Math 521: Lecture 5

Arun Ram
University of Wisconsin-Madison
480 Lincoln Drive
Madison, WI 53706
ram@math.wisc.edu

1 Operations

An **operation** on a set S is a map $S \times S \to S$.

Let

$$\begin{array}{rcl} \circ\colon S \times S & \to & S \\ (s_1, s_2) & \mapsto & s_1 \circ s_2 \end{array}$$

be an operation on S.

The operation $\circ$ is **associative** if it satisfies the condition

$$\text{If } s_1, s_2, s_3 \in S \text{ then } (s_1 \circ s_2) \circ s_3 = s_1 \circ (s_2 \circ s_3).$$

The operation $\circ$ is **commutative** if it satisfies the condition

$$\text{If } s_1, s_2 \in S \text{ then} s_1 \circ s_2 = s_2 \circ s_1.$$

Examples. The operation

$$\begin{array}{rcl} \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z} \\ (i, j) & \mapsto & i + j \end{array}$$

is both commutative and associative.

The operation

$$\begin{array}{rcl} \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z} \\ (i, j) & \mapsto & i - j \end{array}$$

is noncommutative and nonassociative.

2 Monoids, groups, rings and fields

A **monoid without identity** is a set G with an operation

$$\begin{array}{rcl} G \times G & \to & G \\ (i, j) & \mapsto & i?j \end{array} \qquad \text{such that}$$

(a) ($?$ is associative) if $i, j, k \in G$ then $(i?j)?k = i?(j?k)$,

A **monoid** is a set G with an operation

$$\begin{array}{rcl} G \times G & \to & G \\ (i,j) & \mapsto & i?j \end{array} \qquad \text{such that}$$

(a) ($?$ is associative) if $i, j, k \in G$ then $(i?j)?k = i?(j?k)$,

(b) (G has an identity) There exists an element $! \in G$ such that if $y \in G$ then $!?y = y?! = y$,

An **commutative monoid** is a set G with an operation

$$\begin{array}{rcl} G \times G & \to & G \\ (i,j) & \mapsto & i+j \end{array} \qquad \text{such that}$$

(a) G is a monoid,

(b) if $i, j \in G$ then $i + j = j + i$.

A **group** is a set G with an operation

$$\begin{array}{rcl} G \times G & \to & G \\ (i,j) & \mapsto & i?j \end{array} \qquad \text{such that}$$

(a) ($?$ is associative) if $i, j, k \in G$ then $(i?j)?k = i?(j?k)$,

(b) (G has an identity) There exists an element $! \in G$ such that if $y \in G$ then $!?y = y?! = y$,

(c) (G has inverses) if $y \in G$ there is an element $y^\sharp \in G$ such that $y?y^\sharp = y^\sharp?y =!$ where $!$ is the identity in G.

An **abelian group** is a set G with an operation

$$\begin{array}{rcl} G \times G & \to & G \\ (i,j) & \mapsto & i+j \end{array} \qquad \text{such that}$$

(a) G is a group,

(b) if $i, j \in G$ then $i + j = j + i$.

The identity element of an abelian group is denoted 0.

A **ring without identity** is a set R with two operations

$$\begin{array}{rcl} R \times R & \to & R \\ (i,j) & \mapsto & i+j \end{array} \qquad \text{and} \qquad \begin{array}{rcl} R \times R & \to & R \\ (i,j) & \mapsto & ij \end{array}$$

such that

(a) R with the operation $+$ is an abelian group,

(b) ($+$ is commutative) If $i, j \in R$ then $i + j = j + i$,

(c) (multiplication is associative) if $i, j, k \in R$ then $(ij)k = i(jk)$,

(d) (distributive laws) if $i, j, k \in R$ then $i(j+k) = ij + ik$ and $(i+j)k = ik + jk$.

A **ring** is a ring without identity R such that there is an element $1 \in R$ such that if $y \in R$ then $1y = y1 = y$.

A **commutative ring** is a ring such that if $x, y \in R$ then $xy = yx$.

A **field** is a commutative ring $\mathbb{F}$ such that if $y \in \mathbb{F}$ and $y \neq 0$ then there is an element $y^{-1} \in \mathbb{F}$ with $yy^{-1} = y^{-1}y = 1$.

A **division ring** is a ring $\mathbb{D}$ such that if $y \in \mathbb{D}$ and $y \neq 0$ then there is an element $y^{-1} \in \mathbb{D}$ with $yy^{-1} = y^{-1}y = 1$.

The integers $\mathbb{Z}$ with the addition operation is an abelian group. The integers $\mathbb{Z}$ with the addition and multiplication operations is a ring. The rationals $\mathbb{Q}$ with the operations addition and multiplication is a field.