MAT 232 :: Fall 2024

Algebraic Structures; Groups

To finish off the semester, we're going to briefly look at what can be called *algebraic structures*.

The technical definition(s) of "algebra" in math is(are) not exactly the same as the common notion of solving equations using letters to represent unknown quantities.

Broadly speaking, we mean a *system of computation* and the study of properties of such a system.

The "computation" we study does not have to be complicated - in fact, we start with literally the simplest form of computation possible: take two things and combine them according to some specified operation.

The things are usually (but not necessarily) numbers or variable symbols. The specified operation may be something familiar - good old fashioned addition, multiplication, etc. - or it may be strange and difficult to describe.

Believe it or not, such systems of computation are the backbone of a lot of higher level abstract mathematics and have applications in computer science, physics, all over the place.

TWO THINGS = ONE THING

DEF 1. Let A be a nonempty set. A *binary operation on* A is a function from $A \times A$ to A.

$A \times A = \{(x,y) \mid x, y \in A\}$ Ex: $A = \{1,2,3\}$

$(1,1), (1,3), (1,2), (2,2), (2,3), (3,3) \in A \times A$

$*: A \times A \longmapsto A$ Ex: $(2,3) \longmapsto 3$ or $2 * 3 = 3$

$(1,1) \longmapsto 3$ or $1 * 1 = 3$

DEF 2. The set A is said to be *closed under* $*$ if and only if, for all $x, y \in A$, $x * y \in A$.

The result of the $*$ operation "cannot leave" A.

DEF 3. An *algebraic structure* or *algebraic system* is a nonempty set A that is closed under a specified binary operation.

Ex: $A = \{1, 2, 3\}$ AND $*$'s defined

$1 * 2 =$ $\qquad$ $2 * 3 =$

$1 * 3 =$ $\qquad$ $\vdots$

$1 * 1 =$

→ *Asking "Is $(A, *)$ an algebraic structure?" is equivalent to asking "Is A closed under $*$?"*

DEF 4. If A is a finite set, the *order* of $(A, *)$ is the number of elements in A.

EX 1. Let $A = \{1, 2, 3\}$. Define the operation $*$ on A to be determined by the following *Cayley table*:

FIRST

	$*$	1	2	3
SECOND	1	3	2	1
	2	3	1	3
	3	2	3	3

$1 * 2 = 3$
$2 * 1 = 2$
$3 * 3 = 3$
$2 * 3 = 3$

NOTE: ALL OUTCOMES ARE ELEMENTS OF THE ORIGINAL SET $A = \{1, 2, 3\}$, SO A IS CLOSED UNDER $*$, I.E. $(A, *)$ FORM AN ALGEBRAIC STRUCTURE OF ORDER 3.

There are basically no restrictions on how a closed binary operation is defined - beyond the simple requirement that when you operate on two elements from a set, the outcome is an element from that set. That said, some binary operations have desirable properties.

DEF 5. Let $(A, *)$ be an algebraic system. Then

a) $*$ is COMMUTATIVE on A if and only if for all $x, y \in A$, $x * y = y * x$

b) $*$ is ASSOCIATIVE on A if and only if for all $x, y, z \in A$, $(x * y) * z = x * (y * z)$

c) an element e of A is an *identity element* for $*$ if and only if for all $x \in A$, $x * e = e * x = x$

d) if A has an identity element e, and a and b are in A, then b is an INVERSE of a if and only if $a * b = b * a = e$.

EX 2. Consider $(\mathbb{Z}, \cdot)$ STANDARD MULTIPLICATION

SET OF ALL INTEGERS

① IS $\mathbb{Z}$ CLOSED UNDER $\cdot$? YES $\Rightarrow (\mathbb{Z}, \cdot)$ IS AN ALGEBRAIC STRUCTURE.
② IS $\cdot$ COMMUTATIVE? YES
③ IS $\cdot$ ASSOCIATIVE? YES
④ IS THERE AN IDENTITY ELEMENT? For $z \in \mathbb{Z}$, $z \cdot 1 = z$. YES!
⑤ ↳ INVERSE? $z \cdot \underline{\quad} = 1$ FOR SOME Z: IF $z=1$, THEN ITS INVESE IS 1.

$4 \cdot \underline{\tfrac{1}{4}} = 1$ ± 1 have inverses, ONLY TWO ELEMENTS!

$\frac{1}{4} \notin \mathbb{Z}$

EX 3. Consider $(\mathbb{Z}, +)$

COMM. ASSOC. } $\mathbb{Z}$ + ✓

IDENT ELE. ⇝ $z + 0 = z$

↳ INVERSES? ⟶ YES − EVERY ELEMENT HAS AN INVERSE

$$z + (-z) = \underset{e}{0}$$

DEF 6. $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$

EX 4. Consider $(\mathbb{Z}_6, +)$

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

[ADDITION MOD 6]

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$0 + 3 = 3$
$1 + 3 = 4$
$2 + 3 = 5$
$3 + 3 = 6$
$\vdots$
$5 + 3 = \underbrace{8}_{\text{NOT IN } \mathbb{Z}_6} = 2$

$\frac{8}{6} = 1$ REM. 2

IDENTITY ELEMENT: YEP

$0 + \underline{0} = 0$
$1 + \underline{5} = 0$
$2 + \underline{4} = 0$
$3 + \underline{3} = 0$
$4 + \underline{2} = 0$
$5 + \underline{1} = 0$

EX 5. Let $A = \{1, 2, 3\}$. Consider the three operations $\circ$, $\cdot$, and $*$ defined on A according to the following Cayley tables.

a)

$\circ$	1	2	3
1	1	2	3
2	1	2	3
3	1	2	3

NOPE

COMM. $\rightsquigarrow 1 \circ 2 = 2 \;\&\; 2 \circ 1 = 1$

ASSOC. $\rightsquigarrow (1 \circ 2) \circ 3 = 1 \circ (2 \circ 3)$

$1 \circ 3 = 1 \circ 2$

$1 = 1$

NOTE: Need to verify all possible triples to determine associativity.

ID.EL.? $1 \circ \underline{1/2/3} = 1$, $2 \circ \underline{1/2/3} = 2$, $3 \circ \underline{1/2/3} = 3$ ✓

↳ INV. $\underline{\quad} \circ 1 = 1$, $\underline{\quad} \circ 2 = 2$, $\underline{\quad} \circ 3 = 3$

NONE

b)

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

COMM.? ✓

ASSOCIATIVE? $(1 \cdot 2) \cdot 3 = 1 (2 \cdot 3)$

$1 \cdot 3 = 1 \cdot 3$

$2 = 2$

ID.ELE? $1 \cdot \underline{2} = 1$
$2 \cdot \underline{2} = 2$
$3 \cdot \underline{2} = 3$

Yes, the e is $\underline{2}$.

ID. ELE INVERSE? $1 \cdot \underline{?} = 2 = 1 \cdot 3$ ✓
$2 \cdot \underline{?} = 2 = 2 \cdot 2$ ✓
$3 \cdot \underline{?} = 2 = 3 \cdot 1$ ✓

Yes there is per element.

All Elements have an inverse.

c)

$*$	1	2	3
1	3	3	1
2	1	1	2
3	1	2	3

An algebraic structure with "nice enough" properties deserves a special name. What properties constitute "nice enough"? That depends on the situation. But a canonical threshold for nicety is three things: associativity, existence of an identity element, *every* element has an inverse.

Recall that, in a sense, our goal is to keep things as simple as possible, so commutativity does not make the cut. If an algebraic structure has the three *required* properties - associativity, identity element, inverses - and *also* has commutativity, we'll have a special special name for that.

DEF 7. A *group* is an algebraic structure $(G, \cdot)$ such that:

- $a)$ the operation $\cdot$ is associative ✓
- $b)$ there is an identity element $e \in G$ for $\cdot$ ✓
- $c)$ every $x \in G$ has an inverse in G ✓

These are all a group.

ASSOCIATIVE
IDENTITY (Ex. $a \times \_ = a$)
↳ INVERSE (Ex. $\_ \times a = a$)
* ALSO COMMUTATIVE? ABELIAN

If, in addition, the operation $\cdot$ is commutative, the group is called *abelian.*

EX 6. Which algebraic structures from Example 5 are groups? Abelian groups?

$\circ$	1	2	3
1	1	2	3
2	1	2	3
3	1	2	3

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

COM ✓ → Also ABELIAN GROUP
ASSO ✓
ID. ELEM ✓ = $e = 2$
→ INV. ✓
This is a GROUP ✓

$*$	1	2	3
1	3	3	1
2	1	1	2
3	1	2	3

Let's talk about some more examples. Before we do, a reminder of/introduction to some notation:

We've already encountered this notation: $\mathbb{Z}$ is the set of all integers. We can modify that in intuitive ways: $\mathbb{Z}^+$ is the set of positive integers; we've already encountered $\mathbb{Z}_6$ and the like.

$\{0,1,2,3,4,5\}$
$\Rightarrow$ mod 6

A couple other important sets:

$\mathbb{R}$ is the set of all real numbers

$\mathbb{Q}$ is the set of all rational numbers - i.e. the set of all $\dfrac{a}{b}$ where both a and b are integers (and $b \neq 0$)

$\mathbb{N}$ is the set of all natural numbers - sometimes this includes zero, sometimes it doesn't

We'll often want to denote "set exclusion" - i.e. excluding specific elements from a set. To do so, we'll just use the standard subtraction symbol. So $\mathbb{Z} - \{0\}$ is the set of all integers *except* zero; $\mathbb{Z}_8 - \{0, 4\}$ is the set $\{1, 2, 3, 5, 6, 7\}$.

0,4? NO! $\mathbb{Z}_8 - \{0,4\}$

Using this notation, we can briefly give several more examples:

- ⋆ The algebraic systems $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, and $(\mathbb{Z}, +)$ are all groups
- ⋆ The algebraic system $(\mathbb{R}, \cdot)$ is not a group because 0 does not have an inverse; $(\mathbb{R} - \{0\}, \cdot)$ and $(\mathbb{Q} - \{0\}, \cdot)$ are groups

NOT ASSOCIATIVE $\Rightarrow$ $4-0=4$ ✓ $0-4=-4$ ✗

- ⋆ The algebraic systems $(\mathbb{Z}^+, +)$, $(\mathbb{Z}, -)$, and $(\mathbb{Z} - \{0\}, \cdot)$ are not groups

NO IDENTITY

NO INVERSE

TRIVIAL GROUP

- ⋆ $(\{0\}, +)$ is a group
- ⋆ $(\{-1, 1\}, \cdot)$ is a group
- ⋆ Let $Aut(G)$ be the set of all automorphisms of a graph; define $\circ$ to be automorphism composition - i.e. if $\alpha, \beta \in Aut(G)$, then $\alpha \circ \beta$ enacts the automorphisms β then α in sequence; then $(Aut(G), \circ)$ is a group

Cool list. Let's back up and briefly look at one of those examples in a little more detail:

A.K.A. Caley table

EX 7. Construct operation tables for $(\{-1, 1\}, \cdot)$ and $(\mathbb{Z}_2, +)$. Compare.

×	-1	1
-1	1	-1
1	-1	1

NOTE:
e = 1
Every element is its own INVERSE

+	0	1
0	0	1
1	1	0

NOTE:
e = 0
Every element is its own inverse!

$0 + \underline{0} = 0$ ✓
$1 + \underline{0} = 1$
$1 + 1 = \underline{0}$ ✓ = e
$0 + 0 = \underline{0}$ ✓

EX 8. Are the two groups defined by the operation tables below the same group?

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

IDENTITY = e → b·e = b ✓
a·e = a ✓
c·e = c ✓
e·e = e ✓

INVERSE?
a·a = e ✓
b·b = e ✓
c·c = e ✓
e·e = e ✓

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

IDENTITY = 0

INVERSES?

1·3 = 0

NOT ALSO 1, NOT THE SAME GROUPS

EX 9. Define $*$ to be an operation on ordered pairs which enacts component-wise multiplication. Let $A = (\pm 1, \pm 1)$, i.e. all ordered pairs whose components are 1 or -1. Construct an operation table for $(A, *)$.

$*$	(1,1)	(1,-1)	(-1,1)	(-1,-1)
(1,1)	(1,1)	(1,-1)	(-1,1)	(-1,-1)
(1,-1)	(1,-1)	(1,1)	(-1,-1)	(-1,1)
(-1,1)	(-1,1)	(-1,-1)	(1,1)	(1,-1)
(-1,-1)	(-1,-1)	(-1,1)	(1,-1)	(1,1)

e = (1,1)

Every element is its own INVERSE!

* To verify associativity, we have to check all 3 things around.

↳ IF IT SAYS ITS A GROUP, WE ALREADY KNOW THAT IT'S ASSOCIATIVE...

Can you determine if the group $(A, *)$ is the same as either of the groups in Example 4?

In fact, there are a total of   groups of order four.

Our final examples *kinda* connect back to the "standard" use of the term *algebra*, in that we will try to solve equations involving variables . . . but this time in the context of a specified group.

EX 10. Within the group $(\mathbb{Z}_5, +)$, find all solutions to each of the following equations.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

a) $x + 1 = 0$ $\cancel{x = -1}$ 4 $1+4=5 \bmod 5 = 0$

$\boxed{x=4}$

b) $2x = 1$ $\cancel{x = \frac{1}{2}}$ 2x is not $2 \cdot x$, rather, $x+x=1$ → $3+3=1$ ✓

$\boxed{x=3}$

c) $2x + 1 = 0$

$2x = -1$

↓

$x + x = 4 \longrightarrow \boxed{x=2}$

EX 11. Consider the set $\mathbb{Z}_8$.

Construct an "initial" operation table for this set using standard multiplication.

$\cdot$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Within $(\mathbb{Z}_8, \cdot)$, find all solutions to the following equations.

a) $x \cdot 4 = 0$ $x = 0, 2, 4, 6$

b) $x^2 = 1$ $x \cdot x = 1$ $x = 1, 3, 5, 7$

c) $x^2 - 2x = 0$

$x \cdot (x-2) = 0$

$x = 0, 2, 4, 6$

Unfortunately, the above operation table demonstrates that $(\mathbb{Z}_8, \cdot)$ is *not* a group since

Not all elements have inverses

Can we salvage $(\mathbb{Z}_8, \cdot)$? What if we threw out elements which do not have inverses? This would require eliminating the elements:

$0, 2, 4, 6$

So now we're actually dealing with:

$(\mathbb{Z}_8 - \{0, 2, 4, 6\}, \cdot)$

Let's construct an operation table for our remnant group:

$\cdot_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Group!

Every element is it's own inverse.

Oh, so that's actually a group of order 4. Which one? D_4

Group

$(\mathbb{Z}_9 - \{0, 3, 6\}, \cdot)$

$(\mathbb{Z}_? - \{0\}, \cdot)$