

## Groups, rings and fields MAT2200

## Introduction to abstract algebra

We look at sets (collection of "things") with some operations (structures)

Group : two operations

- product of two elements
- inverse of an element

⇒ modeling reversible operations on some system

Ex. translation on  $\mathbb{R}^n$

⇒ group of : set  $\mathbb{R}^n$

vector addition  $v + w$  as "product"

"-1 times" operation  $-v$  as "inverse"

Ex. rotation of the unit sphere  $S^2 \subset \mathbb{R}^3$

⇒ group of : set  $SO(3) = \{ \text{rotation matrix} \}$

$$X \in M_3 \mid X^T X = I_3, \det X = 1$$

matrix product  $XY$  as "product"

inverse matrix  $X^{-1} = X^T$  as "inverse"

→ same as composition of rotation ops.

Ring : three operations

- addition of two elements
- inverse (for the addition) of an element
- product of two elements

⇒ framework for polynomial equations, spectral theory (theory of eigenvalues)

Ex. arithmetic with imaginary unit

$$\text{set } \mathbb{Z}[\sqrt{-1}] = \{ a + b\sqrt{-1} \mid a, b \text{ integers} \}$$

or  $a + bi$

Ex. matrix ring

$$\text{set } M_n = \{ X : n \times n \text{-matrix (of real numbers)} \}$$

Ex. polynomial ring

$$\text{set } \mathbb{R}[X, Y] = \{ p : \text{polynom. in variables } X \& Y \text{ with real coefficients} \}$$

Fields: rings with one more operation!

- inverse (for the product) of nonzero elements

→ number system to solve polynomial equations

Ex. rational numbers  $\mathbb{Q}$

real numbers  $\mathbb{R}$ , complex numbers  $\mathbb{C}$

Ex. finite fields  $\mathbb{F}_p = \{ \text{integers modulo } p \}$

$p$ : prime number

i.e. discard differences by  $p, 2p, \dots$

→ represent numbers by  $0, 1, \dots, p-1$

$-1$  is identified with  $p-1, \dots$

One concrete goal: the Abel-Ruffini theorem

degree 5 polynom equations  $f(x) = 0$   
deg 5 poly

don't admit formulas for solutions with

arithmetic ops  $(+, -, \times, \div)$  and radicals  $\sqrt[n]{\phantom{x}}$

How: we look at symmetry of the field

$$K = \{ p(x) \mid p \text{ is a polynom with rational coeffs.} \}$$

for a sol. to  $f(x) = 0$  given by a group

(cont.) and analyze the structure of this group (Galois theory)

Main reference for the course

Fraleigh "A first course in abstract algebra"

## § 2 Binary operations

We often consider operations with two inputs and one output: addition / multiplication of numbers, matrixes, ...

mathematical model for such operations:

- set  $S$  (for the space of inputs & outputs)

- function  $S \times S \rightarrow S$

often use the infix notation  $a * b$   $a, b \in S$

we can (and do) use different symbols other than  $*$

subsystem for a binary op.

given  $S$  and  $*$  as above, a subset

$H \subset S$  is closed under  $*$  if we have

$$a, b \in H \Rightarrow a * b \in H$$

Ex.  $S = \mathbb{R}$ ,  $a * b = \text{sum of } a \text{ and } b$

$H = \mathbb{Z}$  (integers) closed under sum

$H = \{a \in \mathbb{R} \mid \text{irrational}\}$  not closed

$\sqrt{2} + 1$ ,  $-\sqrt{2}$  are in  $H$  but not their sum

first properties of binary ops  $(S, *)$

$*$  is commutative if we have  $a * b = b * a$

for any inputs  $a, b \in S$

Ex. sum of numbers, vectors, matrixes, ...

Non-ex. product of matrixes is not comm.

$$X = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, Y = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \Rightarrow XY = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$
$$YX = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

$*$  is associative if we have  $(a*b)*c = a*(b*c)$   
for all inputs  $a, b, c \in S$   
(this makes sense b/c  $a*b, b*c \in S$ )

Ex. additions, multiplications of numbers, matrixes, ...

Non-ex. commutator bracket of matrixes

$$[X, Y] = XY - YX \quad X, Y: n \times n\text{-matrix}$$

### §3 Isomorphism of binary structures and identity element

How to compare binary operations

$(S, *)$ ,  $(S', *')$  two sets w/ binary ops.

An isomorphism from  $(S, *)$  to  $(S', *')$  is  
a function  $\phi: S \rightarrow S'$  such that

- $\phi$  is bijective:  $\phi(a) = \phi(b) \Leftrightarrow a = b$   
 $\{\phi(a) \mid a \in S\} = S'$
- compatibility with  $*$  and  $'$ :  $\phi(a*b) = \phi(a)*'\phi(b)$

Ex.  $S = \mathbb{R}$ ,  $a*b$ : sum of  $a$  and  $b$

$S' = \{a \in \mathbb{R} \mid a > 0\}$ ,  $a*b'$ : product of  $a$   
and  $b$

$\Rightarrow \phi(a) = e^a$  is an isomorphism.

An identity element of  $(S, *)$  is an elem.  
 $e \in S$  satisfying  $e*a = a = a*e$

Ex. 0 for the addition of numbers, vectors, ...

$(S, *)$  has identity  $e$  &  $S \xrightarrow{\phi} S'$  is iso  $\Rightarrow \phi(e)$  is id.  
for  $(S', *')$