

Math 4032 Prof. Pennance – Summary of Lecture on Cyclic Groups

1. A subgroup of a cyclic group is cyclic.
2. Corollary. All subgroups of \mathbb{Z} have the form $\langle m \rangle = m\mathbb{Z}$.
3. Let $n \in \mathbb{Z}$. If $a, b \in \mathbb{Z}$ define $a \equiv b \pmod{n}$ if $n|(b - a)$. Then \equiv is an equivalence relation on \mathbb{Z} .
4. Let $Z_n = \{0, 1, \dots, n-1\}$. Then Z_n is a set of equivalence class representatives for the relation \equiv .
5. (Compatibility) If $a \equiv b$ and $a' \equiv b'$ then $a + b \equiv a' + b'$.
6. Let $Z_n = \{0, 1, \dots, n-1\}$. Let $p : \mathbb{Z} \rightarrow Z_n$ be the mod function

$$p(m) = m \text{ modulo } n$$

i.e. $p(m)$ is the unique remainder in the division theorem when m is divided by n . Then the following are trivial exercises.

- (a) Idempotency. $p(p(m)) = p(m)$ for all $m \in \mathbb{Z}$.
- (b) Periodicity. $p(m + n) = p(m)$ for all $m \in \mathbb{Z}$.
- (c) The restriction of p to Z_n is the identity function on Z_n .
- (d) For any integer m , $m \equiv p(m) \pmod{n}$.
- (e) The following are equivalent
 - i. $a \equiv b \pmod{n}$
 - ii. $p(a) = p(b)$

7. Define $+_n : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ (addition modulo n) by $x +_n y = p(x + y)$ then p is a morphism, i.e.

$$p(x + y) = p(x) +_n p(y)$$

for all $x, y \in \mathbb{Z}$.

Proof: There exist integers q, q' such that $x = qn + p(x)$ and $y = q'n + p(y)$. Hence $x + y = (q + q')n + p(x) + p(y)$. By periodicity, $p(x + y) = p(p(x) + p(y)) = p(x) +_n p(y)$.

Another Proof. Use compatibility and 6(d).

8. $(\mathbb{Z}_n, +_n)$ is a group.
Proof Use morphism property of p .
9. Let G be an infinite cyclic group. Then G is isomorphic to $(\mathbb{Z}, +)$.
Proof. Let $g \in G$ be a generator. Then the exponential function $n \mapsto g^n$ is an isomorphism from \mathbb{Z} to G .
10. Let G be a finite cyclic of order n then $G \cong (\mathbb{Z}_n, +_n)$.
Proof. Define $\phi : G \rightarrow \mathbb{Z}_n$ by $\phi(g^m) = p(m)$. It is easy to check that ϕ is an isomorphism.
11. $o(x^n) = \frac{o(x)}{\text{gcf}(o(x), n)}$
12. The lattice of subgroups of C_n .
13. $\text{lcm}(n, m) = \frac{nm}{\text{gcf}(n, m)}$