CS 5319
Advanced Discrete Structure

Lecture 12:
Introduction to Group Theory II

Outline

- Introduction
- Groups and Subgroups
- Generators
- Cosets (and Lagrange's Theorem)
- Permutation Group (and Burnside's Theorem)
- Group Codes

Generators

Generators

- Let $(A, \star)$ be an algebraic system where $\star$ is a closed binary operation
- Let $B = \{ a_1, a_2, \ldots \}$ be a subset of A
- Let B_1 denote the subset of A which contains

  (1) all elements of B ; and

  (2) the element $a_j \star a_k$ for all a_j, a_k in B

- B_1 is called the set generated directly by B

Generators

- Similarly, we let

$$B_2 \; = \text{ the set generated directly by } B_1$$

$$B_{i+1} = \text{ the set generated directly by } B_i$$

- Let B^* denote the union of B_1, B_2, …

➔ $(B^*, \star)$:= the subsystem generated by B

➔ any element in B^* is said to be generated by B

Note : $\star$ is a closed operation on B^* (why?)

Generators

Ex : Consider the algebraic system $(N, +)$.

Let $B = \{ 3, 5 \}$

➔ $B_1 = \{ 3, 5, 6, 8, 10 \}$

$B_2 = \{ 3, 5, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 20 \}$

$\ldots$

$B^* = N - \{ 1, 2, 4, 7 \}$

Generators

- If $B^* = A$, B is called a generating set of $(A, \star)$

  Ex : { 1, 3 } is a generating set of $(N, +)$

- When $(A, \star)$ is a group, and $(B^*, \star)$ is finite, then $(B^*, \star)$ is a subgroup of $(A, \star)$ [why?]

  Ex : A = all possible angular rotation

  $\star$ = combination of two angular rotations

  $B = \{ 120° \}$, $B^* = \{ 0°, 120°, 240° \}$

  ➔ $(B^*, \star)$ is a subgroup

Generators

- When a group has a generating set of one element, the group is called a cyclic group

Ex : $(Z_n , \oplus_n)$ is a cyclic group,

with generating set = { 1 }

Ex : $(Z_7 \backslash\{0\} , \otimes_n)$ is a cyclic group,

with generating set = { 3 }

~~Ex : (Z, +) is not a cyclic group~~

Generators

Lemma 1 :

All cyclic groups are commutative.

Proof : Let $(A, \star) =$ a cyclic group

$\{ a \} =$ generating set of $(A, \star)$

➔ each element in A is equal to a^j for some j

Since $\star$ is associative, we have

$$a^j \star a^k = a^k \star a^j$$

➔ All cyclic groups must be commutative

Generators

- There is an interesting problem that is related to generator called addition chain problem

- Given a positive integer n , a sequence

$$a_1, a_2 , \ldots, a_r$$

is called an addition chain for n if

$$a_1 = 1, \; a_r = n \, ,$$

and each a_j is the sum of two previous terms (possibly equal)

Generators

Ex : Some addition chains for 9 are show below.

(a) 1, 2, 3, 4, 5, 6, 7, 8, 9

(b) 1, 2, 4, 8, 9

(c) 1, 2, 3, 4, 5, 9

(d) 1, 2, 3, 6, 9

Generators

- Given an integer n, the addition chain problem is to find the shortest addition chain for n
- This problem is extremely interesting, and was studied rather extensively
  - We do not know how to find the shortest chain, but there are two simple ways to find relatively short chain

Generators

- Method 1 (Binary Method) :

  We generate the chain for n in reverse order, based on recursion, stopping when $n = 1$:

  If n = even, recursively generate $n / 2$

  If n = odd, recursively generate $n - 1$

  Ex : Addition Chain for 45

  1, 2, 4, 5, 10, 11, 22, 44, 45 (9 steps)

Generators

- Method 2 (Factor Method) :

  If n can be factored into $p \times q$, we can find the chains for p and q first, and use these chains to construct a chain for n

  Suppose chain for p : $1, p_1, p_2, \ldots, p_r$

  chain for q : $1, q_1, q_2, \ldots, q_s$

  ➔ $q_1, q_2, \ldots, q_s, p_1 q_s, p_2 q_s, \ldots, p_r q_s$
  is a chain for n

Generators

- Ex : Addition Chain for 5 : 1, 2, 4, 5

  Addition Chain for 9 : 1, 2, 4, 8, 9

  ➔ Addition Chain for 45 :

  1, 2, 4, 8, 9, 18, 36, 45 (8 steps)

- It is known that the length of the shortest addition chain for n is bounded by :

  $[\ \log_2 n + \log_2 \nu(n) - 2.13,\ \ \log_2 n + \nu(n) - 1\ ]$

  where $\nu(n)$ = #1's in binary representation of n

Cosets and Lagrange’s Theorem

Cosets

- Let $(A, \star)$ be an algebraic system where $\star$ is a binary operation (not necessarily closed)
- Let a be an element in A, and H be a subset of A

Definition (Cosets) :

$a \star H := \{ a \star x \mid x \in H \}$ is called the left coset of H with respect to a

$H \star a := \{ x \star a \mid x \in H \}$ is called the right coset of H with respect to a

Cosets

Ex :

Suppose an initial rotation of either 0°, 120°, or 240° is followed by a subsequent rotation of 60°.

What are the possible total angular rotations?

➔ This is equal to the right coset of

{ 0°, 120°, 240° } with respect to 60°

Cosets

- Suppose $(A, \star)$ is a group, and $(H, \star)$ is a subgroup of $(A, \star)$

Theorem 1 :

Let $a \star H$ and $b \star H$ be two cosets of H.

Then it follows that either

(1) $a \star H$ and $b \star H$ are disjoint, or

(2) they are identical

Cosets

Proof : Suppose they are not disjoint

➔ there exists a common element, say f

➔ there exist h_1 and h_2 in H such that

$$f = a \star h_1 = b \star h_2$$

so that $a = b \star h_2 \star h_1^{-1}$

Now, for any x in $a \star H$, x must be in $b \star H$, since $x = a \star h_3 = b \star h_3 \star h_2 \star h_1^{-1}$

$= b \star h_4$ for some h_3 and h_4 in H

Cosets

Proof (cont) :

Thus, we have

$$a \star H \subseteq b \star H$$

Similarly, we have

$$b \star H \subseteq a \star H$$

➔ the two cosets are identical

Lagrange's Theorem

- Suppose $(A, \star)$ is a finite group, and $(H, \star)$ is a subgroup of $(A, \star)$

  Fact : Any coset of H has the same size as H

Theorem 2 (Lagrange) :

> The order of any subgroup of a finite group divides the order of the finite group

Lagrange's Theorem

Proof : Suppose $(A, \star)$ is a finite group,

and $(H, \star)$ is a subgroup of $(A, \star)$

➔ Identity element e must be in H

➔ For each element a in A,

a is in the left coset $a \star H$

➔ Let r be # of distinct left cosets of H

Since each element is in some coset of H,
and each coset has equal size ➔ $r\,|H| = |A|$

Lagrange's Theorem

Corollary :

Suppose the order of a group G is prime.

Then we have :

1. There is no non-trivial subgroup of G
2. Any set with one element (except identity) is a generating set of G
3. G is a cyclic group

Lagrange's Theorem

Ex : $(Z_7 , \oplus_7)$ is a group of order 7.

1. The only subgroups of $(Z_7 , \oplus_7)$ are :

   $(\{ 0 \} , \oplus_7)$ and $(Z_7 , \oplus_7)$
2. Any element (except 0) is a generator.

   For instance, from { 2 }, we can generate

   2, 4, 6, 1, 3, 5, 0
3. From (2), we see that $(Z_7 , \oplus_7)$ is cyclic