Questions? Next time: Ilya Dumanski will cover me

New topic: rings and fields!

$\mathbb{Z}/n\mathbb{Z}$ ← has $+, \cdot$, both of these operations are important, so far we never considered them "together"

(considered $(\mathbb{Z}/n\mathbb{Z}, +)$ or $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$)

On the other hand we noticed that

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}, +) \xleftarrow{\sim} ((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$$

$(x \mapsto mx)$ ← $\mapsto m$

So these operations are in some sense "compatible"

What if we consider $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$?

Definition A **ring** R is a set

with

$$+ : R \times R \to R; \quad \cdot : R \times R \to R$$

addition

multiplication

such that:

a) $(R, +)$ ← commutative group, its identity is $0 \in R$

b) $(R, \cdot)$ ← monoid, identity is R

$((a \cdot b) \cdot c = a \cdot (b \cdot c))$

$(a \cdot 1 = a = 1 \cdot a)$

c) distributive law: $\forall a, b, c \in R$

$(a+b)\cdot c = a\cdot c + b\cdot c$

$\Leftrightarrow$

$c\cdot(a+b) = c\cdot a + c\cdot b$

$: (R,+) \to (R,+)$

$x \mapsto c\cdot x$

$x \mapsto x\cdot c$

homomorphisms

in particular, $x\cdot 0 = 0 = 0\cdot x \quad \forall x \in R$

(homomorphisms send identity to identity)

Remark: in general, people also consider rings without identity ($(R,\cdot)$ a semigroup), we will not consider this generalization

Examples: $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Commutative rings ($\cdot$ is commutative)

$$Mat_{2\times 2} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{R} \right\}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}$$

$\emptyset$

Exercise: check that $(Mat_{2\times 2}, +, \cdot)$ is a noncommutative ring

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$\#$

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Note: R ring $\rightsquigarrow$ $R^\times$ group

$$= \{x \in R \mid \exists y \in R,\ xy = yx = 1\}$$

Important subclass of rings:

R a division ring (skew field) if $R^\times = R - \{0\}$

field if 1) R a division ring

2) R commutative

Examples:

$\mathbb{Z}$ not a field

$\mathbb{Q}$ field

$\mathbb{R}$ field

$\mathbb{C}$ field

Claim $\mathbb{Z}/n\mathbb{Z}$ a field iff n a prime

proof. $(\mathbb{Z}/n\mathbb{Z})^\times = \{k = 1, \dots, n-1 \mid \gcd(k,n)=1\}$

coincides with $\{1, \dots, n-1\}$

iff n a prime

More examples of rings:

R a ring, define

$$R[X] := \left\{ \underbrace{a_n X^n + a_{n-1} X^{n-1} + \dots + a_0}_{\text{formal linear combination}} \;\middle|\; a_i \in R \right\}$$

X: formal symbol

For example, if $R = \mathbb{Z}$, then examples of elements of $\mathbb{Z}[x]$ are:

	deg	leading	constant	monic?
5	0	5	5	$\times$
$x+5$	1	1	5	$\checkmark$
$3x^2$	2	3	0	$\times$
$2x^{100}+1$	100	2	1	$\times$
$\vdots$				

terminology: if $f(x) \in R[x]$, then

$\deg(f(x))$ ← largest n s.t. coeff. in front of x^n in $f(x)$ is nonzero

leading term ← coefficient in front of x^n

$f(x)$ ← monic if leading term of f is 1

constant term ← a_0

Operations on polynomials: $f(x) = \sum a_i x^i$, $g(x) = \sum b_i x^i$

$$+ : R[x] \times R[x] \to R[x]$$

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \dots$$

$$(2X + 3) + (X^2 + 8x + 4) = X^2 + 10x + 7$$

$$\cdot : R[x] \times R[x] \to R[x]$$

$$f(x) \cdot g(x) = \sum_{i,j} a_i b_j \cdot x^{i+j} =$$

$$= \sum_k \left(\sum_{i+j=k} a_i b_j \right) x^k$$

$$(a_0 + a_1 x + a_2 x^2 + \dots)(b_0 + b_1 x + b_2 x^2 + \dots) =$$

$$= a_0 b_0 + (a_1 b_0 + a_0 b_1) x + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + \dots$$

$$(3 + 2x)(4 + 8x + x^2) = 12 + (24 + 8)x +$$

2 × 3 — 1 — 2 3 — 32

$$+ (3 + 16)x^2 + (2 \cdot 1)x^3$$

6 ✓ — 4 5 — 19 — 6

$$2x^3 + 19x^2 + 32x + 12$$

Proposition $(R[x], +, \cdot)$ is a ring

proof: direct computation → exercise (will be in PSet)

Roots of polynomials.

Elements $p \in R[x]$ define functions

$$\begin{array}{ccc} R & \to & R \\ \cup & & \cup \\ \alpha & \longmapsto & p(\alpha) = a_0 + a_1 \cdot \alpha + a_2 \cdot \alpha^2 + \dots + a_n \cdot \alpha^n \end{array}$$

$\alpha \in R$ is a <u>root</u> of p if $p(\alpha) = 0$

<u>Example</u>: $R = \mathbb{R}$, $x^2 - 2$ has roots

$$\alpha = \pm\sqrt{2}$$

$x^2 - 2x + 1$ has root 1

Next time we will prove the following theorem:

Thm: if R ← field, $f \in R[x]$

then $\boxed{\#\text{roots of } f \leq \deg f}$ (*)

From now on assume R ← commutative

Division with reminder:

Pick: $f(x), h(x) \in R[x]$, assume $h(x)$ ↗ monic

($h(x) = x^n +$ lower degree terms)

Then $\exists!$ $q(x), r(x) \in \mathbb{R}[x]$ s.t.

$$f(x) = q(x) \cdot h(x) + r(x), \quad \deg r(x) < \deg h(x)$$

Lemma: α a root of $f(x)$ iff

$$f(x) = (x-\alpha) \cdot q(x)$$

for some $q(x) \in \mathbb{R}[x]$

proof: if $f(x) = (x-\alpha)\, q(x)$

$$\Downarrow$$

$$f(\alpha) = (\alpha - \alpha) \cdot q(\alpha) = 0 \checkmark$$

if $f(\alpha) = 0$ then let's divide

$f(x)$ by $x - \alpha$:

$$f(x) = (x-\alpha)\, q(x) + r(x)$$

r: polynomial of $\deg < \deg(x-\alpha)$ (= 1)

$\deg r(x) = 0 \Rightarrow r(x) = r$ — just an element of R

$$f(\alpha) = (\alpha-\alpha)\, q(\alpha) + r = r$$

$f(\alpha) = 0 \Rightarrow r = 0$

We get $f(x) = (x-\alpha)\cdot q(x)$ ✓

Proof of Thm (*)

By induction on $\deg f = n$

Induction step: pick α a root of f.

Decompose $f(x) = (x-\alpha) \cdot \underbrace{q(x)}_{g}$

$\deg(q) = n-1$

Induction hypothesis $\leftarrow$ # roots of $q(x)$ is $\leq n-1$

If β $\leftarrow$ root of $f(x)$, $\beta \neq \alpha \Rightarrow$

$\Rightarrow \underbrace{(\beta-\alpha)}_{\neq 0} \cdot q(\beta) = 0$

$\Downarrow$ exists (use R-field) $(\beta-\alpha)^{-1}$

$q(\beta) = (\beta-\alpha)^{-1} \cdot 0 = 0 \Rightarrow \beta$ - root of q

So $\{\text{roots of } f\} = \{\alpha\} \cup \{\text{roots of } q\}$

$\Downarrow$

$\#\{\text{roots of } f\} \leq 1 + (n-1) = n$ $\checkmark$