}}$

<u>Fact</u>. $G = \bigcup_{n \in \mathbb{N}} R(n)$ is a subgroup of $\mathbb{C}^*$.