

# CSCI 124/224

## Discrete Structures II: Subgroups and Rings

Poorvi L. Vora

Recall that a group consists of a set  $G$  and a related operation  $\diamond$  such that  $G$  is closed under  $\diamond$ , has an identity wrt  $\diamond$ , and each element in  $G$  has inverses wrt  $\diamond$  (wrt= with respect to). Also,  $\diamond$  is an associative operation. A subgroup of  $G$  is a group inside  $G$  wrt the same operation  $\diamond$ .

### 1 A Subgroup

**Definition** A *subgroup* of group  $G$  with operation  $\diamond$ , is a subset  $H$  of  $G$ , i.e.  $H \subseteq G$ , such that  $H$  is itself a group under operation  $\diamond$ .

This also implies the following:

- *Closure*  
 $H$  is closed under the operation, i.e.  $x, y \in H \Rightarrow x \diamond y \in H$ .
- *Associativity*  
The operation is associative, i.e.  $(x \diamond y) \diamond z = x \diamond (y \diamond z)$  (This holds in any case because the operation  $\diamond$  is associative because  $G$  is a group, independent of whether  $H$  is a subgroup. Hence, for subgroups, this condition need not be checked).
- *Identity*  
There is an element  $e \in H$  such that  $x \diamond e = e \diamond x = x$ . As  $G$  is a group and has an identity wrt  $\diamond$ , all that needs to be checked is if this identity is in  $H$ .
- *Inverses exist*  
Every element in  $H$  has an inverse in  $H$ , i.e.  $\forall g \in H, \exists \bar{g} \in H$  such that  $\bar{g} \diamond g = g \diamond \bar{g} = e$ .

### 2 Examples

**Example 1:** To see that  $m\mathbb{Z}$ , the set of all integer multiples of integer  $m$ , is a subgroup of  $\mathbb{Z}$  with  $\diamond = +$ , we check each of the requirements of a subgroup (note that associativity need not be checked):

- *Subset*  
All integer multiples of integer  $m$  are integers, hence  $H$  is a subset of  $G$ .

- *Closure*

Suppose  $x, y \in m\mathbb{Z}$ , i.e.  $x = k_1m$  and  $y = k_2m$  for some integers  $k_1$  and  $k_2$ . Their sum,  $x + y = (k_1 + k_2)m$  is also a multiple of  $m$ , that is,  $x + y \in m\mathbb{Z}$ . Hence the closure condition holds.

- *Identity*

The element 0 is the identity in  $G = \mathbb{Z}$  with operation  $\diamond = +$ . We need only check that it belongs to  $H$ , and it does, because 0 is a multiple of  $m$ ,  $0 = 0m$ .

- *Inverses exist*

Given  $g = km \in m\mathbb{Z}$ , consider  $\bar{g} = -km$ ,  $\bar{g} \diamond g = e$ , and  $\bar{g} \in m\mathbb{Z}$ . Hence inverses exist in  $H$ .

Hence  $H$  is a subgroup of  $G$ .

**Example 2:** Consider some integer  $n \leq p - 1$  for prime  $p$ . The set  $H = \{x \in G \mid x^n = 1 \text{ mod } p\}$  is a subset of the group  $G = \mathbb{Z}_p^* = \{1, 2, \dots, p - 1\}$  with operation  $\diamond = \times \text{ mod } p$ . We check each of the requirements of a subgroup:

- *Subset*

$H$  is defined as a set of elements from  $G$ , hence  $H$  is a subset of  $G$ .

- *Closure*

Suppose  $x, y \in H$ , i.e.  $x^n = 1 \text{ mod } p$  and  $y^n = 1 \text{ mod } p$ . Then,  $(xy)^n = x^n y^n = 1 \text{ mod } p$ , and  $xy \in H$ . Hence the closure condition holds.

- *Identity*

The element 1 is the identity in  $G$  with operation  $\diamond$ . We need only check that it belongs to  $H$ , and it does, because  $1^n = 1 \text{ mod } p$ .

- *Inverses exist*

Given  $g \in H$ , consider  $\bar{g} = g^{n-1}$ ,  $\bar{g} \diamond g = g^n = 1 \text{ mod } p$ . Further,  $(g^{n-1})^n = g^{n(n-1)} = (g^n)^{n-1} = 1 \text{ mod } p$  and  $\bar{g} \in H$ . Hence inverses exist in  $H$ .

Hence  $H$  is a subgroup of  $G$ . (examples of  $H$  include:  $\{x \mid x^3 = 1 \text{ mod } 7\} \subset \mathbb{Z}_7$  and  $\{x \mid x^2 = 1 \text{ mod } 5\} \subset \mathbb{Z}_5$ . The first is the set  $\{1, 2, 4\}$ , and the second the set  $\{1, 4\}$ ).

### 3 Rings

We have seen that the integers have both an additive and a multiplicative structure. The set of integers does not contain multiplicative inverses, however, the set of integers satisfies all other requirements for a group with respect to multiplication. We similarly see this also in the set of integers modulo  $m$ . Motivated by this, we define a ring. Before we do so, we define a special type of group, the abelian group (a group in which the operation,  $\diamond$ , is commutative):

**Definition 2:** A group  $G$  is an *abelian* group if,  $\forall x, y, \in G, x \diamond y = y \diamond x$ .

Examples of abelian groups include all groups wrt addition or addition *mod*  $m$  for integer  $m$ . The group of invertible matrices with operation multiplication is, however, not abelian.

**Definition 3:** A *ring* is a set  $R$  with two associated operations:  $\diamond$  (similar to addition) and  $\circ$  (similar to multiplication), such that the following hold:

- $R$  is an abelian group wrt  $\diamond$
- $R$  satisfies all properties of a group wrt  $\circ$ , except the inverse property:
  - $\circ$  is associative
  - $R$  is closed wrt  $\circ$ . i.e.  $x, y \in R \Rightarrow x \circ y \in R$ .
  - The identity wrt  $\circ$  exists: *exists*  $\mathbf{1} \in R$  such that,  $\forall x \in R, x \circ \mathbf{1} = \mathbf{1} \circ x = x$
- $\circ$  distributes over  $\diamond$  (much as multiplication distributes over addition):
  - $a \circ (b \diamond c) = (a \circ b) \diamond (a \circ c)$
  - $(b \diamond c) \circ a = (b \circ a) \diamond (c \circ a)$