Section 6.3 we have a group-theoretic proofs of Fermat's little theorem and Eulers theorem.

— Applying Lagrange's theorem to.

$U(n)$

— which we've proved directly in number theory lectures.

6.5 Exercises

Q1. A finite group G has elements $g, h \in G$ where $|g| = 5$, $|h| = 7$.

Why must $|G| \geq 35$?

Remember for any $x \in G$, $|x| = |\langle x \rangle|$ where $\langle x \rangle$ is the cyclic subgroup generated by x.

By Lagrange's theorem. $|g| = |\langle g \rangle|$ divides $|G|$, and similarly $|h| \,/\, |G|$.

So $5 \,/\, |G|$ & $7 \,/\, |G|$.

$\Rightarrow$ $35 \,/\, |G|$, since 5, 7 are coprime (result from number theory)

$$\left(25 \mid 100 \ \& \ 5 \mid 100\right) \not\Rightarrow \underbrace{5\cdot 25}_{125} \mid 100$$

So this means $|G| \geq 35$.

<u>Q2</u> If $|G| = 60$

Then its subgroups will have orders which come from $\{1, 2, 3, 4, 5, 10, 15, 12, 20, 30, 60\}$

6, 18,

by Lagrange's theorem.

<u>Q5</u> $\langle 8 \rangle$ in $\mathbb{Z}_{24}$

group under addition.

subgroup gen. by 8 under addition.

What are the cosets of $\langle 8 \rangle$ in $\mathbb{Z}_{24}$.

$\langle 8 \rangle = \{0, 8, 16\} = 8 + \langle 8 \rangle = 16 + \langle 8 \rangle$

So we expect seven more cosets.

$1 + \langle 8 \rangle = \{1, 9, 17\} = 9 + \langle 8 \rangle = 17 + \langle 8 \rangle$

$2 + \langle 8 \rangle = \{2, 10, 18\}$

$3 + \langle 8 \rangle$

$4+\langle 8\rangle$

$5+\langle 8\rangle$

$6+\langle 8\rangle$

$7+\langle 8\rangle = \{7, 15, 23\}$

cosets partition $\mathbb{Z}_{24}$

Since $\mathbb{Z}_{24}$ is abelian, left/right cosets are the same.

(h) $G = S_4$ = all permutations of the four objects 1, 2, 3, 4

$|S_4| = 24$. group operation is composition.

$H = \{(1), (1\,2\,3), (1\,3\,2)\}$

We're expecting eight left cosets.

1. $\boxed{H = \{(1), (1\,2\,3), (1\,3\,2)\}}$

2. $(1\,2\,3\,4)H$

$= \{(1\,2\,3\,4), (1\,2\,3\,4)(1\,2\,3), (1\,2\,3\,4)(1\,3\,2)\}$

$= \{(1\,2\,3\,4), (1\,3\,2\,4), (1\,4)(2)(3)\}$

$= \boxed{\{(1\,2\,3\,4), (1\,3\,2\,4), (1\,4)\}}$

3. $(1\ 2)H = \{(1\ 2), (1\ 2)(1\ 2\ 3),$
$(1\ 2)(1\ 3\ 2)\}$

$$= \boxed{\{(1\ 2), (2\ 3), (1\ 3)\}}$$

4. $(2\ 4)H = \{(2\ 4), (2\ 4)(1\ 2\ 3),$
$(2\ 4)(1\ 3\ 2)\}$

$$= \boxed{\{(2\ 4), (1\ 4\ 2\ 3), (1\ 3\ 4\ 2)\}}$$

Find the four other cosets in a similar fashion.

Since S_4 is non-abelian we don't expect the left/right cosets to be the same.

~~are~~ subgroups where these are equal are important and called "normal".

<u>Let's investigate</u>

$H(1\ 2\ 3\ 4) = \{(1\ 2\ 3\ 4), (1\ 2\ 3)(1\ 2\ 3\ 4),$
$(1\ 3\ 2)(1\ 2\ 3\ 4)\}$

$= \{(1\ 2\ 3\ 4), (1\ 3\ 4\ 2), (3\ 4)\}$

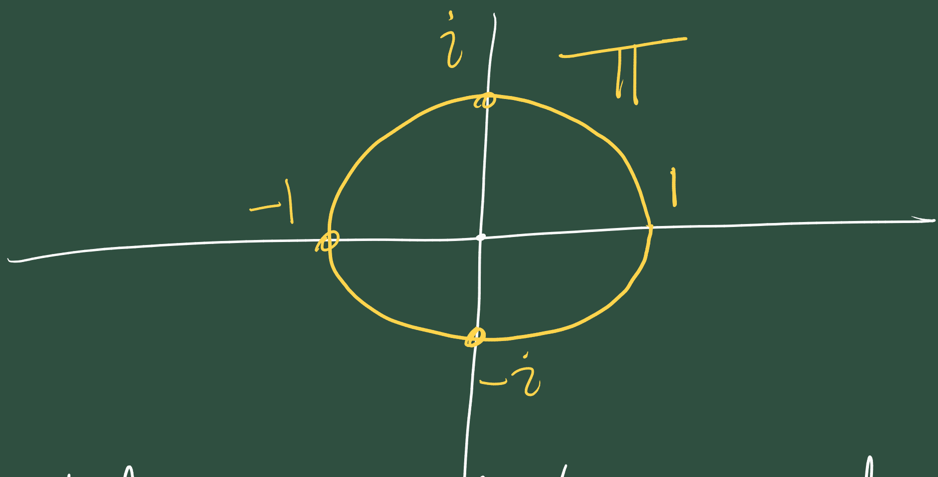
$\neq (1\ 2\ 3\ 4)H$

So H is not a 'normal' subgroup of S_4.

(g) ~~The~~ $\mathbb{C}^*$ is the multiplicative group of non-zero complex numbers

$\mathbb{T}$ is the circle subgroup.

$= \{ z : |z| = 1 \}$.



$\mathbb{C}^*$ is abelian so left/right cosets are the same.

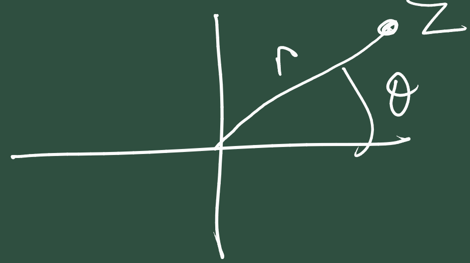
For any $z \in \mathbb{C}^*$ $\quad w \in \mathbb{T}$.

$$z\mathbb{T} = \{ zw : |w| = 1 \}.$$

We know cosets will partition $\mathbb{C}^*$, and that $\mathbb{T}$ is one of the cosets.

Suppose $|z| = r$

say $z = re^{i\theta}$



for any $w \in \mathbb{T}$ $\quad |zw|$

$$= |z||w|$$

$$= |z| = r$$

So everything in $z\mathbb{T}$, will have magnitude r

and vice versa, any complex number of magnitude r will be in $z\mathbb{T}$.

Say $x \in \mathbb{C}^*$ $\quad |x| = r$.

note that $\left|\frac{x}{z}\right| = \frac{|x|}{|z|} = \frac{r}{r} = 1$.

ie $\frac{x}{z} \in \mathbb{T}$.

so $\quad x = z\frac{x}{z} \in z\mathbb{T}$.

So $z\mathbb{T}$ is the circle of radius r centred on origin. So the cosets partition $\mathbb{C}^*$ into the infinite set of concentric circles centred on 0.

Q6. Consider the group

$G = GL_2(\mathbb{R})$ = group of all 2×2 invertible matrices with real entries under the op. of mat. mult.

Its subgroup $S = SL_2(\mathbb{R})$ is the special linear group.

$$S = SL_2(\mathbb{R}) = \{ A \in GL_2(\mathbb{R}) : \det(A) = 1 \}.$$

Describe the left cosets of S in G.

Let $X \in G$. What can say about

XS?

Conjecture: $XS = \{ XB : B \in S \}$

$$= \{ Y \in G : \det(Y) = \det(X) \}$$

<u>Proof</u> Let $B \in S$,

$$\det(XB) = \det(X)\det(B)$$

$$= \det(X), \text{ since } \det(B) = 1 \text{ as } B \in S$$

So for all $Y \in XS$, $\det(Y) = \det(X)$.

Suppose $Z \in G$ and $\det(Z) = \det(X)$

Is $Z \in XS$?

i.e. $Z = X \underbrace{(X^{-1}Z)}_{\in S \checkmark}$

since $\det(X^{-1}Z) = \det(X^{-1})\det(Z)$

$= \dfrac{1}{\det(X)} \det(Z)$

$= 1$

So this proves the conjecture.

So ~~that~~ each coset consists of all matrices from G with the same determinant.

$[G:S] = \infty$ as the determinant can be any element from $\mathbb{R}^*$.

G is non-abelian. Are left/right cosets different/same? They're the same.

Q19 Let H, K be subgroups of G

Recall we have proved that $H \cap K$ is a subgroup.

Claim For any $g \in G$.

$gH \cap gK$ is a coset of $H \cap K$ in G

in fact $\underbrace{gH \cap gK}_{A} = \underbrace{g(H \cap K)}_{B}$

$A = B$

Proof

Show $A \subseteq B$ & $B \subseteq A$

$A \subseteq B$ Let $x \in gH \cap gK$.

$\Leftrightarrow$ $x \in gH$ AND $x \in gK$.

$\Leftrightarrow$ $x = gh$ AND $x = gk$. for some $h \in H$, $k \in K$.

$\Leftrightarrow$ $x = gh = gk$

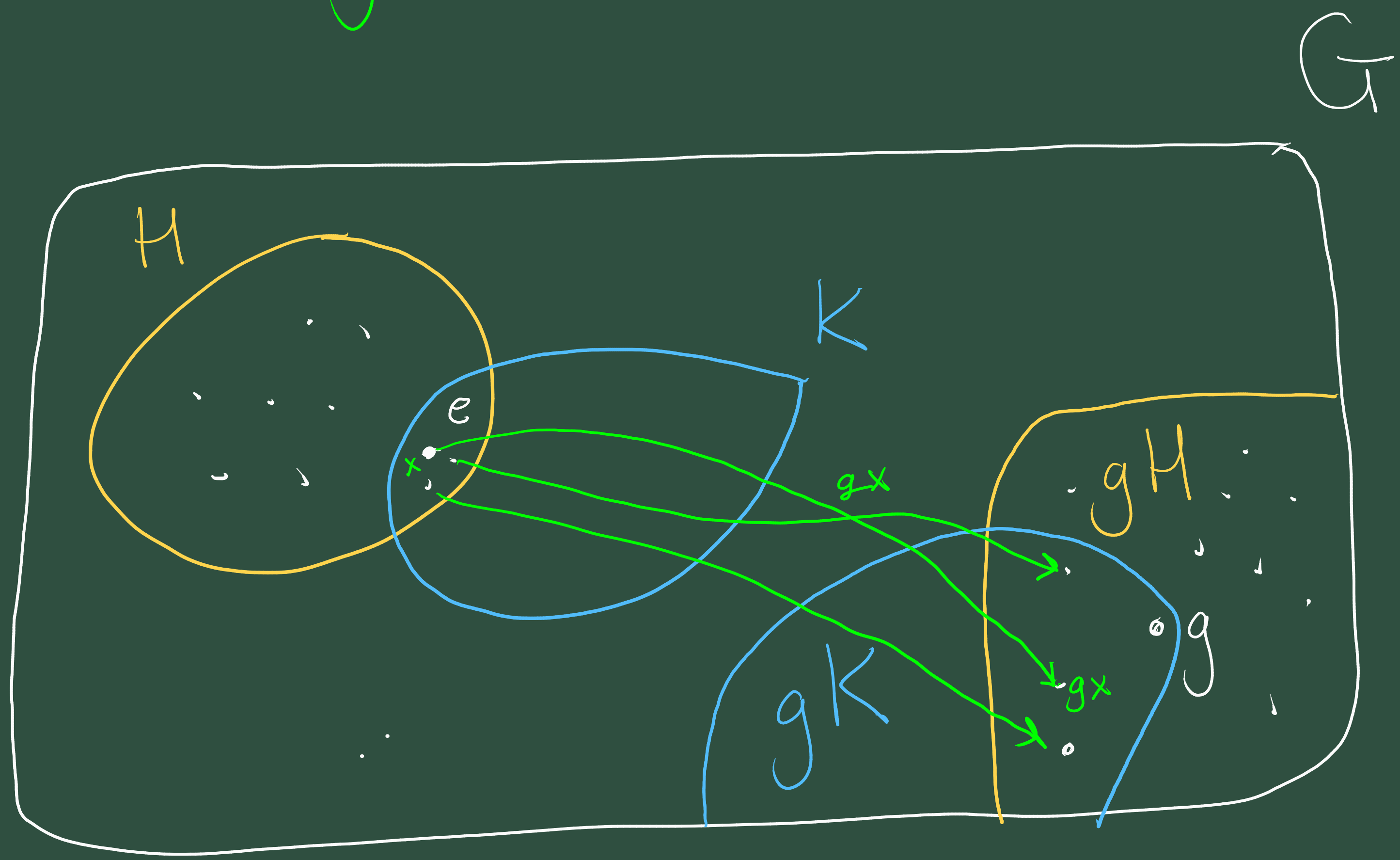
$\Leftrightarrow$ $h = k$ ✓

$\Leftrightarrow$ $x = g\underbrace{h}_{\in H \cap K}$.

$\Leftrightarrow$ $x \in g(H \cap K)$

In fact this is a sequence of equivalences.

So $gH \cap gK = g(H \cap K)$



Q13 | Can we prove theorem 6.8 by defining a map $\phi : \mathcal{L}_H \to R_H$ by the definition $\phi(gH) = Hg$?

The issue here is: is this even a valid definition??

because the coset gH has other representatives.

Suppose $gH = xH$.
$\Rightarrow x = gy$, for some $y \in H$.

for this to be a valid definition we would need it to be true that $Hg = Hx$. or $g = xy^{-1}$

Can we prove this?

For any hg, can we write it as $hg = \underline{\quad k \quad} x$, for some element k of H.

$$hg = hxy^{-1} = \cdots\cdots \overset{?}{=} \underset{\in H.}{\underline{\qquad}}\, x$$

I don't see how to do it.

Can we find a counter-example?

Examine earlier example.

$H \subset S_4$

$H = \{(1), (123), (132)\}$

$$(1\,2\,3\,4)H = \{(1\,2\,3\,4), (1\,3\,2\,4), (1\,4)\}$$
$$= (1\,4)H$$

$$H(1\,2\,3\,4) = \{(1\,2\,3\,4), (1\,3\,4\,2), (3\,4)\}$$
$$\cancel{=}$$

$$H(1\,4) = \{(1\,4), \ldots, \ldots\}$$

This is a counterexample.