Class 5: Cyclic Subgroups - 20220921

Group of Integer

Integers $\mathbb{Z}$ with addition $(\mathbb{Z}, +)$ is a group.

Notations

- $\mathbb{N}$: Natural numbers: $0, 1, 2, 3, \ldots$.
- $\mathbb{Z}$: Integers
- $\mathbb{Q}$: Rational numbers
- $\mathbb{R}$: Real numbers
- $\mathbb{C}$: Complex numbers

Subgroups

Question: What are the subgroups of $(\mathbb{Z}, +)$?

- Observation:
  - For any $a \in \mathbb{N}, \;\; a\mathbb{Z} = \{ak \in \mathbb{Z} | k \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$:
  - $\forall ak_1, ak_2 \in a\mathbb{Z}, \quad (-ak_1) + (ak_2) = a(k_2 - k_1) \in a\mathbb{Z}$.
- Also, note that $a\mathbb{Z} = (-a)\mathbb{Z}$.

Proposition

- If H is a subgroup of $(\mathbb{Z}, +)$, then $H = a\mathbb{Z}$ for some $a \in \mathbb{N}$.
- Proof:
  - If $H = \{0\}$, then $H = 0\mathbb{Z}$
  - If $H = \mathbb{Z}$, then $H = 1\mathbb{Z}$.
  - If $\{0\} \subsetneq H \subsetneq \mathbb{Z}$:
    - $\{0\} \subsetneq H$, so H contains a nonzero element m.
      - H is a subgroup, so $-m \in H$.
      - $m \neq 0$, so m or $-m$ is positive
      - so $S = \{h \in H | h > 0\} \neq \emptyset$, $S \subseteq \mathbb{N}$
    - Take $a = \min(S)$, the smallest number in S.
      - Note a is the smallest positive number in H.
      - Also, $a \neq 1$. otherwise, $1 \in H$, which implies $H = \mathbb{Z}$.
    - We'll show $H = a\mathbb{Z}$.

        - Suppose $H \neq a\mathbb{Z}$:
            - $a \in H$, so $a\mathbb{Z} \in H.$ and $H \neq a\mathbb{Z}$.
            - so $\exists h \in H \backslash a\mathbb{Z}$.
            - Divide h by a:
                - $h = aq + r$, with $q \in \mathbb{Z}, 0 < r < a$
                - $r = h - aq \in H.$
            - Contradicts with our choice of a that a is the smallest positive number.
        - Since we get a contradiction, we conclude that $H = a\mathbb{Z}$

Greatest common divisor

Definition

- a, b are integers, not both zero. Define the greatest common divisor of a, b to be the positive integer g such that $g\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$

Lemma

- $a\mathbb{Z} + b\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.
    - Proof as exercise
- Combine the Lemma with the prop. we just proved, we verified the existence of g.

Proposition

- If $g = gcd(a, b)$, then:
    - $g|a$ and $g|b$
    - For any $c \in \mathbb{Z}$ with $c|a$ and $c|b$, we have $c|g$.
- Proof:
    - $g = \mathrm{gcd}(a, b), g\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$
    1. $a = a * 1 + b * 0 \in g\mathbb{Z},$ so $g|a$

       $b = a * 0 + b * 1 \in g\mathbb{Z},$ so $g|b$
    2. $g = g * 1 \in g\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z},$ so $\exists k, l \in \mathbb{Z}, g = ak + bl$

       If $c|a$ and $c|b$, then $c|ak$ and $c|bl$, so $c|ak + bl = g$

Corollary

- If $g = \mathrm{gcd}(a, b)$, then $g = ak + bl$ for some $k, l \in \mathbb{Z}$.
- Furthermore, g is the smallest positive number among all the integer linear combinations of a and b.

Relatively Prime

Definition

- $a, b \in \mathbb{Z}$, not both zero, are <u>relatively prime</u>, if $\gcd(a, b) = 1$
- i.e., a, b are relatively prime if $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$
- In particular, we have:

Proposition

- $\exists k, l \in \mathbb{Z},\ ak + bl = 1 \iff a, b$ relatively prime
- Proof:
  - $\exists k, l \in \mathbb{Z}, ak + bl = 1 \iff a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z} \iff \gcd(a, b) = 1$

Proposition

- p is a prime, $a, b \in \mathbb{Z}, p|ab$. If $p \nmid a$, then $p|b$.
- Proof:
  - p is prime, $p \nmid a$, so $\gcd(p, a) = 1$
  - $\exists k, l,\ pk + al = 1 \Rightarrow\ pkb + abl = b$
  - Since $p|ab$, $p|b$

Cyclic Subgroup

Definition

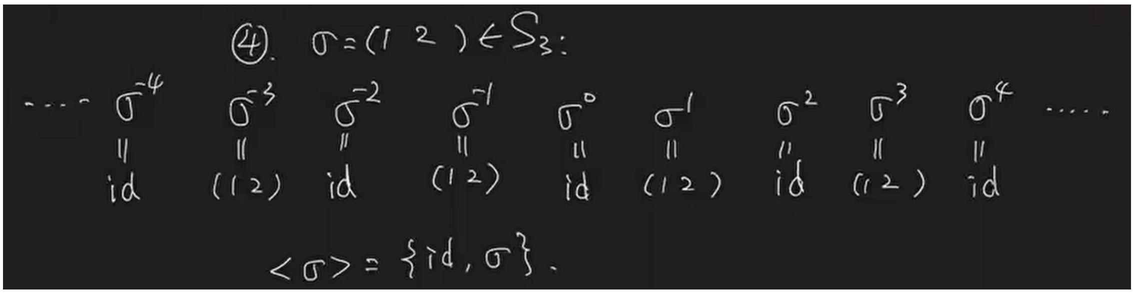
- G is a group. $a \in G$. Define the <u>cyclic subgroup</u> of G generated by a to be $< a >= \{a^k \in G | k \in \mathbb{Z}\}$

Lemma

- $< a >$ is a subgroup of G.
  - $a^k a^l = a^{k+l} \in < a >$
  - $1 = a^0 \in < a >$
  - $\forall a^k \in < a >, (a^k)^{-1} = a^{-k} \in < a >$

Examples

1. $\{1\} =< 1 >$
2. Every subgroup of $(\mathbb{Z}, +)$ is a cyclic subgroup.
3. In any group G, if $a \in G$, then $< a >=< a^{-1} >$
4. $\sigma = (1\ 2) \in S_3$: $<\sigma> = \{id, \sigma\}$



5. $\tau = (1\ 2\ 3) \in S_3, \quad <\tau> = \{id, \tau, \tau^2\}$

Proposition

- $a \in G$. Let $S = \{k \in \mathbb{Z} | a^k = 1\}$. Then S is a subgroup of $(\mathbb{Z}, +)$
- Proof:
  - $k, l \in S$. $a^k = 1, a^l = 1, a^{k+l} = a^k * a^l = 1$. $k + l \in S$
  - $a^0 = 1 \Rightarrow 0 \in S$
  - $k \in S. a^k = 1, a^{-k} = (a^k)^{-1} = 1$. $-k \in S$

Corollary

> “
>
> The order of an element in a group is **the smallest positive power of the element which gives you the identity element**.

- 00:59:00 没有听的很懂
- The set S in the above Prop. can be written as $S = n\mathbb{Z}$ for some $n \in \mathbb{N}$
- If $n = 0, S = \{0\}$, write $|a| = \infty$
- If $n \neq 0, S = n\mathbb{Z} \neq \{0\}$, write $|a| = n$
- we call $|a|$ the <u>order</u> of $a \in G$

Example

- Let's study the case $S \neq \{0\}$. i.e. $|a| = n$ for some positive integer n
- $a^k = a^l \iff a^{k-l} = 1 \iff k - l \in S = |a|\mathbb{Z} \iff |a| \Big| k - l$
- Gives us the proposition below:

Proposition

- $a^k = a^l \iff |a| \Big| k - l$

Prop

- If $|a|$ is finite (ie. $|a|$ is a positive integer), than $< a >= \{1, a, a^2, \ldots, a^{|a|-1}\}$
- In particular, we see $< a >$ has $|a|$ elements
- This gives an equivalent definition of |a|: $|a| = |< a >|$

- Example

1. $1 \in G, |1| = 1$
2. $\sigma = (1\ 2) \in S_3, |\sigma| = 2$
3. $\tau = (1\ 2\ 3) \in S_3,\ \ |\tau| = 3$
4. $1 \in \mathbb{Z}, |1| = \infty, < 1 >= \mathbb{Z}$
5. $K_4 = \{1, a, b, c\}, |a| = 2, < a >= \{1, a\}$