1.6 Cyclic Subgroups

Recall: cyclic subgroup, cyclic group, generator.

Def 1.68. Let G be a group and $a \in G$. If the cyclic subgroup $\langle a \rangle$ is finite, then the *order* of a is $|\langle a \rangle|$. Otherwise, a is of *infinite order*.

1.6.1 Elementary Properties

Thm 1.69. *Every cyclic group is abelian.*

Thm 1.70. *If $m \in \mathbf{Z}^+$ and $n \in \mathbf{Z}$, then there exist unique $q, r \in \mathbf{Z}$ such that*

$$n = mq + r \qquad \textit{and} \qquad 0 \leq r \leq m.$$

In fact, $q = \lfloor \frac{n}{m} \rfloor$ and $r = n - mq$. Here $\lfloor x \rfloor$ denotes the maximal integer no more than x.

Ex 1.71 (Ex 6.4, Ex 6.5, p60).

1. Find the quotient q and the remainder r when $n = 38$ is divided by $m = 7$.

2. Find the quotient q and the remainder r when $n = -38$ is divided by $m = 7$.

Thm 1.72 (Important). *A subgroup of a cyclic group is cyclic.*

Proof. (refer to the book) □

Ex 1.73. The subgroups of $\langle \mathbf{Z}, + \rangle$ are precisely $\langle n\mathbf{Z}, + \rangle$ for $n \in \mathbf{Z}$.

Def 1.74. Let $r, s \in \mathbf{Z}$. The *greatest common divisor* (gcd) of r and s is the largest positive integer d that divides both r and s. Written as $d = \gcd(r, s)$.

In fact, d is the positive generator of the following cyclic subgroup of $\mathbf{Z}$:

$$\langle d \rangle = \{nr + ms \mid n, m \in \mathbf{Z}\}.$$

So d is the smallest positive integer that can be written as $nr + ms$ for some $n, m \in \mathbf{Z}$.

Ex 1.75. $\gcd(36, 63) = 9$, $\gcd(36, 49) = 1$. (by unique prime factorization, or so)

Def 1.76. Two integers r and s are *relative prime* if $\gcd(r, s) = 1$.

If r and s are relative prime and r divides sm, then r must divide m.

1.6.2 Structure

Thm 1.77. *Let G be a cyclic group with generator a. If the order of G is infinite, then G is isomorphic to $\langle Z, +\rangle$. If G has finite order n, then G is isomorphic to $\langle Z_n, +_n\rangle$.*

1.6.3 Subgroups of Cyclic Groups

The subgroups of infinite cyclic group $\mathbf{Z}$ has been presented in Ex 1.73.

Thm 1.78. *Let $G = \langle a\rangle$ be a cyclic group with n elements. A cyclic subgroup of $\langle a\rangle$ has the form $\langle a^s\rangle$ for some $s \in \mathbf{Z}$. The subgroup $\langle a^s\rangle$ contains n/d elements for $d = \gcd(s, n)$. Two cyclic subgroup $\langle a^s\rangle$ and $\langle a^t\rangle$ are equal if and only if $\gcd(s, n) = \gcd(t, n)$.*

So given $\langle a\rangle$ of order n and $s \in \mathbf{Z}$, we have $\langle a^s\rangle = \langle a^d\rangle$ for $d = \gcd(s, n)$.

Thm 1.79. *If $G = \langle a\rangle$ is a cyclic group of order n, then all of G's generators are a^r, where $1 \leq r < n$ and r is relative prime to n.*

Ex 1.80. The subgroup diagram of $\mathbf{Z}_{24}$.

1.6.4 Homework, I-6, p66-68

6, 13, 23, 44, **45**, 50
(opt) 32, 49, 51, 52, 53.