Modern algebra II — Lect 1

M. Khovanov
Sept 9, 2020

MA I: Groups set G, binary operation $G \times G \to G$ (multiplication)
unit element $1 \in G$, $1g = g1 = g \ \forall g \in G$, associativity $(fg)h = f(gh)$,
Inverse $g^{-1}g = gg^{-1} = 1$

Principle 1) Take any object X. The set of its symmetries $\mathrm{Sym}(X)$ is a group.
2) Objects with more symmetries are easier to understand.

Example: Any triangle $\triangle$ vs. isosceles triangle $\triangle$ vs equilateral triangle $\triangle$

$\mathrm{Sym}(\triangle) = \{1\}$ $\mathrm{Sym} \simeq C_2$ $\mathrm{Sym} \simeq S_3$

$c^2 = a^2 + b^2 - 2ab\cos\gamma$ simpler formulas all angles $= 60°$.

1) Symmetric group S_n: symmetries of n-element set $\{1, 2, \ldots, n\}$
2) $GL_n(\mathbb{R})$ symmetries (invertible linear maps) of vector space $\mathbb{R}^n$
3) Dihedral group D_n with $2n$ elements - symmetries of regular n-gon

$n=5$ case

4) Symmetry groups of graphs.
5) $O(n)$ - symmetries of ?

Exercise: a) find an object with the symmetry group C_n (cyclic group of order n)

b) Find an object with the symmetry group $C_n \times C_m$

this exercise has many answers. one up to isomorphism.

Finite groups $\longleftrightarrow$ number theory (only 1 group of order p, p a prime)

many groups when order is a product of many primes.

Principle Abelian groups are much easier to understand and classify than arbitrary groups.

fin. abelian group $\simeq C_{n_1} \times C_{n_2} \ldots \times C_{n_k}$ product of cyclic groups.

Many basic structures in math have two binary operations

$\mathbb{N} = \{0, 1, 2 \dots\}$ natural numbers $+, \cdot$

$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ integers $+, \cdot$

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

$n \times n$ matrices $A+B$, $A \cdot B$ $\quad M_n(\mathbb{R})$ $n \times n$ matrices with real coefficients.

<u>Def 1</u> A ring $R = (R, +, \cdot)$ is a set R with two binary operations $+, \cdot$ such that

(1) $(R, +)$ is an abelian group, i.e. operation $+$ turns R into an abelian group

(2) Operation $\cdot$ is associative. Shortcut ab instead of $a \cdot b$

(3) (interaction axioms between $+$ and $\cdot$). Left and right distributive laws hold

$$(a+b)c = ac + bc \quad , \quad c(a+b) = ca + cb.$$

(1) : $a+b = b+a$, $(a+b)+c = a+(b+c)$, 0 - identity of $(R, +)$ additive identity

$-a$ - additive inverse of a $\qquad 0 + a = a + 0 = a$

$$a + (-a) = (-a) + a = 0$$

(2) $(ab)c = a(bc)$. Usually require that multiplicative identity 1 exist (unity / identity element)

$1 \cdot a = a \cdot 1 = a \quad \forall a \in R$ [rings without 1 are also called rngs

We almost always consider rings with 1, assume this property.

Basic properties: $0 = 0 + 0$ (identity for $+$) $\Rightarrow 0 \cdot a = (0+0) \cdot a \Rightarrow$

$0 \cdot a = 0 \cdot a + 0 \cdot a$ distributivity

$0a = 0a + 0a$, abelian group under $+$

$b + b = b \Rightarrow b = 0$

$\Downarrow$

$0a = 0$

1) $0a = a0 = 0 \quad \forall a \in R$ multiplication by 0 is 0.

$$ab \rightsquigarrow \begin{cases} (-a)b \\ a(-b) \\ -(ab) = -ab \end{cases}$$

3 elements. what's the relation?

multiplication takes precedence over $-/+$

$0 = a + (-a) \Rightarrow 0 \cdot b = (a + (-a))b = ab + (-a)b$, and $0b = 0$

additive inverse of a

distributivity

$\Rightarrow 0 = ab + (-a)b \Rightarrow (-a)b = -ab$

likewise, $a(-b) = -ab$.

2) $(-a)b = a(-b) = -ab \quad \forall a, b \in R$

$\Rightarrow (-a)(-b) = ab \qquad (-1)(-1) = 1$

minus sign can be moved around in the product.

$-2 a = (-a) + (-a)$
$-1 \cdot a = -a$
$0 \cdot a = 0$
$1 \cdot a = a$
$2 \cdot a = a + a$

$n \in \mathbb{N} \qquad na = \underbrace{a + a + \dots + a}_{n \text{ times}} \qquad 3a = a + a + a$

$(-n)a = -(na) = -\underbrace{(a + a + a)}_{n \text{ times}} \qquad (-2)a = -a - a.$

Another way to think of na:

$1 \in R \Rightarrow 1 + 1 \in R$ denote by $2 \in R$, $\underbrace{1 + \dots + 1}_{n \text{ times}} \in R$ denote by $n \in R$

distinguish between n natural number and $n \in R$

negative: $-1 \in R$, $-n = (-1)n = \underbrace{(-1) + (-1) + \dots + (-1)}_{n \text{ times}} \in R$

map $\mathbb{Z} \longrightarrow R$

integers $\quad$ ring

$n \longrightarrow n$

same notation (for convenience) of different structures

$\boxed{\text{nice map, but not always injective}}$

then na is the product in R

different elements

$na = an$

both $a + \dots + a$ (if $n > 0$)

$(-a) + (-a) + \dots + (-a)$ if $n < 0$

rational real complex nxn matrices

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $M_n(\mathbb{R})$

$\mathbb{Q}_+ = \{a \in \mathbb{Q} \mid a \geq 0\}$

which are rings?

Multiplication in $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ is commutative.

Not in $M_n(\mathbb{R})$, $AB \neq BA$ for $n \times n$ matrices, usually $(n>1)$

<u>Def 2</u> Ring R is called commutative if $ab = ba$ $\forall a, b \in R$.

R is noncommutative if $ab \neq ba$ for some $a, b \in R$.

<u>Proposition</u> 1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are commutative rings

2) $M_n(\mathbb{R})$ is a noncommutative ring, for $n > 1$.

Generalized distributive laws

$(a+b)(c+d) = (a+b)c + (a+b)d = ac + bc + ad + bd$

b to the left of c

order in each product is important, unless R is commutative

By induction can prove

$(a_1 + a_2 + \dots + a_n)(b_1 + b_2 + \dots + b_m) = a_1b_1 + a_1b_2 + \dots + a_1b_m + a_2b_1 + a_2b_2 + \dots + a_nb_m$

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1, j=1}^{n, m} a_i b_j$$

$(a+b)(a+b) = aa + ab + ba + bb = a^2 + ab + ba + b^2$

Cannot simplify further in any R

$a^2 = a \cdot a$, $a^3 = a \cdot a \cdot a$ ..

Define $a^n = \underbrace{a \cdot a \cdot a \dots a}_{n}$ $n \geq 0$ since $\cdot$ is associative, this is well-defined

$a^0 = 1$

$(ab)^n = \underbrace{ababab \dots ab}_{n \text{ times}}$ does not simplify

If R is commutative, can further simplify

distinct in a non-comm ring

$(a+b)^2 = a^2+ab+ba+b^2 = a^2+2ab+b^2$

$(a+b)^3 = (a^2+ab+ba+b^2)(a+b) = a^3 + \underline{a^2b} + \underline{aba} + \underline{ab^2} + \underline{ba^2} + \underline{bab} + \underline{b^2a} + b^3 =$

distinct in a noncommutative ring

if R is commutative

$= \quad a^3+3a^2b+3ab^2+b^3$

<u>Prop</u> If R is commutative and $a, b \in R$ then

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

$\binom{n}{k}$ - binomial coefficient

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

this definition does not always work. $\frac{1}{m}$ not in R sometimes.

$n! = 1\cdot 2\cdot 3 \dots n.$

Cannot divide if $R=\mathbb{Z}$, for instance

Instead use inductive definition

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Pascal triangle

each term is an integer and makes sense in R

```
          1
        1   1
      1   2   1
    1   3   3   1
  1   4   6   4   1
1   5  10  10   5   1
        . . .
```

$(ab)^n = abab\dots ab \underset{\substack{\text{if } R \\ \text{commutative}}}{=} a^n b^n$

$(a-b)^2 = (a-b)(a-b) = a^2-ab-ba+b^2 \underset{}{\overset{\substack{\text{if } R \\ \text{commutative}}}{=}} a^2-2ab+b^2$

Ring $\mathbb{Z}/n$ of residues modulo n

fix $n > 0$ and consider an equivalence relation on $\mathbb{Z}$

$a \sim b$ if $n \mid a-b$ or $a = b + nk$, some $k \in \mathbb{Z}$

$a \sim a$, $a \sim b \Leftrightarrow b \sim a$, $a \sim b, b \sim c \Rightarrow a \sim c$

Equivalence classes $a + n\mathbb{Z}$. Representatives $0, 1, \ldots, n-1$

$0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots \quad n-1+n\mathbb{Z}$.

addition and multiplication in $\mathbb{Z}$ descends to a well-defined addition and multiplication on equivalence classes.

Define 1) $(a+n\mathbb{Z}) + (b+n\mathbb{Z}) = a+b+n\mathbb{Z}$

well-defined, $(\mathbb{Z}/n, +)$ is a cyclic group of order n.

2) $(a+n\mathbb{Z})(b+n\mathbb{Z}) = ab+n\mathbb{Z}$

need to check that definition does not depend on representatives of equivalence classes. if $a' = a + kn$, $b' = b + \ell n$

$a' + n\mathbb{Z} = a + n\mathbb{Z}$, $b' + n\mathbb{Z} = b + n\mathbb{Z}$. Need $a'b' + n\mathbb{Z} = ab + n\mathbb{Z}$

$a'b' = (a+kn)(b+\ell n) = ab + \underline{(a\ell + kb + k\ell n)}n$. differ by multiple of n

Get a commutative ring $\mathbb{Z}/n = (\mathbb{Z}/n, +, \cdot)$ of residues mod n.

<u>Question</u>: How can we check the axioms quickly? know that $\mathbb{Z}$ is a comm. ring.

Identity 1

<u>Example</u>: $n=6$ $\mathbb{Z}/6 = \{0,1,2,3,4,5\}$ $3+5 \equiv 2 \pmod 6$

or do write $3+5=2$

$3 \cdot 5 = 15 \equiv 3 \pmod 6$

$3 \cdot 5 = 3$ in $\mathbb{Z}/6$.

In this ring $2 \cdot 3 = 0$.

Zero ring

If $1=0$ in R then $1\cdot a = 0\cdot a \quad \forall a \in R$

$1\cdot a = a$ (axiom) $\quad 0\cdot a = 0$ (derived)

$\Rightarrow \quad a = 1\cdot a = 0\cdot a = 0 \quad \Rightarrow a=0.$ R is the zero ring, consists of a single element, $R=\{0\}$

Isomorphism of rings. A map $\alpha: R \longrightarrow S$ is an isomorphism of rings R and S if

(1) α is a bijection of sets

(2) α respects the binary operations $+, \cdot$ in R and S

$\alpha(a+b) = \alpha(a) + \alpha(b)$ for all $a,b \in R$

$\underset{\substack{\uparrow \\ \text{mult in } R}}{\alpha(ab)} = \underset{\substack{\uparrow \\ \text{mult in } S.}}{\alpha(a)\alpha(b)} \quad \forall a,b \in R$

α intertwines addition in R & S

α intertwines multiplication in R & S

Can also write 1_R for 1 in R. 1_S for 1 in S.

Exercise a) An isomorphism α takes $1 \in R$ to $1 \in S$.

b) $\alpha(0) = 0$

(c) $\alpha^{-1}: S \to R$ the inverse of α, also an isomorphism

(d) Composition of isomorphisms is an isomorphism.

General definition An isomorphism of objects is a bijection that respects all the structure.

Isomorphism of sets (have the same cardinality)

Isomorphism of vector spaces (have the same dimension)

Isomorphism of groups, ...

<u>Subrings</u> Given a ring R, a subring $S \subset R$ is a subset such that

(1) S is an abelian subgroup of R

(2) S is closed under multiplication

(3) S contains the identity 1 of R.

Sometimes condition (3) is dropped (I usually keep it). If you drop it, S may or may not contain its own identity element, different from that of R.

<u>Examples</u>

1) $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ subrings

2) $R \subset M_n(R)$ $\quad \{aI \mid a \in R\}$ $\quad I$ - identity matrix $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$

$$\left\{ \begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix}, a \in R \right\}$$

Let's look for rings in between $\mathbb{Z}$ and $\mathbb{Q}$. Take $n > 1$ and try to add $\frac{1}{n}$ to $\mathbb{Z}$. Then we must also add $\frac{1}{n} \cdot \frac{1}{n} = \frac{1}{n^2}$, $\frac{1}{n^2} \cdot \frac{1}{n} = \frac{1}{n^3}$ and so on. All's $\frac{1}{n^k}$ must be in the subring. & - taking sums, $\frac{m}{n^k}$, $m \in \mathbb{Z}$ must be in the subring

Define $\mathbb{Z}[\frac{1}{n}] = \left\{ \frac{m}{n^k} \mid m \in \mathbb{Z}, k \in \mathbb{N} \right\} \subset \mathbb{Q}$ $\qquad$ not unique $\frac{m}{n^k} = \frac{mn}{n^{k+1}}$

all rational numbers that can be written this way.

<u>Exercise</u> 1) $\mathbb{Z}[\frac{1}{n}]$ is a subring of $\mathbb{Q}$.

2a) How can you redefine $\mathbb{Z}[\frac{1}{n}]$ if you know the prime factors of n, $n = p_1^{k_1} \cdots p_r^{k_r}$? 2b) When is $\mathbb{Z}[\frac{1}{n}] = \mathbb{Z}[\frac{1}{k}]$?

3) ~~Are~~ Does $\mathbb{Q}$ have subrings beyond those we already know: $\mathbb{Z}$, $\mathbb{Z}[\frac{1}{n}]$, $\mathbb{Q}$?