L8: Cyclic groups & subgroups

Cyclic groups & (their) subgroups

Def A group H is cyclic if it can be generated by a single element, i.e. $\exists x \in H$ s.t. $H = \langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$.

Prop If $H = \langle x \rangle$, then $|H| = |x|$. Moreover,

i) if $|H| = n < \infty$, then the elts $e, x, \ldots, x^{n-1}$ are all distinct and $H = \{e, x, \ldots, x^{n-1}\}$

ii) if $|H| = \infty$ then $H = \{\ldots, x^{-2}, x^{-1}, e, x, x^2, \ldots\}$ and $x^a \neq x^b$ if $a \neq b$.

Proof Case $|x| = n$: $\cdot$) We show $H = \langle x \rangle \subseteq \{e, x, \ldots, x^{n-1}\}$. Let $x^m \in H$, we write $m = kn + r$ $\quad 0 \le r \le n-1$ (division with remainder).

Then $x^m = x^{kn+r} = \underbrace{x^n \cdot x^n \cdots x^n}_{k\text{-times}} \cdot x^r = e \cdot x^r = x^r$.

$\cdot$) To show $\{e, x, \ldots, x^{n-1}\}$ are distinct assume $x^i = x^j$ for $0 \le i < j \le n-1$. Then $x^{j-i} = e$ for $0 < j-i < n-1$. This contradicts $|x| = n$.

Case $|x| = \infty$: We show $x^i \neq x^j$ for $i \neq j$ as above. $\square$

Thm Let $H = \langle x \rangle$. Then

i) if $|H| = n$, $\quad \varphi : \mathbb{Z}/n\mathbb{Z} \to H$, $\quad k \mapsto x^k$

ii) if $|H| = \infty$, $\quad \varphi : \mathbb{Z} \to H$, $\quad k \mapsto x^k$

define group isomorphisms.

Pf $\cdot$ φ well-defined $\quad k \equiv l \pmod n \Rightarrow k = l + mn$ for some $m \in \mathbb{Z}$.

Then $x^k = x^{l+mn} = x^l \cdot (x^n)^m = x^l$

- φ group hom: ✓
- φ bijection: previous prop.

Subgroups of the infinite cyclic group

Subgroups of cyclic groups

Prop Let $G = \langle x \rangle$ be cyclic an $H \leq G$ a subgroup. Then H is also cyclic.

Pf If $H = \{e\}$ we are done. Otherwise let $l = \min\{m \in \mathbb{Z}^{>0} \mid x^m \in H\}$. Then clearly $\langle x^l \rangle \subseteq H$.
Let now $x^k \in H$ be arbitrary. Write $k = l \cdot k' + r \quad 0 \leq r \leq l-1$
then $x^r = x^{k-lk'} = x^k \cdot (x^l)^{-k'} \in H$. But l was minimal hence $r = 0$, and thus $x^k = (x^l)^{k'} \in \langle x^l \rangle$. $\square$

Prop Let $G = \langle x \rangle$ be infinite cyclic ($|G| = \infty$). Then the assignment $n \mapsto \langle x^n \rangle$ defines a bijection between $\mathbb{N}$ and subgroups of G.

Pf By prev prop every subgroup is of the form $\langle x^n \rangle$ for $n \in \mathbb{Z}$.
Since $\langle x^{-n} \rangle = \langle x^n \rangle$ we can assume $n \in \mathbb{N}$. Suppose $\langle x^n \rangle = \langle x^m \rangle$
then $x^n = x^{km} \Rightarrow n = km$ and similarly $m = k'n$
and thus $n = kk'n$, i.e. $kk' = 1$ but $k, k' \in \mathbb{N}$ hence $k = k' = 1$. $\square$

Rmk Using that G is isomorphic to $\mathbb{Z}$ we have shown that subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ for $n \in \mathbb{N}$.