III

Algebraic Structures - continued

Groups revisited - Let $G = \langle \mathbb{Z}_{12}, +_{12} \rangle$ and the subgroup $H = \langle \{0, 3, 6, 9\}, +_{12} \rangle$

Composition table for H:

$+_{12}$	0	3	6	9
0	0	3	6	9
3	3	6	9	0
6	6	9	0	3
9	9	0	3	6

- We note that H is closed under the group operation (mod 12 addition).
- Since $\langle \mathbb{Z}_{12}, +_{12} \rangle$ is Abelian (commutative), we know that the left cosets will equal the right cosets.

left cosets

$0 + H = \{0, 3, 6, 9\}$
$1 + H = \{1, 4, 7, 10\}$
$2 + H = \{2, 5, 8, 11\}$

right cosets

$H + 0 = \{0, 3, 6, 9\}$
$H + 1 = \{1, 4, 7, 10\}$
$H + 2 = \{2, 5, 8, 11\}$

$\therefore$ H is a normal subgroup

Recall also, that the number of left cosets of G relative to H is called the index of H under G, $[G : H]$

$|G| = 12$ $\qquad$ $|H| = 4$

$$[G : H] = 12/4 = 3$$

- Composition table for $\langle \{1, -1, i, -i\}, \cdot \rangle$

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Is this group a cyclic group?
i.e. Is every element $g \in G$ expressible as g^k for some k
... well let $g = i$
i.e. $g^1 = i$
then $g^2 = i \cdot i$
$= -1$
$g^3 = (-1) g$
$= (-1)(i)$
$= -i$
$g^4 = g^2 \cdot g^2$
$= (-1) \cdot (-1) = 1$

Since this group G is cyclic,
i.e. it is an instance of C_4.
Hence $\langle \{1, -1, i, -i\} \rangle$ is isomorphic to $\langle \mathbb{Z}_4, +_4 \rangle$

hw : ~~Find an isomorphism~~
$f : \langle \mathbb{Z}_4, +_4 \rangle \to \langle \{1, -1, i, -i\}, \cdot \rangle$; yes!

Note : $H = \langle \{1, -1\}, \cdot \rangle$ is a subgroup, where $|H| = 2$

Since $\langle \{1, -1, i, -i\}, \cdot \rangle$ is an instance of C_4 this group G is abelian.
$\therefore$ H is a normal subgroup of $\langle \{1, -1, i, -i\}, \cdot \rangle$
The two distinct cosets of H in G are:
$1 \cdot H = \{1, -1\}$
$i \cdot H = \{i, -i\}$

And $[G : H] = 4/2 = 2$

Additional structures with one operation

Def: $\langle S, \circ \rangle$ is a groupoid if $\circ$ is a composition s.t. i) $\circ$ is closed

e.g. $\langle \mathbb{Z}^+, + \rangle$ is a groupoid
$\langle \mathbb{N}, - \rangle$ is not.

Def: $\langle S, \circ \rangle$ is a semigroup if $\circ$ is a composition s.t. i) $\circ$ is closed
ii) $\circ$ is associative

e.g. $\langle \mathbb{Z}^+, + \rangle$ is a semigroup
$\langle \mathbb{Z}, - \rangle$ is not.

Def: $\langle M, \circ \rangle$ is a monoid if $\circ$ is a composition s.t. i) $\circ$ is closed
ii) $\circ$ is associative
iii) $\langle M, \circ \rangle$ possesses an identity e s.t. $e \circ x = x \circ e = x \quad \forall x \in M$

e.g. let Σ be a finite alphabet, say, $\Sigma = \{0, 1\}$
then $\langle \Sigma^*, \circ \rangle$ where Σ^* is the Kleene closure of Σ
i.e. $\Sigma^* = \bigcup_{i=0}^{\infty} \Sigma^i$, in English all words over Σ, $\{\epsilon, 0, 1, 00, \ldots\}$
and where $\circ$ is the concatenation of words, e.g. $10 \circ 11 = 1011$
$\langle \Sigma^*, \circ \rangle$ is a monoid; why is $\langle \Sigma^*, \circ \rangle$ not a group?

Algebraic Structures with two Operations.

Def.: A ring $R = \langle R, \circ, * \rangle$ is an algebraic structure s.t. R is a set, $\circ, *$ are compositions on R and the following hold:

i) $\langle R, \circ \rangle$ is an abelian group.

ii) $\langle R, * \rangle$ is a semigroup

iii) $*$ distributes over $\circ$, i.e.,

$$x * (y \circ z) = (x * y) \circ (x * z) \text{ and}$$
$$(y \circ z) * x = (y * x) \circ (z * x)$$
$$\forall x, y, z \in R$$

- Examples of rings:

$$\langle \mathbb{Z}, +, \cdot \rangle$$
$$\langle \mathbb{Q}, +, \cdot \rangle$$
$$\langle \mathbb{R}, +, \cdot \rangle$$
$$\langle \mathbb{C}, +, \cdot \rangle$$
$$\langle \mathbb{Z}_n, +_n, \cdot_n \rangle$$

Def: In a ring $\langle R, \circ, * \rangle$, the unique identity in $\langle R, \circ \rangle$ is called zero (denoted 0).

Thm: In any ring, 0 is a two-sided zero in the semigroup $\langle R, * \rangle$

Special classes of rings

i) commutative ring − R is a ring and $\langle R - \{0\}, *\rangle$ is commutative

ii) ring with identity − R is a ring and there is an identity (1) in $\langle R - \{0\}, *\rangle$

iii) ring without divisors of 0 − R is a ring and $\langle R - \{0\}, *\rangle$ is closed

iv) integral domain − R is a ring and $\langle R - \{0\}, *\rangle$ satisfies:

- identity
- commutivity
- closure

v) skew field − R is a ring and $\langle R - \{0\}, *\rangle$ is a group

vi) field − R is a ring and $\langle R - \{0\}, *\rangle$ is an abelian group

Examples of rings

- Let S be the set of reals of the form

$x + y\sqrt{2}$ $x, y \in \mathbb{Z}$

$\langle S, +, \cdot \rangle$ is a ring.

$+, \cdot$ ordinary addition, multiplication

We require: I) $\langle S, + \rangle$ is an abelian group

i) $(x_1 + y_1\sqrt{2}) + (x_2 + y_2\sqrt{2}) = (x_1 + x_2) + (y_1 + y_2)\sqrt{2}$

closure ✓

ii) $x_1 + y_1\sqrt{2} + (x_2 + y_2\sqrt{2} + x_3 + y_3\sqrt{2}) \stackrel{?}{=}$

$(x_1 + y_1\sqrt{2} + x_2 + y_2\sqrt{2}) + x_3 + y_3\sqrt{2}$

$x_1 + y_1\sqrt{2} + (x_2 + x_3) + (y_2 + y_3)\sqrt{2} = (x_1 + x_2 + x_3) + (y_1 + y_2 + y_3)\sqrt{2}$

associativity ✓

iii) identity $e = 0 + 0\sqrt{2}$

iv) inverses $(x + y\sqrt{2})^{-1} = -x - y\sqrt{2}$

v) $+$ is commutative

$$\left[(x_1 + y_1\sqrt{2}) + (x_2 + y_2\sqrt{2})\right] \stackrel{?}{=} \left[(x_2 + y_2\sqrt{2}) + (x_1 + y_1\sqrt{2})\right]$$

$$\left[(x_1 + x_2) + (y_1 + y_2)\sqrt{2}\right] = \left[(x_2 + x_1) + (y_2 + y_1)\sqrt{2}\right] ✓$$

II) $\langle R, \cdot \rangle$ is a semigroup

i) closure $(x_1 + y_1\sqrt{2}) \cdot (x_2 + y_2\sqrt{2}) = (x_1 \cdot x_2 + 2y_1y_2)$
$+ (x_1 \cdot y_2 + x_2y_1)\sqrt{2}$ ✓

ii) associativity verify this

III $\cdot$ distributes over $+$ "

In fact S is a commutative ring with identity

- Let $R = \{u, v, w, x\}$ where $+, \cdot$ defined below:

$+$	u	v	w	x
u	u	v	w	x
v	v	u	x	w
w	w	x	u	v
x	x	w	v	u

$\cdot$	u	v	w	x
u	u	u	u	u
v	u	v	w	x
w	u	w	w	u
x	u	x	u	x

$\langle R, +, \cdot \rangle$ is a commutative ring. Verify this.

- The set $T = \{0, e\}$ is a ring with two elements $+, \cdot$ defined as:

$+$	0	e
0	0	e
e	e	0

$\cdot$	0	e
0	0	0
e	0	e

0 is the zero of this ring
e is the identity (unity).

- $K = \{a, b, c, d\}$, $+, \cdot$ defined below:

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	a	a	a
d	a	b	c	d

$\langle K, +, \cdot \rangle$ is a ring, but it is not commutative (naturally, we mean that $\cdot$ is not commutative!)

note: $cd = a$ whereas $d \cdot c = c$.

→ Does this ring have an identity?
→ What is the zero?

- Once again $K = \{a, b, c, d\}$ however $\cdot$ defined differently

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	c

this $\langle K, +, \cdot \rangle$ is a commutative ring

- Let W be the set of all symbols of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ $a, b, c, d \in \mathbb{Z}$.

addition : $\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}$

multiplication : $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$

W is the ring of all matrices of order two over the integers.

W is not a commutative ring.

If a, b, c, d chosen to be rational (or real, or complex numbers) we would obtain the ring of all matrices of order two over the rationals (or reals, or complex numbers).

- let $S = \{a, b, c\}$, $\langle S, +, \cdot \rangle$ is a ring

+	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$\cdot$	a	b	c
a	a	a	a
b	a	b	?
c	a	?	?

- Make use of the distributive law to fill in mult. table
- Is this ring commutative?
- Does $\langle S, +, \cdot \rangle$ have an identity?

Examples of Fields

- $\langle \mathbb{R}, +, \cdot \rangle$ where $\mathbb{R}$ is the set of reals
  $\langle \mathbb{C}, +, \cdot \rangle$ $\mathbb{C}$ set of complex numbers
  $\langle \mathbb{Q}, +, \cdot \rangle$ $\mathbb{Q}$ set of rationals

→ Why is $\langle \mathbb{Z}, +, \cdot \rangle$ not a field ?
In fact $\langle \mathbb{Z}, +, \cdot \rangle$ is an integral domain.

Def: A field with q elements is called a finite field, or a Galois field, denoted by $GF(q)$.

examples of finite fields:

$S = \{0, 1\}$, $\langle S, +, \cdot \rangle$ is a field

+	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$GF(2)$

Why must a field have at least two elements?

GF(3)

$S = \{0,1,2\}$, $\langle S, +, \cdot \rangle$ with

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

GF(4)

$S = \{0,1,2,3\}$, $\langle S +, \cdot \rangle$ with

not mod 4 addition

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

not mod 4 multiplication

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

GF(2) is contained in GF(4)

However GF(2) is not contained in GF(3)

(see top of page)

Def. 2.4.2 : Let F be a field. A subset of F is called a subfield if it is a field under the inherited addition and multiplication. The original field F is then called an extension field of the subfield.

To prove that a subset of a finite field is a subfield

- it contains a nonzero element
- closed under +
- closed under ·

Thm. 2.4.3 : In any field, if $ab = ac$
and $a \neq 0$
then $b = c$

Proof : - Multiply by a^{-1}.

(In a field, it is always possible to cancel).

III

Vector Space

Def. 2.5.1: Let F be a field. The elements of F are called scalars. A set V is called a vector space, and its elements are called vectors

We require: vector addition operation

- $\bar{v}_i + \bar{v}_j = v_K$ for all $\bar{v}_i, \bar{v}_j, v_K \in V$

scalar multiplication operation

- $f_i \in F$, $\bar{v}_j \in V$ then
  $f_i \bar{v}_j = \bar{v}_K$, $\bar{v}_K \in V$.

The following axioms must hold:

1) $\langle V, + \rangle$ is an abelian group
2. $c(\bar{v}_1 + \bar{v}_2) = c\bar{v}_1 + c\bar{v}_2$, $\bar{v}_1, \bar{v}_2 \in V$, c: scalar
3. $1\bar{v} = \bar{v}$, $\forall \bar{v} \in V$ Distributivity
   and $(c_1 + c_2)\bar{v} = c_1\bar{v} + c_2\bar{v}$ c_1, c_2 scalars
4. $(c_1 c_2)\bar{v} = c_1(c_2\bar{v})$ $\forall \bar{v} \in V$, c_1, c_2 scalars
   Associativity

The zero element of V is called the origin of V and is denoted by 0.

And $0\bar{v} = 0$ $\forall \bar{v} \in V$.

- The space of n-tuples over the real numbers : $\mathbb{R}^n$

→ (Addition notes on Vector Spaces and Linear Algebra -
→ check my class notes for I 0600 (Fundament Algorithms): Lessons 3-5