Notes from P. Pylyavskyy, subbing Sept. 24, 2018

Let G be a group with law of composition $+$.

A subset $S \subseteq G$ is a **subgroup** if

- if $a, b \in S$ then $a+b \in S$
- 0 is in S
- if $a \in S$ then $-a \in S$

(closure, identity, inverses)

How can a subgroup of $\mathbb{Z}^+$ look like?

Ex Assume $8, 14 \in S$. What else has to be there?

Let $a \in \mathbb{Z}$, $a \neq 0$.

Let $\mathbb{Z}a$ be multiples of a.

Subgroup. (why?)

$\boxed{\text{Thm}}$ Let S be a subgr. of $\mathbb{Z}^+$. Either $S = \{0\}$, or $S = \mathbb{Z}a$ for ~~some~~ a – smallest pos. int. in S.

Proof: $0 \in S$. If $S = \{0\}$ – done. Otherwise $\exists\, n \in S$, $n \neq 0$. Can assume $n > 0$ (why?)

Let a be smallest such n (why exists?).

Claim: $S = \mathbb{Z}a$.

First, $\mathbb{Z}a \subseteq S$.

Indeed, for $k > 0$, $k \in \mathbb{Z}$

[illegible] $a \in S$. Th[illegible] $ka \in S$

Then $-ka \in S$. Finally $0 \in S$.

Second, $S \subseteq \mathbb{Z}a$. Assume $n \in S$. Divide n by a with remainder:

$n = qa + r$, $\quad 0 \leq r < a$.

(Ex. $n = -8$, $a = 5$?)

$n \in S$, $qa \in S \Rightarrow n - qa = r \in S$.

Contradiction unless $r = 0$. ∎

Let $a, b \in \mathbb{Z}$. Claim:

$S = \mathbb{Z}a + \mathbb{Z}b = \{n \in \mathbb{Z} \mid n = ra + sb\}$ is a subgroup of $\mathbb{Z}$. (why?)

We know $S = \mathbb{Z}d$ for some $d \in \mathbb{Z}_{\geq 0}$. What is d?

$d = \gcd(a, b)$ – greatest common divisor

Ex $\gcd(8, 14) = 2$.

$\mathbb{Z}8 + \mathbb{Z}14 = \mathbb{Z}2$.

$\boxed{\text{Prop}}$ Let $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$. Let d be (the unique) el-t of $\mathbb{Z}_{\geq 0}$ s.t. $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d$.

(a) $d \mid a, b$

(b) if $e \mid a, b$ then $e \mid d$.

(c) $\exists\, r, s \in \mathbb{Z}$ s.t. $ra + sb = d$.

Proof: ...

How can we find gcd?

Euclids algorithm. Ex $\gcd(26, 34)$

Any other method?

$18 = 2^1 \cdot 3^2$, $24 = 2^3 \cdot 3^1$ $\Big\}$ $\gcd(18,24) = 2^1 3^1 = 6$

Why can we write $d = ra + sb$?

a and b are <u>relatively prime</u> if $\gcd(a,b) = 1 \iff \mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}$

$\boxed{\text{Cor}}$ $\gcd(a,b) = 1$ iff $\exists\, r, s$ s.t. $ra + sb = 1$.

$\boxed{\text{Cor}}$ Assume p is prime. If $p \mid ab$ then $p \mid a$ or $p \mid b$.

<u>Proof</u>: assume $p \mid ab$, $p \nmid a$. Then $\gcd(p,a) = 1$. Then $\exists\, r, s \in \mathbb{Z}$ s.t. $ra + sp = 1 \Rightarrow$ $\Rightarrow rab + spb = b$. Since p divides left side, it divides b.

What about <u>least common multiple</u>?

For $a, b \in \mathbb{Z}_{\neq 0}$ take $S = \mathbb{Z}a \cap \mathbb{Z}b$. <u>Subgroup</u> (why?)

Can it be $\{0\}$? No.

Thus $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}m$ for some $m \in \mathbb{Z}_{>0}$.

$\boxed{\text{Prop}}$ (a) $m \vdots a, b$

(b) If $n \vdots a, b$ then $n \vdots m$.

Pr

$\boxed{\text{Cor}}$ Let $d = \gcd(a,b)$, $m = \text{lcm}(a,b)$. Then $ab = dm$.

<u>Proof</u>: $b/d \in \mathbb{Z} \Rightarrow a \mid \frac{ab}{d}$. Similarly $b \mid \frac{ab}{d}$. Then $m \mid \frac{ab}{d} \Rightarrow dm \mid ab$.

Now, write $d = ra + sb \Rightarrow$ $dm = ram + sbm$. Right side is $\vdots ab \Rightarrow ab \mid dm$. Since both $\geq$ in $\mathbb{Z}_{>0}$, done.

Let G be a group, use multip. not.

Let $x \in G$.

<u>Cyclic subgroup</u> generated by x is

$H = \{\ldots, x^{-2}, x^{-1}, 1, x, x^2, x^3, \ldots\}$

Smallest subgroup containing x.

$H = \langle x \rangle$.

Can $\langle x \rangle$ be finite?

Ex Take $\mathbb{R}^\times$. Take $x = -1$. Then $H = \{-1, 1\}$.