Some of the results on hom's and subgroups

Tuesday, June 29, 2021 3:29 PM

We have discussed group homomorphisms and subgroups, and proved many of their basic properties. Here are some of the results that we have proved:

1. $\forall g \in G$, $C_G(g) := \{x \in G \mid g \cdot x = x \cdot g\} \leq G$ (We write $H \leq G$ if H is a subgroup of G.)

2. $Z(G) := \{g \in G \mid \forall x \in G, g \cdot x = x \cdot g\}$.

3. Suppose $H \leq G$. Then $e_G \in H$ and $x, y \in H \Rightarrow x \cdot y^{-1} \in H$.

4. Suppose $H \subseteq G$ and $H \neq \emptyset$. Then if for every $x, y \in H$, $x \cdot y^{-1} \in H$, then $H \leq G$. (subgroup criterion)

5. If $f: G \to K$ is a group homomorphism, then

$$\ker f \leq G \text{ and } \operatorname{Im} f \leq K.$$

6. If $f: G \to K$ is a group homomorphism, then $f(e_G) = e_K$ and $f(g^{-1}) = f(g)^{-1}$ for every $g \in G$.

7. For every $g \in G$, $f: \mathbb{Z} \to G$, $f(n) := g^n$ is a group homomorphism.

Subgroups usually help us construct G little-by-little and understand

Subgroup generated by a subset

Tuesday, June 29, 2021 3:29 PM

For a non-empty subset X of a group G, there is the smallest subgroup of G which contains. This subgroup is called the subgroup generated by X and it is denoted by $\langle X \rangle$.

__Lemma.__ Suppose $(G, \cdot)$ is a group and X is a non-empty subset of G. Then there is a unique subgroup H of G such that the following statements hold.

(1) $X \subseteq H$, and (2) If $K \leq G$ and $X \subseteq K$, then $H \subseteq K$.

This means H is the smallest subgroup of G which contains X.

__Pf.__ Let $\Sigma := \{K \leq G \mid X \subseteq K\}$ (the family of all subgps of G which contain X as a subset). Notice that $G \in \Sigma$, and so Σ is not empty. Since intersection of a family of subgroups is a subgroup, $\bigcap_{K \in \Sigma} K$ is a subgroup of G.

Let $H := \bigcap_{K \in \Sigma} K$. Then:

$$K \leq G, X \subseteq K \Rightarrow K \in \Sigma \Rightarrow H \subseteq K, \text{(I)} \text{ and}$$

$$\forall K \in \Sigma, X \subseteq K \Rightarrow X \subseteq \bigcap_{K \in \Sigma} K \Rightarrow X \subseteq H. \text{(II)}$$

Cyclic groups

Tuesday, June 29, 2021 3:29 PM

By (I) and (II), we see that H satisfies the desired properties.

(Uniqueness) If H' satisfies the desired properties, then $H' \in \Sigma$ as $X \subseteq H'$ and $H' \leq G$. Hence $H \overset{(I)}{\subseteq} H'$. On the other hand, since H is a subgroup of G which contains X, $H' \overset{(II)}{\subseteq} H$. Thus (I) and (II) imply that $H = H'$. This completes the proof. ∎

Def. • A subgroup of $(G, \cdot)$ which is generated by one element is called a cyclic subgroup; that means $\langle \{g\} \rangle$ for some $g \in G$. Subgroup generated by $\{g\}$ is simply denoted by $\langle g \rangle$.

• A group $(G, \cdot)$ is called cyclic if $G = \langle g \rangle$ for some $g \in G$.

Lemma. Suppose $(G, \cdot)$ is a group and $g \in G$. Then

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

Pf. We have proved that $f: \mathbb{Z} \to G$, $f(n) := g^n$ is a group homomorphism. Hence $\operatorname{Im} f$ is a subgroup of G. Notice that $\operatorname{Im} f = \{ g^n \mid n \in \mathbb{Z} \}$ and $g = f(1) \in \operatorname{Im} f$. Therefore $\langle g \rangle$ is

Elements of cyclic groups

Tuesday, June 29, 2021 3:29 PM

a subset of $\{g^n \mid n\in\mathbb{Z}\}$ (because $\langle g\rangle$ is the smallest subgp of G which contains g). (I)

Next we want to show that $\{g^n \mid n\in\mathbb{Z}\}\subseteq\langle g\rangle$.

Claim 1. For every $n\in\mathbb{Z}$, $n\geq 0$, $g^n\in\langle g\rangle$.

Pf of Claim 1. We proceed by induction on n.

Base case. $n=0$. $g^0=e_G$ and e_G is in every subgroup. Hence $g^0\in\langle g\rangle$.

Induction step. $g^k\in\langle g\rangle \Rightarrow g^{k+1}\in\langle g\rangle$.

Pf of induction step.

$$\left.\begin{array}{l} g\in\langle g\rangle \\ g^k\in\langle g\rangle \\ \langle g\rangle : \text{subgp} \end{array}\right\} \Rightarrow g^k\cdot g\in\langle g\rangle \Rightarrow g^{k+1}\in\langle g\rangle.$$

Claim 2. For every $n\in\mathbb{Z}$, $n\geq 0$, $g^{-n}\in\langle g\rangle$

Pf of Claim 2. By claim 1, $g^n\in\langle g\rangle$. Hence $(g^n)^{-1}\in\langle g\rangle$, and so $g^{-n}\in\langle g\rangle$.

By Claim 1 and Claim 2, we conclude that

$$\{g^n\mid n\in\mathbb{Z}\}\subseteq\langle g\rangle. \quad \text{(II)}$$

By (I) and (II), $\langle g\rangle=\{g^n\mid n\in\mathbb{Z}\}$. ∎

Subgroups of cyclic subgroups

Tuesday, June 29, 2021 3:29 PM

<u>Ex.</u> Cyclic groups are abelian.

<u>Pf.</u> Suppose $(G,\cdot)$ is cyclic. Then $G=\langle g\rangle$ for some $g\in G$. Hence $G=\{g^n \mid n\in\mathbb{Z}\}$. For every $x,y\in G$, there are integers m and n such that $x=g^m$ and $y=g^n$. Hence

$$\left.\begin{aligned} x\cdot y &= g^m\cdot g^n = g^{m+n} \\ y\cdot x &= g^n\cdot g^m = g^{m+n} \end{aligned}\right\} \Rightarrow x\cdot y = y\cdot x.$$

Next we study subgroups of a cyclic group.

<u>Theorem.</u> Every subgroup of a cyclic group is cyclic.

<u>Pf.</u> Suppose $(G,\cdot)$ is generated by g and H is a subgroup of G. So $G=\{g^n \mid n\in\mathbb{Z}\}$. If $H=\{e_G\}$, then it is generated by e_G, and so it is cyclic! So without loss of generality, we can and will assume that $H\neq\{e_G\}$. Hence, for some $\ell\in\mathbb{Z}\setminus\{0\}$, $g^\ell\in H$. Because H is a subgroup, $(g^\ell)^{-1}\in H$. Thus $g^{-\ell}\in H$. Either $\ell>0$ or $-\ell>0$. Therefore there is a positive integer m such that $g^m\in H$. By the well-ordering principle, there is

$$s:=\min\{m\in\mathbb{Z} \mid m>0,\ g^m\in H\}.$$

Subgroups of cyclic subgroups

Tuesday, June 29, 2021 3:29 PM

Since $s \in \{m \in \mathbb{Z} \mid m > 0, g^m \in H\}$, $g^s \in H$. Because H is a subgroup of G and $g^r \in H$, $\langle g^s \rangle \subseteq H$. (I) This implies

$$\{(g^s)^k \mid k \in \mathbb{Z}\} \subseteq H, \text{ and so}$$

$$\{g^{sk} \mid k \in \mathbb{Z}\} \subseteq H. \qquad \text{(II)}$$

Claim. $H = \langle g^s \rangle$.

Pf of Claim. By (I), it is enough to show that $H \subseteq \langle g^s \rangle$.

Suppose $h \in H$. Because $H \subseteq G$, $h = g^m$ for some $m \in \mathbb{Z}$.

By long division, there are integers q and r such that

$m = sq + r$ and $0 \leq r < s$ (III) (dividing m by s).

$$\left.\begin{array}{l} \text{Then } g^m = g^{sq+r} \in H \\ g^{sq} \in H \text{ (by (II))} \end{array}\right\} \Rightarrow g^m \cdot (g^{sq})^{-1} \in H \Rightarrow g^r \in H.$$

$$\left.\begin{array}{l} \text{Notice that } s = \min\{g^m \mid m > 0, g^m \in H\} \\ r < s \text{ and } g^r \in H \end{array}\right\} \Rightarrow r \leq 0 \quad \text{(IV)}$$

By (III) and (IV), $\underline{r = 0}$. Hence $g^m = g^{sq} \in \langle g^s \rangle$. ∎

Corollary. Every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some non-negative integer n.

Exponents that give the neutral element

Tuesday, June 29, 2021 3:29 PM

Pf. Let's recall that in an additive structure, instead of g^m we write mg. Hence in an additive group $(G,+)$ the subgroup generated by g is $\{mg \mid m\in\mathbb{Z}\}$. Hence the subgroup of $\mathbb{Z}$ which is generated by n is

$$\{mn \mid m\in\mathbb{Z}\} = n\mathbb{Z}. \qquad (\mathrm{I})$$

In particular, $\langle 1\rangle = \mathbb{Z}$. Therefore $\mathbb{Z}$ is a cyclis group. Hence by the previous theorem, every subgroup of $\mathbb{Z}$ is cyclic. So if $H\le\mathbb{Z}$, then $H=\langle n\rangle$ for some $n\in\mathbb{Z}$. By (I), we obtain that $H=n\mathbb{Z}$. Notice that $n\mathbb{Z} = (-n)\mathbb{Z}$, hence $H=|n|\mathbb{Z}$ where $|n|$ is the absolute value of n. This completes the proof. $\blacksquare$

Theorem. Suppose $(G,\cdot)$ is a group. For every $g\in G$, there is a unique non-negative integer d such that for every $n\in\mathbb{Z}$

$$g^n = e_G \quad \text{if and only if} \quad d\mid n.$$

Pf. Let's recall that $f:\mathbb{Z}\to G$, $f(n):=g^n$ is a group homomorphism. Hence $\ker(f)$ is a subgroup of $\mathbb{Z}$.

Order of elements

Tuesday, June 29, 2021 3:29 PM

By the previous corollary $\ker f = d\mathbb{Z}$ for some non-negative integer d. This means

$$\{n \in \mathbb{Z} \mid g^n = e_G\} = d\mathbb{Z}.$$

Hence $g^n = e_G \iff d \mid n$. This shows the existence of such a non-negative integer. Next we show it is unique.

Suppose d' is a non-negative integer with the same property. Hence $g^{d'} = e_G$, which implies that $d \mid d'$. (I)

Because $g^d = e_G$, we conclude that $d' \mid d$. (II)

If $d=0$, then (I) implies $d'=0$; and so $d=d'$.

If $d'=0$, then (II) implies $d=0$; and so $d=d'$.

If $d \neq 0$ and $d' \neq 0$, then $d, d' > 0$, and so (I) implies $d' \geq d$ and (II) implies that $d \geq d'$. Altogether we get that $d=d'$. $\blacksquare$

Def. For $g \in G$, let d be the non-negative integer given by the previous theorem. The order of g is d if $d \neq 0$, and it is ∞ if $d=0$. The order of g is denoted by $o(g)$.

The next theorem gives us a list of distinct elements of a cyclic

List of distinct elements of a cyclic group

Tuesday, June 29, 2021 3:29 PM

subgroup.

Theorem. Suppose $(G,\cdot)$ is a group and $g\in G$. Let $d:=o(g)$.

- If $d<\infty$, then $\langle g\rangle=\{e_G, g, \ldots, g^{d-1}\}$ and $|\langle g\rangle|=d$.
- If $d=\infty$, then $g^i\neq g^j$ for $i\neq j$.

In either case, $|\langle g\rangle|=o(g)$.

Pf. Suppose $d<\infty$. This means $g^n=e_G$ if and only if $d\mid n$, (I)

and $d>0$. For every integer n, by long division, there are

integers q and r such that $n=dq+r$ and $0\le r<d$

(dividing n by d). Hence

$$g^n=g^{dq+r}=g^{dq}\cdot g^r \underset{\boxed{d\mid dq}}{=} e_G\cdot g^r=g^r\in\{e_G, g, \ldots, g^{d-1}\}.$$

Hence $\langle g\rangle\subseteq\{e_G, g, \ldots, g^{d-1}\}$. Clearly $\{e_G, g, \ldots, g^{d-1}\}\subseteq\langle g\rangle$.

Therefore $\langle g\rangle=\{e_G, g, \ldots, g^{d-1}\}$.

To show $|\langle g\rangle|=d$, it is enough to prove $g^i\neq g^j$ if

$0\le i<j<d$. Suppose to the contrary that for some

integers $0\le i<j<d$, we have $g^i=g^j$. (II) Multiplying

both sides of (II) by g^{-i}, we obtain that $e_G=g^{j-i}$.

List of distinct elements of a cyclic group

Tuesday, June 29, 2021 3:29 PM

By (I), we know that $g^n = e_G \iff d \mid n$. Hence $g^{j-i} = e_G$ implies that $d \mid j-i$. This is a contradiction as

$0 < j-i \leq j < d$ and there is no multiple of d in the interval $[1 .. d-1]$. Thus $|\{e_G, g, \ldots, g^{d-1}\}| = d$, and so $|\langle g \rangle| = d$.

- Suppose $d = \infty$. This means $g^n = e_G \iff n = 0$. (I)

If $g^i = g^j$ (II) for some integers i and j, then multiplying both sides of (II) by g^{-j} we obtain that

$$g^i \cdot g^{-j} = g^j \cdot g^{-j} \Rightarrow g^{i-j} = e_G.$$

$$\overset{(I)}{\Longrightarrow} \quad i-j = 0$$

$$\Longrightarrow \quad i = j.$$

Hence all g^i's are distinct as i ranges in $\mathbb{Z}$. (III)

- If $o(g) = d < \infty$, then $|\langle g \rangle| = d = o(g)$
- If $o(g) = \infty$, then $|\langle g \rangle| = \infty$ because of (III). ∎

Next we study properties of order of an element and use them to investigate subgroups of finite cyclic groups further.

Order of powers of an element

Tuesday, June 29, 2021 3:29 PM

Theorem. Suppose $(G,\cdot)$ is a group and $o(g)=n<\infty$. Then for every integer m, $o(g^m)=\dfrac{n}{\gcd(n,m)}$.

Pf. Since $o(g)=n<\infty$, we have that

$$g^k=e_G \iff n \mid k. \qquad \text{(I)}$$

$$(g^m)^\ell = e_G \iff g^{m\ell}=e_G \overset{\text{(I)}}{\iff} n \mid m\ell$$

$$\iff \frac{n}{\gcd(n,m)} \;\Big|\; \frac{m}{\gcd(n,m)}\ell \qquad \text{(II)}$$

Let $d:=\gcd(n,m)$. Then $\gcd(\frac{n}{d},\frac{m}{d})=1$. Notice that by Euclid's lemma, $\frac{n}{d} \mid \frac{m}{d}\ell$ implies that $\frac{n}{d}\mid \ell$. Clearly the converse holds as well; that means that $\frac{n}{d}\mid\ell$ implies $\frac{n}{d}\mid\frac{m}{d}\ell$. Therefore by (II)

$$(g^m)^\ell=e_G \iff \frac{n}{d}\;\Big|\;\frac{m}{d}\ell$$

$$\iff \frac{n}{d}\;\Big|\;\ell \qquad \text{(III)}$$

(III) implies that $o(g^m)=\dfrac{n}{d}=\dfrac{n}{\gcd(n,m)}$. ∎

Corollary. Suppose $o(g)=n<\infty$. Then $\langle g^m\rangle=\langle g\rangle$ if and only if $\gcd(m,n)=1$. Hence a cyclic group of cardinality n has $\phi(n)$ generators.

Generators of a cyclic group

Tuesday, June 29, 2021 3:29 PM

Pf. Since $\langle g^m\rangle \subseteq \langle g\rangle$ and $\langle g\rangle$ is finite, we have $\langle g^m\rangle = \langle g\rangle$ if and only if $|\langle g^m\rangle| = |\langle g\rangle|$. Because these are finite cyclic groups, $|\langle g^m\rangle| = o(g^m) = \frac{n}{\gcd(n,m)}$ and $|\langle g\rangle| = o(g) = n$. Therefore

$$\langle g^m\rangle = \langle g\rangle \Leftrightarrow \frac{n}{\gcd(n,m)} = n \Leftrightarrow \gcd(n,m) = 1.$$

Since $\langle g\rangle = \{e_G, g, \dots, g^{n-1}\}$, number of generators of $\langle g\rangle$ is $|\{m \mid 0 \le m < n,\ \gcd(n,m)=1\}|$, which is $\phi(n)$. ∎

Lemma. Suppose $o(g) = n < \infty$. Then, for every integer a,

$$\langle g^a\rangle = \langle g^{\gcd(a,n)}\rangle.$$

Pf. Let $d := \gcd(a,n)$. Then $d \mid a$, which implies that $a = dk$ for some $k \in \mathbb{Z}$. Hence $g^a = (g^d)^k \in \langle g^d\rangle$. Therefore $\langle g^a\rangle \subseteq \langle g^d\rangle$. (I) On the other hand,

$$|\langle g^a\rangle| = o(g^a) = \frac{n}{\gcd(n,a)} = \frac{n}{d} \text{ and}$$

$$|\langle g^d\rangle| = o(g^d) = \frac{n}{\gcd(n,d)} = \frac{n}{d}.$$

($d \mid n$ as $d = \gcd(n,a)$. This is why $d = \gcd(n,d)$.)

(II)

By (I) and (II), we deduce that $\langle g^a\rangle = \langle g^d\rangle$. This completes the proof. ∎

Subgroups of a finite cyclic group

Tuesday, June 29, 2021 3:29 PM

<u>Theorem.</u> Suppose $G=\langle g\rangle$ and $|G|=n$. Then

(1) Every subgroup of G is of the form $\langle g^m\rangle$ where $m|n$, $m>0$.

(2) If $H_1, H_2 \le G$ and $|H_1|=|H_2|$, then $H_1=H_2$.

(3) If $d|n$ and $d>0$, then there is a unique subgroup of G which has cardinality d.

<u>Pf</u> (1) We have proved that every subgroup of a cyclic group is cyclic. Hence every subgroup H of G is of the form $\langle g^a\rangle$ for some integer a. By the previous lemma, $\langle g^a\rangle = \langle g^{\gcd(n,a)}\rangle$. Hence every subgroup of G is of the form $\langle g^m\rangle$ where m is a positive divisor of n. (notice that $\gcd(n,a)$ is a positive divisor of n.)

(2) By the 1st part $H_1=\langle g^{m_1}\rangle$ and $H_2=\langle g^{m_2}\rangle$ for some $m_i|n$ and $m_i>0$. So

$$|H_i| = |\langle g^{m_i}\rangle| = o(g^{m_i}) = \frac{n}{\gcd(n,m_i)} \underset{\{m_i|n \text{ and } m_i>0\}}{=} \frac{n}{m_i} \quad (*)$$

Because $|H_1|=|H_2|$, we deduce that $m_1=m_2$; and so $H_1=H_2$.

(3) If $d|n$, $d>0$, then $|\langle g^{n/d}\rangle| \overset{(*)}{=} \frac{n}{n/d} = d$. Hence

Subgroups of a finite cyclic group

Tuesday, June 29, 2021 3:29 PM

there is a subgroup of G which has cardinality d. The uniqueness follows from the 2nd part.

Altogether we got a concrete bijection between

subgroups of a cyclic group of cardinality n and positive divisors of n.

This is an important result which is extremely useful in (finite) field theory as well.