LECTURE 6

September 18, 2023

1. Groups: Binary Operations on a Set

DEFINITION 1.1. Let X be a set. A binary operation on X is a function $* : X \times X \to X$. Informally, it is a rule that assigns to every pair $(a, b) \in X \times X$ another member of X, usually denoted $a * b$.

EXAMPLE 1.2. On $\mathbb{Z}$, "$+$" and "$\cdot$" are binary operations.

EXAMPLE 1.3. For $\mathbb{N}$, denote $\mathcal{M}_n(\mathbb{R})$ to be the set of all $n \times n$ matrices with real entries. Then "$+$" and "$\cdot$" (matrix multiplication) are binary operations on $\mathcal{M}_n(\mathbb{R})$. If $A, B \in \mathcal{M}_n(\mathbb{R})$, then sometimes $A \cdot B \neq B \cdot A$, hence why the order matters.

EXAMPLE 1.4. On $\mathbb{R}^n$, with $n \geq 2$, then "$+$" is a binary operation on $\mathbb{R}^n$.

EXAMPLE 1.5. However, "$\langle \cdot, \cdot \rangle$" is not a binary operation on $\mathbb{R}^n$ because for $x, y \in \mathbb{R}^n$, $\langle x, y \rangle \notin \mathbb{R}^n$.

EXAMPLE 1.6. On $\mathbb{N}$, define $m * n = \frac{m}{n}$ is not a binary operation on $\mathbb{N}$ since sometimes $\frac{m}{n} \notin \mathbb{N}$.

EXAMPLE 1.7. On $\mathbb{Q}$, $a * b = \frac{a}{b}$, is also not a binary operation on $\mathbb{Q}$ since sometimes it is not defined.

2. Integers Modulo n

NOTATION 2.1. For $n \in \mathbb{N}$, denote $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$. Therefore, if $a \in \mathbb{Z}_n$, then $a \in \mathbb{Z}$ and $0 \leq a < n$.

REMARK 2.2. Usual addition and multiplication are *not* binary operations on $\mathbb{Z}_n$. For example, define $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Then take $3, 4 \in \mathbb{Z}_5$ and define the operation "$+$". Then $3+4 = 7$, so it is not a binary operation since $7 \notin \mathbb{Z}_5$.

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then there exists a unique $r \in \mathbb{Z}_n$ such that $a \equiv r \pmod{n}$. In particular, r is the remainder of a divided by n.

DEFINITION 2.3. Let $n \in \mathbb{N}$. For $a, b \in \mathbb{Z}_n$, define the following:

(1) $a +_n b$ as the unique $r \in \mathbb{Z}_n$ such that $a + b \equiv r \pmod{n}$. This means $a +_n b \in \mathbb{Z}_n$ and $a + b \equiv a +_n b \pmod{n}$.

(2) $a \cdot_n b$ as the unique $s \in \mathbb{Z}_n$ such that $a \cdot b \equiv s \pmod{n}$. This means $a \cdot_n b \in \mathbb{Z}_n$ and $a \cdot b \equiv a \cdot_n b \pmod{n}$.

EXAMPLE 2.4. Take $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Take $3, 4 \in \mathbb{Z}_5$, $3 +_5 4 = 2$ because $3 + 4 = 7 \equiv 2 \pmod{5}$ and $2 \in \mathbb{Z}_5$. Similarly, take $2, 3 \in \mathbb{Z}_5$, then $2 \cdot_5 3 = 1$ since $2 \cdot 3 = 6 \equiv 1 \pmod{5}$ and $1 \in \mathbb{Z}_5$.

PROPOSITION 2.5. *Let $n \in \mathbb{N}$. Then the following hold for $a, b \in \mathbb{Z}_n$:*

(1) $a +_n b = b +_n a$ *and* $a \cdot_n b = b \cdot_n a$ *(commutativity of "$+_n$" and "$\cdot_n$")*
(2) $(a +_n b) +_n c = a +_n (b +_n c)$ *and* $(a \cdot_n b) \cdot_n c = a \cdot_n (b \cdot_n c)$. *(associativity of $+_n$ and $\cdot_n$)*
(3) *There exists an additive identity and multiplicative identity $0 \in \mathbb{Z}_n$ and $1 \in \mathbb{Z}_n$, respectively, such that $a +_n 0 = a$ and $a \cdot_n 1 = a$, respectively.*
(4) $a \cdot_n (b +_n c) = a \cdot_n b + a \cdot_n c$ *(distributive property)*
(5) *There exists $a\ b \in \mathbb{Z}_n$ such that $a +_n b = 0$*
(6) *For $b \in \mathbb{Z}_n$, the following are equivalent:*
   (a) *There exists $k \in \mathbb{Z}_n$ such that $b \cdot_n k = 1$*
   (b) $\gcd(n, b) = 1$.

PROOF. We will prove (2) and (6). Let $a, b, c \in \mathbb{Z}_n$ be arbitrary and write $a+b \equiv a+_n b \pmod{n}$ (this is a defining property) Write $a+b+c \equiv (a+_n b)+c \pmod{n}$. Similarly, $b + c \equiv b +_n c \pmod{n}$ and add a to both sides of this equation so that $a + b + c \equiv a + (b +_n c) \pmod{n}$. Thus, $(a +_n b) + c \equiv (a+_n b)+_n c \equiv a+b+c \pmod{n}$. Similarly,$a+(b+_n c) \equiv a+_n(b+_n c) \equiv a+b+c \pmod{n}$, and therefore, $(a +_n b) +_n c \equiv a +_n (b +_n c) \pmod{n}$. Since both sides are in $\mathbb{Z}_n$, they are equal.

To show that (6) is true, we show that (a) $\Rightarrow$ (b). Let $b, k \in \mathbb{Z}_b$ such that $b \cdot_n k = 1$. We will show that $\gcd(n, b) = 1$. Indeed, $1 = b_n k \equiv bk \pmod{n}$, which meas that $bk \equiv 1 \pmod{n}$. By definition $n \mid bk - 1$. Then by definition, there exists a $m \in \mathbb{N}$ such that $bk - 1 = mn$ and so $bk - mn = 1$. Since $d = \gcd(n, b)$ divides both n and b, it will also divide any linear combination of n and b, i.e. $bk - mn = 1$. But then, $d = \gcd(n, b) = 1$. Now show that (b) $\Rightarrow$ (a). Assume that $\gcd(n, b) = 1$. By Bezout's Theorem, there exists $x, y \in \mathbb{Z}$ such that $xb + yn = 1$. In other words, $xb - 1 = -yn$, which implies that $x \cdot b \equiv 1 \pmod{n}$. Take $k \in \mathbb{Z}_n$ such that $x \equiv k \pmod{n}$. Then we claim that $b \cdot_n k = 1$. Indeed, $b \cdot_n k \equiv b \cdot k \equiv b \cdot x \equiv 1 \pmod{n}$ and so $b \cdot_n k = 1$, as desired. □

3. Multiplication and Addition Tables of $\mathbb{Z}_4$

Let us consider $\mathbb{Z}_4$ given below for operations $+_n$ and $\cdot_n$.

$\cdot_n$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$+_n$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2