MAT414 - Modern Algebra

Miraj Samarakkody

Tougaloo College

03/28/2025

Example

Find all generators of the cyclic group $U(50)$.

Fundamental Theorem of Cyclic Groups

Theorem 4.3

Fundamental Theorem of Cyclic Group

Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k—namely, $\langle a^{n/k} \rangle$.

Example

Suppose $G = \langle a \rangle$ and G has order 30. Find all the subgroups of G.

Corollary

Subgroups of $\mathbb{Z}_n$

For each positive divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k; moreover, these are the only subgroups of $\mathbb{Z}_n$.

Example 7

Write the list of subgroups of $\mathbb{Z}_{30}$.

Example 8

Find the generators of the subgroup of order 9 in $\mathbb{Z}_{36}$.

Euler Phi Function

Let $\phi(1) = 1$, and for any integer $n > 1$, let $\phi(n)$ denote the number of positive integers less than n and relatively prime to n.

Example

Write each $\phi(n)$ for $n \in \{1, 2, \ldots, 12\}$

Some Properties

- For any prime p, $\phi(p^n) = p^n - p^{n-1}$
- For relatively prime m and n, $\phi(mn) = \phi(m)\phi(n)$

Theorem 4.4

Number of Elements of Each Order in a Cyclic Group

If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.

Theorem 4.4

Number of Elements of Each Order in a Cyclic Group

If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.

Corollary

Number of Elements of Order d in a Finite Group

In a finite group, the number of elements of order d is a multiple of $\phi(d)$.

Subgroup Lattice

The relationship among the various subgroups of a group can be illustrated with a subgroup lattice of the group. This is a diagram that includes all the subgroups of the groups of the group and connects a subgroup H at one level to a subgroup K at a higher level with a sequence of line segments if and only if H is a proper subgroup of K.