Algebra Review
Modular Arithmetic
Boolean Algebra
Lecture 2

Termeh Shafie

algebraic properties* [axioms]
field properties

property	addition	multiplication
associative	$(a+b)+c = a+(b+c)$	$(ab)c = a(bc)$
commutative	$a+b = b+a$	$ab = ba$
identity	$a+0 = a = 0+a$	$a \cdot 1 = a = 1 \cdot a$
inverse	$a+(-a) = 0 = (-a)+a$	$a \cdot a^{-1}=1=a^{-1} \cdot a$ if $a \neq 0$
distributive	$a(b + c) = ab + ac$ and $ab + ac = a(b + c)$	

*given a, b, and c are real numbers

algebraic properties* [axioms]
properties of equality and inequality (1)

property	equality	inequality
multiplicative property of zero	$a \cdot 0 = 0 = 0 \cdot a$	
zero product	if $ab= 0$, then $a = 0$ or $b =0$	
reflexive	a = a	
symmetric	if $a = b$, then $b = a$	
transitive	if $a = b$ and $b = c$, then $a = c$	if $a > b$ and $b > c$, then $a > c$ if $a < b$ and $b < c$, then $a < c$
addition	if $a=b$, then $a+c = b+c$	if $a < b$, then $a + c < b + c$ if $a > b$, then $a + c > b + c$
subtraction	if $a = b$, then $a-c = b-c$	if $a < b$, then $a - c < b - c$ if $a > b$, then $a - c > b - c$

*given a, b, and c are real numbers

→

algebraic properties* [axioms]
properties of equality and inequality (2)

property	equality	inequality
multiplication	if $a = b$, then $ac = bc$	if $a < b$ and $c > 0$, then $ac < bc$ if $a < b$ and $c < 0$, then $ac > bc$ if $a > b$ and $c > 0$, then $ac > bc$ if $a > b$ and $c < 0$, then $ac < bc$
division	If $a = b$ and $c \neq 0$, then a/b = b/c	if $a < b$ and $c > 0$, then $a/c < b/c$ if $a < b$ and $c < 0$, then $a/c > b/c$ if $a > b$ and $c > 0$, then $a/c > b/c$ if $a > b$ and $c < 0$, then $a/c < b/c$
substitution	if $a = b$, then b can be substituted for a in any equation or inequality	

*given a, b, and c are real numbers

FOIL and PEMDAS

FOIL → **F**irst **O**uter **I**nner **L**ast

$(3y - 4)(5 + 2y) = 3y \cdot 5 = 15y$

$(3y - 4)(5 + 2y) = 3y \cdot 2y = 6y^2$

$(3y - 4)(5 + 2y) = (-4) \cdot 5 = (-20)$

$(3y - 4)(5 + 2y) = (-4) \cdot 2y = (-8y)$

$= 15y + 6y^2 - 20 - 8y$

$= 6y^2 + 7y - 20$

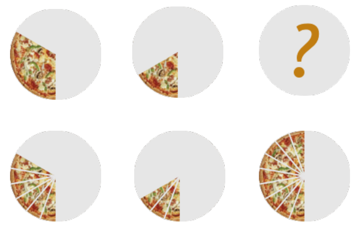
PEMDAS → **P**lease **E**xcuse **M**y **D**ear **A**unt **S**ally

1) Parentheses
2) Exponents
3) Multiplication
4) Division
5) Addition
6) Subtraction

fractions (or pizza math)

addition and subtraction: Least Common Denominator (LCD)

$\frac{1}{3} + \frac{1}{6} = ?$



$\frac{6}{18} + \frac{3}{18} = \frac{9}{18}$

generally

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d}{b \cdot d} + \frac{c \cdot b}{d \cdot b}$$

fractions (or pizza math)

division

$\frac{1}{2} \div \frac{1}{6}$

is actually asking how many

$\frac{1}{6}$ in $\frac{1}{2}$ $= 3$

generally

$$\frac{a}{b} \div \frac{c}{d} = \frac{a}{b} \times \frac{d}{c}$$

fractions (or pizza math)

multiplication

solving $\frac{2}{5} \times \frac{1}{2}$

$\frac{2}{5}$ $\quad \frac{2}{5} \times \frac{1}{2} = \frac{2}{10} = \frac{1}{5}$

generally

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

fractions

Addition

Same denominator: $\dfrac{a}{b}+\dfrac{c}{b}=\dfrac{a+c}{b}$

Different denominator: $\dfrac{a}{b}+\dfrac{c}{d}=\dfrac{a\cdot d}{b\cdot d}+\dfrac{c\cdot b}{d\cdot b}=\dfrac{ad+cb}{bd}$

Subtraction

Same denominator: $\dfrac{a}{b}-\dfrac{c}{b}=\dfrac{a-c}{b}$

Different denominator: $\dfrac{a}{b}-\dfrac{c}{d}=\dfrac{a\cdot d}{b\cdot d}-\dfrac{c\cdot b}{d\cdot b}=\dfrac{ad-cb}{bd}$

fractions

Multiplication $\dfrac{a}{b}\cdot\dfrac{c}{d}=\dfrac{ac}{bd}$

Division $\dfrac{a}{b}\div\dfrac{c}{d}=\dfrac{a}{b}\cdot\dfrac{d}{c}=\dfrac{ad}{bc}$

Double fractions $\dfrac{\frac{a}{b}}{c}=\dfrac{\frac{a}{b}\cdot b}{c\cdot b}=\dfrac{a}{cb}$ or $\dfrac{\frac{a}{b}}{\frac{c}{1}}=\dfrac{a\cdot 1}{c\cdot b}=\dfrac{a}{cb}$

Simplifying fractions ("building bridges") $\dfrac{\frac{a}{b}}{\frac{c}{d}}=\dfrac{a\cdot d}{b\cdot c}$

factoring

writing a polynomial as a product of polynomials

- The greatest common factor (GCF): largest quantity that is a factor of all the integers or polynomials involved

Example: 6, 8 and 46

$6 = 2\cdot 3$
$8 = 2\cdot 2\cdot 2$
$46 = 2\cdot 23$
$\Longrightarrow$ GCF is 2

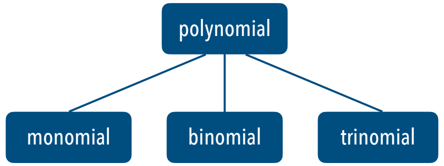
Example: $6x^5$ and $4x^3$

$6x^5 = 2\cdot 3\cdot x\cdot x\cdot x\cdot x\cdot x$
$4x^3 = 2\cdot 2\cdot x\cdot x\cdot x$
$\Longrightarrow$ GCF is $2\cdot x\cdot x\cdot x$

Exercise 1. a^3b^2, a^2b^5 and a^4b^7
$\Longrightarrow$ GCF is a^2b^2

factoring

writing a polynomial as a product of polynomials



examples:	$28x$	$5x+8xy$	$15xy-25y+18$
	$5a^3b$	$b^3/2+c/3$	$2a^2+5a+7$
	$2ax/3y$	$5m^2n^2+1/7$	$x^2/3+ay-6bz$

factoring

algorithm

1. Look for **common** factors and "factor them out"
2. Check if a **binomial/identity** applies
3. **Repeat** steps 1 and 2 until completion

Binomial identities and formulas

$$\boxed{\begin{aligned}(a+b)(a-b) &= (a-b)^2\\ (a+b)(a+b) &= a^2+2ab+b^2\\ (a-b)(a-b) &= a^2-2ab+b^2\\ (a+b)(a^2-ab+b^2) &= a^3+b^3\\ (a-b)(a^2+ab+b^2) &= a^3-b^3\\ a^3+3a^2b+3ab^2+b^3 &= (a+b)^3\\ a^3-3a^2b+3ab^2-b^3 &= (a-b)^3\end{aligned}}$$

factoring

Example:

$$\begin{aligned}4z^2+20z &= 4(z^2+5z)\\ &= 4z(z+5)\end{aligned}$$

Both of these are correct, but we often choose the version without exponent

Example:

$$\begin{aligned}9z^2-36 &= (9z)^2-6^2\\ &= (3z+6)(3z-6)\end{aligned}$$

why it's handy to know certain factor identities and (quadratic) binomials: $(a+b)(a-b)=(a-b)^2$

quadratic polynomials

Typically of the form

$$ax^2+bx+c=0, \quad \text{where } a \neq 0$$

Quadratic formula:

$$x_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$$

p/q formula:

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$$

(think $a=1$)

we will look at two ways of solving the square →

1. solving the square

Example. $25x^2+20x+4$

- possible factors of $25x^2$ are $\{x,25x\}$ or $\{5x,5x\}$ and possible factors of 4 are $\{1,4\}$ or $\{2,2\}$
- try each pair of factors until we find a combination that works (or exhausts all possible pairs)
- look for a combination that gives sum of the products of the outside terms and the inside terms equal to $20x$

Factors of $25x^2$	Factors of 4	Resulting Binomials	Product of Outside Terms	Product of Inside Terms	Sum of Products
$\{x,25x\}$	$\{1,4\}$	$(x+1)(25x+4)$ $(x+4)(25x+1)$	$4x$ x	$25x$ $100x$	$29x$ $101x$
$\{x,25x\}$	$\{2,2\}$	$(x+2)(25x+2)$	$2x$	$50x$	$52x$
$\{5x,5x\}$	$\{2,2\}$	$(5x+2)(5x+2)$	$10x$	$10x$	$20x$

- Answer: $(5x+2)(5x+2)$ (check via FOIL)

Exercise 2. Factor the polynomial $21x^2-41x+10$

solving quadratic equations by factoring

algorithm

step by step for solving a quadratic equation by factoring

1. write the equation in standard form.
2. factor the quadratic completely
3. set each factor containing a variable equal to 0
4. solve the resulting equations
5. check each solution in the original equation

example: solve $x^2 - 5x = 24$

$$x^2 - 5x - 24 = 0$$

$$x^2 - 5x - 24 = (x-8)(x+3) = 0$$

$x - 8 = 0$ and $x + 3 = 0$

$\implies x = 8$ and $\implies x = -3$

$8^2 - 5(8) = 64 - 40 = 24 \implies$ *true*
$(-3)^2 - 5(-3) = 9 - (-15) = 24 \implies$ *true*

Exercise 3. $4x(8x+9) = 5$

2. solving the square

algorithm

1. Divide by quadratic's coefficient and move constant to RHS
2. Divide x's coefficient by 2, square it and add it to both sides of the equation
3. Factor LHS into $(a \pm b)^2$ and simplify RHS
4. Take square root of both sides (remember: Solution on RHS will be of sign $\pm$)
5. Solve for x

Example. $4x^2 + 18x + 8$

$$4x^2 + 18x + 8 = 0 \quad | \div 4$$

$$x^2 + \frac{18}{4}x + 2 = 0 \quad | -2$$

$$x^2 + \frac{18}{4}x = -2 \quad | + \left(\frac{\frac{18}{4}}{2}\right)^2$$

$$x^2 + \frac{18}{4}x + \left(\frac{18}{8}\right)^2 = -2 + \left(\frac{18}{8}\right)^2$$

$$(x + 2.25)^2 = 3.0625 \quad | \sqrt{\ }$$

$$x + 2.25 = \pm 1.75 \quad | -2.25$$

$$x_1 = -0.5$$

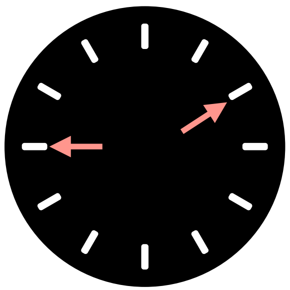
$$x_2 = -4$$

modular arithmetic

a fundamental tool in number theory ("the study of integers")

we are not interested in a fractions/decimal numbers as a result of division

deals with repetitive cycles of numbers and remainders



mod 12 arithmetic

If it's 9 o'clock and you add 5 hours, what time is it then?

That's modular arithmetic with mod 12:

$$9 + 5 \equiv 2 \pmod{12}$$

We read this as **"9 plus 5 is congruent to 2 modulo 12.**

What is modulo?

The modulus is the number at which you "wrap around" and keeping track of the remainder when dividing.

What is congruence? ➡

congruence modulo

Definition Congruence
We say that a is congruent to b modulo m if and only if m divides $a - b$

- Whether two integers a and b have the same remainder when divided by n
- Notation: $a \equiv b \mod m \leftrightarrow$ a is congruent to b modulo m
  $a \not\equiv b \mod m \leftrightarrow$ a is not congruent to b modulo m
- A congruence modulo asks whether or not a and b are in the same **equivalence class**

Example.
The numbers 31 and 46 are congruent $\mod 3$ because they differ by a multiple of 3.
We can write this as $31 \equiv 46 \mod 3$
Since the difference between 31 and 46 is 15, then these numbers also differ by a multiple of 5; i.e., $31 \equiv 46 \mod 5$

Exercise 4.
Find the equivalence classes of $\mod 3$

rules of modular arithmetic

Addition (and subtraction)

If $a \equiv b \mod m$ and
$c \equiv d \mod m$ then
$a + c \equiv b + d \mod m$

Example.
$87 \equiv 2 \mod 17$ and
$222 \equiv 1 \mod 17$
$\implies 87 + 222 \mod 17 \equiv 2 + 1 \mod 17 \equiv 3 \mod 17$

Multiplication

If $a \equiv b \mod m$ and
$c \equiv d \mod m$ then
$a \times c \equiv b \times d \mod m$

Example.
$9876 \equiv 6 \mod 10$ and
$17642 \equiv 2 \mod 10$
$\implies 9876 \times 17642 \mod 10 \equiv 6 \times 2 \mod 10 \equiv 2 \mod 10$

Division

A number is always congruent to its remainder (mod the divisor).

Example.
What is the remainder of 17×18 when it is divided by 19?
We know that $17 \equiv -2 \mod 19$ and $18 \equiv -1 \mod 19$
$\implies 17 \times 18 \equiv (-2) \times (-1) = 2 \mod 19$

modular arithmetic in the real world

Modular arithmetic is math for things that loop, repeat, or cycle whether it's time, data, computations or patterns.

- Computers use modular arithmetic constantly:
  - Memory addresses "wrap around" at a maximum size.
  - CPUs use mod operations to manage overflows.
  - Hashing functions in data storage use mod to assign data to buckets:
    index $=$ (hash value) mod (number of slots)
- Modern encryption (like RSA) is built on modular arithmetic and relies on operations like: $a^b \mod n$
  These are easy to compute in one direction but very hard to reverse (which keeps your data safe) which implies secure messaging, online payments, and digital signatures.
- Credit cards, ISBNs, and barcodes use modular arithmetic to detect typing errors.
  For example, a credit card's last digit (the check digit) is computed using mod 10 arithmetic on the other digits Implies error detection in identification numbers.

Boolean algebra

- consider the following statements that can be either TRUE or FALSE:
  - *Today is Monday AND it is raining*
  - *Today is Monday OR today is NOT Monday*
  - *Today is Monday AND today is NOT Monday*
- Boolean algebra allows us to formalize this sort of reasoning
- Boolean variables may take one of only two possible values: TRUE, FALSE
- there are three fundamental Boolean operators: AND, OR, NOT
- an exhaustive approach to describing when some statement is true (or false): TRUTH TABLES
- the = in Boolean algebra indicates equivalence

Boolean algebra

The three fundamental Boolean operators

1. Logical conjunction: AND $\wedge$
   True only when both A and B are true.

A	B	A AND B
F	F	F
F	T	F
T	F	F
T	T	T

A AND B $= A \wedge B = AB$

Boolean algebra

The three fundamental Boolean operators

1. Logical disjunction: OR ∨

True unless both A and B are false.

A	B	A OR B
F	F	F
F	T	T
T	F	T
T	T	T

A OR B = A ∨ B = A+B

Boolean algebra

The three fundamental Boolean operators

1. Logical negation: NOT ¬

True when A is false
False when A is true.

A	NOT A
F	T
T	F

NOT A= ¬ A = A′

Boolean algebra

Truth table

A	B	A′	B′	AB	A+B
F	F				
F	T				
T	F				
T	T				

Boolean algebra

Truth table

A	B	A′	B′	AB	A+B
F	F	T	T	F	F
F	T	T	F	F	T
T	F	F	T	F	T
T	T	F	F	T	T

Boolean algebra

Exercise 5. write the truth table for (A+B)B

A	B	A+B	(A+B)B
F	F		
F	T		
T	F		
T	T		

Truth tables can be used to prove equivalencies.
What have we proved in this table?