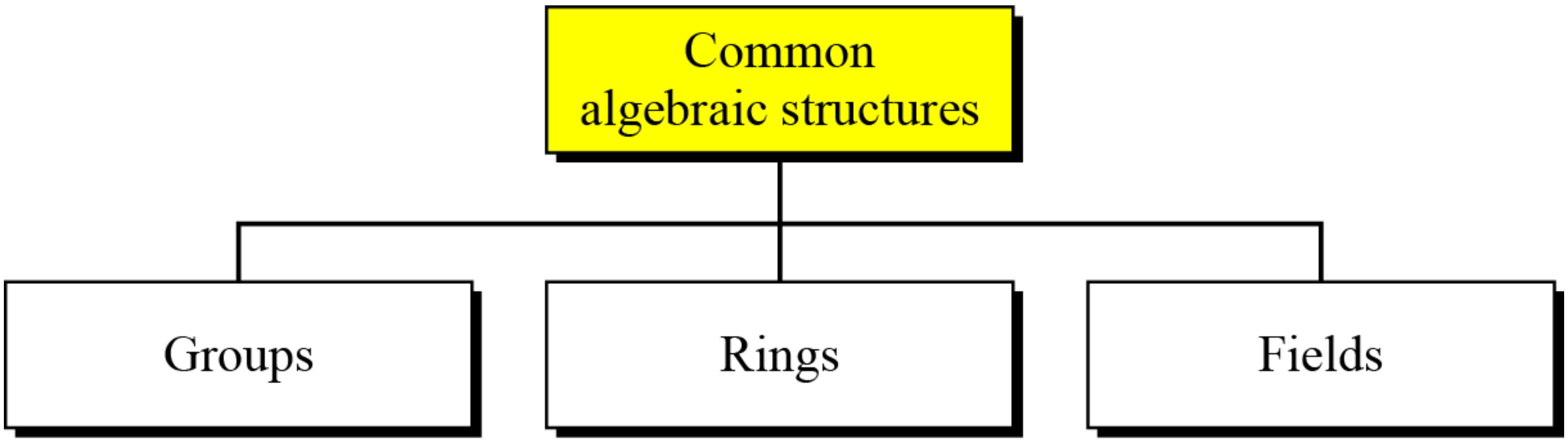
ALGEBRAIC STRUCTURES

Introduction

- Some sets of numbers, such as Z, Z_n, Z_n^*, Z_p, Z_p^*
- Cryptography requires sets of integers and specific operations that are defined for those sets.
- The combination of the set and the operations that are applied to the elements of the set is called an algebraic structure.

Introduction



Common algebraic structure

Group

- A group (G) is a set of elements with a binary operation (•) that satisfies four properties (or axioms).

- A commutative group satisfies an extra property, commutativity:

- Closure
- Associativity
- Commutativity
- Existence of identity
- Existence of inverse

Group

- Closure
  - If a and b are elements of G, then $c = a \bullet b$ is also an element of G.
- Associativity
  - If a, b and c are elements of G, then
    $(a \bullet b) \bullet c = a \bullet (b \bullet c)$
- Existence of identity
  - For all a in G, there exist an element e, called the identity element, such that $e \bullet a = a \bullet e = a$
- Existence of inverse
  - For each a in G, there exists an element a’, called the inverse of a, such that $a \bullet a' = a' \bullet a = e$

Group

- A Commutative group (Abelian group) is group in which the operator satisfies four properties plus an extra property that is commutativity.
  - For all a and b in G, we have a • b = b • a

Group

- Example:
- The set of residue integers with the addition operator,

$$G = < Z_n , +>,$$

- is a commutative group. We can perform addition and subtraction on the elements of this set without moving out of the set.

Group

- Application
  - Although a group involves a single operation, the properties imposed on the operation allow the use of a pair of operations!!!!

Group

- The set Zn* with the multiplication operator, G = <Zn*, ×>, is also an abelian group.

Group

- Finite Group
- Order of a Group
- Subgroups

Group

- Finite Group:
  - If the set has a finite number of elements; otherwise, it is an infinite group.

- Order of a Group $|G|$
  - The number of elements in the group.
  - If the group is finite, its order is finite

- Subgroups
  - A subset H of a group G is a subgroup of G if H itself is a group with respect to the operation on G

SubGroup

- Subgroups(cont.)
  - If $G=\langle S, \bullet \rangle$ is a group, $H=\langle T, \bullet \rangle$ is a group under the same operation, and T is a nonempty subset of S, then H is a subgroup of G
  - If a and b are members of both groups, then $c=a \bullet b$ is also member of both groups
  - The group share the same identity element
  - If a is a member of both groups, the inverse of a is also a member of both groups
  - The group made of the identity element of G, $H=\langle \{e\}, \bullet \rangle$, is a subgroup of G
  - Each group is a subgroup of itself

SubGroup

- Find all subgroups of Group G = $\langle Z_6, + \rangle$

SubGroup

- Find all subgroups of Group G = <Z_6, +>
- Z_6 = {0,1,2,3,4,5} has subgroups
- {0}
- {0,3}
- {0,2,4}
- {0,1,2,3,4,5}
- {0,1,5} -> valid subgroup?

SubGroup

- Find all subgroups of Group G = $<Z_{10^*}, X>$

SubGroup

- Find all subgroups of Group G = $<Z_{10*}, X>$
- Z_{10*} = {1,3,7,9} has subgroups
- {1}
- {1,9}
- {1,3,7,9}

SubGroup

- Is the group $H = <Z_{10}, +>$ a subgroup of the group $G = <Z_{12}, +>$?

SubGroup

- Is the group $H = \langle Z_{10}, + \rangle$ a subgroup of the group $G = \langle Z_{12}, + \rangle$?

- Solution: No.
- Although H is a subset of G, the operations defined for these two groups are different.
- The operation in H is addition modulo 10; the operation in G is addition modulo 12.

Cyclic Subgroups

- If a subgroup of a group can be generated using the power of an element, the subgroup is called the cyclic subgroup.

$$\boxed{a^n \rightarrow a \bullet a \bullet \ldots \bullet a \quad (n \text{ times})}$$

Cyclic Subgroups

- Four cyclic subgroups can be made from the group G = <Z6, +>.

- $H_1 = <\{0\}, +>$,
- $H_2 = <\{0, 2, 4\}, +>$,
- $H_3 = <\{0, 3\}, +>$,
- $H_4 = G$.

Cyclic Subgroups

- Four cyclic subgroups can be made from the group G = <Z6, +>. They are H1 = <{0}, +>, H2 = <{0, 2, 4}, +>, H_3 = <{0, 3}, +>, and H4 = G.

$$0^0 \bmod 6 = 0$$

$$\begin{aligned}
1^0 &\bmod 6 = 0 \\
1^1 &\bmod 6 = 1 \\
1^2 &\bmod 6 = (1 + 1) \bmod 6 = 2 \\
1^3 &\bmod 6 = (1 + 1 + 1) \bmod 6 = 3 \\
1^4 &\bmod 6 = (1 + 1 + 1 + 1) \bmod 6 = 4 \\
1^5 &\bmod 6 = (1 + 1 + 1 + 1 + 1) \bmod 6 = 5
\end{aligned}$$

$$\begin{aligned}
2^0 &\bmod 6 = 0 \\
2^1 &\bmod 6 = 2 \\
2^2 &\bmod 6 = (2 + 2) \bmod 6 = 4
\end{aligned}$$

$$\begin{aligned}
3^0 &\bmod 6 = 0 \\
3^1 &\bmod 6 = 3
\end{aligned}$$

$$\begin{aligned}
4^0 &\bmod 6 = 0 \\
4^1 &\bmod 6 = 4 \\
4^2 &\bmod 6 = (4 + 4) \bmod 6 = 2
\end{aligned}$$

$$\begin{aligned}
5^0 &\bmod 6 = 0 \\
5^1 &\bmod 6 = 5 \\
5^2 &\bmod 6 = 4 \\
5^3 &\bmod 6 = 3 \\
5^4 &\bmod 6 = 2 \\
5^5 &\bmod 6 = 1
\end{aligned}$$

Cyclic Subgroups

- Find all cyclic subgroups from the group $G = \langle Z_{10}^{*}, \times \rangle$.

Cyclic Subgroups

- Find all cyclic subgroups from the group G = <Z10*, ×>.

- G has only four elements: 1, 3, 7, and 9. The cyclic subgroups are H1 = <{1}, ×>, H2 = <{1, 9}, ×>, and H3 = G.

$1^0 \bmod 10 = 1$

$3^0 \bmod 10 = 1$
$3^1 \bmod 10 = 3$
$3^2 \bmod 10 = 9$
$3^3 \bmod 10 = 7$

$7^0 \bmod 10 = 1$
$7^1 \bmod 10 = 7$
$7^2 \bmod 10 = 9$
$7^3 \bmod 10 = 3$

$9^0 \bmod 10 = 1$
$9^1 \bmod 10 = 9$

Cyclic Groups

- A cyclic group is a group that is its own cyclic subgroup.

$$\boxed{\{e, g, g^2, \ldots, g^{n-1}\}, \text{ where } g^n = e}$$

Cyclic Groups

- Three cyclic subgroups can be made from the group $G = <Z10*, \times>$.
- G has only four elements: 1, 3, 7, and 9. The cyclic subgroups are $H1 = <\{1\}, \times>$, $H2 = <\{1, 9\}, \times>$, and $H3 = G$.

- The group $G = <Z6, +>$ is a cyclic group with two generators, $g = 1$ and $g = 5$.

- The group $G = <Z10*, \times>$ is a cyclic group with two generators, $g = 3$ and $g = 7$.

Cyclic Groups

- Lagrange's Theorem
- Assume that G is a group, and H is a subgroup of G. If the order of G and H are $|G|$ and $|H|$, respectively, then, based on this theorem, $|H|$ divides $|G|$.

- Order of an Element
- The order of an element is the order of the cyclic group it generates.

Cyclic Groups

- In the group G = <Z6, +>, the orders of the elements are:
- ord(0) = 1,
- ord(1) = 6,
- ord(2) = 3,
- ord(3) = 2,
- ord(4) = 3,
- ord(5) = 6.

Cyclic Groups

- In the group $G = \langle Z_{10}^*, \times \rangle$, the orders of the elements are:

  $ord(1) = 1$, $ord(3) = 4$, $ord(7) = 4$, $ord(9) = 2$.