Abstract algebra

Lecture note 3. Cyclic groups

Lecturer : O-joung Kwon
Spring, 2019

Definition 1. *If the cyclic subgroup* $< a >$ *of* G *is finite, then the* order *of* a *is the order* $|< a >|$. *Otherwise, it is of infinite order.*

Note : Cyclic groups share many properties with natural numbers.

Elementary properties

Theorem 1. *Every cyclic group is abelian.*

PROOF

Recall the division algorithm for $\mathbb{Z}$.

Theorem 2. *Let m be a positive integer and n be an integer. Then there exist unique integer q and r such that $n = mq + r$ and $0 \leq r < m$.*

PROOF

Example 1. Find the quotient q and remainder r when 38 is divided by 7 according to the division algorithm.

Theorem 3. *A subgroup of a cyclic group is cyclic.*

Corollary 1. *The subgroup of $\mathbb{Z}$ under addition are precisely the groups $n\mathbb{Z} := \{nx : x \in \mathbb{Z}\}$ under addition for $n \in \mathbb{Z}$.*

PROOF. As any subgroup is cyclic, so, it has a generator.

This corollary give us an elegant way to define the greatest common divisor of two positive integers r and s.
Observe that $H = \{nr + ms : n, m \in \mathbb{Z}\}$ is a subgroup of the group $\mathbb{Z}$ under addition. Thus, H must have a generator d, which we may choose to be positive.

Definition 2. *Let r and s be two positive integers. The positive generator d of the cyclic group*

$$H = \{nr + ms : n, m \in \mathbb{Z}\}$$

under addition is the greatest common divisor of r and s. We write $d = gcd(r, s)$.

Example 2. Find the gcd of 42 and 72.

Theorem 4. *Let G be a cyclic group with n elements and generated by a. Let $b \in G$ and $b = a^s$. Then b generates a cyclic subgroup H of G containing n/d elements, where $d = gcd(n, s)$. Also, $< a^s >=< a^t >$ if and only if $gcd(s, n) = gcd(t, n)$.*

PROOF