

Last time: $(\mathbb{Z}, +)$ is a sg

$H \subseteq \mathbb{Z}$ subgps

We proved: Such H are of the form $\{0\}$ or
 $H = \mathbb{Z}a$ where a is the least pos integer in H .

Questions ① If $a, b \neq 0$ integers, consider

$$S = \mathbb{Z}a + \mathbb{Z}b = \{ma + nb : m, n \in \mathbb{Z}\}.$$

Is S a subgp of $(\mathbb{Z}, +)$?

② If $a = 3, b = 5$, what is S ?

③ If $a = 6, b = 10$, what is S ?

① The answer is Yes, S is a subgp.

Check from defn:

✓ closed under addition? $(ma + nb) + (m'a + n'b)$

$$= (m + m')a + (n + n')b$$

✓ contains the identity?

✓ closed under inverses?

② First note that $S \ni 1 = 2 \cdot 3 + (-1)5$.

$$\Rightarrow \mathbb{Z} \cdot 1 \subseteq S \Rightarrow S = \mathbb{Z}.$$

③ Claim: S is all multiples of 2, i.e. $S = \mathbb{Z} \cdot 2$.

OTOH, $2|6$ and $2|10 \Rightarrow 2|m \cdot 6 + n \cdot 10$ for all $m, n \in \mathbb{Z}$.

OTOH, $2|6$ and $2|10 \Rightarrow 2|m \cdot 6 + n \cdot 10$ for all $m, n \in \mathbb{Z}$

$\Rightarrow 2$ divides every elt of S , $S \subseteq \mathbb{Z} \cdot 2$

Need converse: $2 = 2 \cdot 6 + (-1) \cdot 10 \Rightarrow 2 \in S$

$\Rightarrow \mathbb{Z}2 \subseteq S \Rightarrow S = \mathbb{Z} \cdot 2$.

S is called the subgp of $\mathbb{Z}$ generated by a and b
 " $\mathbb{Z}a + \mathbb{Z}b$ ".

It is the smallest subgp of $(\mathbb{Z}, +)$ that contains both a & b .

Know Given $a, b \in \mathbb{Z}$, $\exists$ $d \neq 0$ integer so that
_{not both 0}

$S = \mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d$.

Propⁿ Suppose a, b, d are as above. Then

- $d|a$ and $d|b \Rightarrow d$ is the $\gcd(a, b)$.
- If $e|a$ and $e|b$ then $e|d$.
- $\exists$ int. r, s so that $d = ra + sb$.

Pf:

c) immediate: $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d$ and d is in the LHS

a) $b|c$ a and b are in $\mathbb{Z}d$, $d|a$ & $d|b$.

b) $d = ra + sb$ from part c). Thus if $e|a$ & $e|b$ then $e|$ RHS $\Rightarrow e|$ LHS $= d$.

Aside! Euclidean Algorithm: An algorithm to compute $\gcd(a, b)$

Propⁿ Suppose $a, b \in \mathbb{Z}$, $a = qb + r$ with $0 \leq r < b$.

Then $\gcd(a, b) = \gcd(b, r)$.

Pf: Claim $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}b + \mathbb{Z}r$

$$ma + nb = m(qb + r) + nb = (mq + n)b + mr \\ \Rightarrow \text{LHS} \subseteq \text{RHS}.$$

$$mb + nr = mb + n(a - qb) \Rightarrow \text{RHS} \subseteq \text{LHS} \\ = na + (m - nq)b$$

Problem Use Propⁿ to compute $\gcd(98, 77)$.

$$98 = 1 \cdot 77 + 21 \\ \gcd(98, 77) = \gcd(77, 21)$$

$$77 = 3 \cdot 21 + 14 \\ \gcd(77, 21) = \gcd(21, 14)$$

$$21 = 1 \cdot 14 + 7 \\ \gcd(21, 14) = \gcd(14, 7) = 7.$$

Recall: • Can also find $\gcd$ by factoring integers

- We use Euclidean Algorithm b/c it is much faster.

Defⁿ Integers a & b are said to be relatively prime if $\gcd(a, b) = 1$.

Cor $\gcd(a,b) = 1 \iff \exists$ integers r,s so that $1 = ra + sb$.

Cor p prime. Then $p|ab \Rightarrow p|a$ or $p|b$.

One needs this corollary to prove unique factorization of integers into products of primes.

Pf: Suppose $p|a \Rightarrow \gcd(p,a) = 1$.

$\Rightarrow \exists$ int. r,s so that $1 = rp + sa$.

$\Rightarrow b = \underbrace{brp}_{p \text{ divides}} + \underbrace{sab}_{p \text{ divides } ab, \text{ by assumption}}$ $\Rightarrow p|b$.

p also divides

QED

We just looked @ $\mathbb{Z}a + \mathbb{Z}b$.

Question: Is $\mathbb{Z}a \cap \mathbb{Z}b$ a subgroup of $\mathbb{Z}$?

Propⁿ G a gp, H_1, H_2 subgps of G . Then $H_1 \cap H_2$ is a subgroup of G .

Pf

closure: if $h \in H_1 \cap H_2$ and $h' \in H_1 \cap H_2$ then $hh' \in H_1 \cap H_2$.

$hh' \in H_1$ b/c $h, h' \in H_1$ and H_1 is a subgp.

sim: $hh' \in H_2$ $\underbrace{\hspace{10em}}_{H_2}$

$\Rightarrow hh' \in H_1 \cap H_2$.

identity $1 \in H_1 \cap H_2$

inverses?

QED

$$\mathbb{Z}_a, \mathbb{Z}_b \Rightarrow \mathbb{Z}_a \cap \mathbb{Z}_b = \mathbb{Z}_m \text{ for some } m \in \mathbb{Z}.$$

Ex $\mathbb{Z}(15) \cap \mathbb{Z}(10) = \mathbb{Z}(30).$

Propⁿ Notation as above.

a) m is div. by a & b . $\Rightarrow m$ is the $\text{lcm}(a, b)$.

b) If $a|n$ & $b|n$ then $m|n$.

Pf: a) $\mathbb{Z}_a \cap \mathbb{Z}_b = \mathbb{Z}_m.$

$$\Rightarrow m \in \mathbb{Z}_a + m \in \mathbb{Z}_b$$

$$\Downarrow$$

$$a|m$$

$$\Downarrow$$

$$b|m.$$

b) If $\begin{matrix} a|n \Rightarrow n \in \mathbb{Z}_a \\ b|n \Rightarrow n \in \mathbb{Z}_b \end{matrix} \Rightarrow n \in \mathbb{Z}_a \cap \mathbb{Z}_b = \mathbb{Z}_m$

$$\Rightarrow m|n. \quad \square$$

Cor a, b integers. $d = \text{gcd}(a, b)$, $m = \text{lcm}(a, b)$.

Then $ab = dm$.

Pf: Check: $dm|ab$ and $ab|dm$.

Know: $d|a \Rightarrow b|(\frac{a}{d})b \Rightarrow m|\frac{ab}{d} \Rightarrow md|ab.$

$d|b \Rightarrow a|\frac{ab}{d}$

Conversely, $d = ra + sb$ for int. r, s .

$$\Rightarrow md = \underbrace{rma}_{\text{div}} + \underbrace{smb}_{\uparrow \uparrow}$$

$\Rightarrow \text{L.I.}$

$$ma - rmy + smz$$

$\underbrace{\hspace{1.5cm}}_{\substack{\text{div} \\ \text{by} \\ ab}} \quad \underbrace{\hspace{1.5cm}}_{\substack{\uparrow \\ ab \text{ divides}}}$

$$\cdot a|m$$

$$\Rightarrow ab | md. \quad \text{QED}$$
