lecture 2

Jan 24

Ring: $R = (R, +, \cdot)$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $M_n(\mathbb{R})$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$

1) $(R, +)$ - abelian group, 0

2) $(R, \cdot)$ $\cdot$ associative, 1 identity $1a = a1 = a$ $\forall a \in R$

3) distributivity $(a+b)c = ac + bc$, $a(b+c) = ab + ac$

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

($a + (-a)$: additive inverse of a; $(a+(-a))b = ab + (-a)b$: distributivity)

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

Likewise, $a(-b) = -ab$

$(-a)b = a(-b) = -ab$ minus sign can be moved around in the product

Powers of elements: $a^2 = a \cdot a$, $a^3 = a \cdot a \cdot a$

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

$(ab)^n = abab \cdots ab$ does not simplify

$= a^n b^n$ if R is commutative (or if a, b commute $ab = ba$)

Polynomials $R[x] = \left\{ \sum_{i=0}^{n} a_i x^i \mid a_i \in R \right\}$

To R add x, its powers x^n. Monomials ax^n

$(ax^n)(bx^m) = abx^{n+m}$.

Extend to sums $\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{i=0, j=0}^{n, m} a_i b_j x^{i+j}$

Addition is termwise

$f(x) = a_0 + a_1 x + a_2 x^2$

$g(x) = b_0 + b_1 x + b_2 x^2 + b_3 x^3$

if $\deg f < \deg g$, pad f by 0's when adding

$f(x)+g(x) = (a_0+b_0) + (a_1+b_1)x + (a_2+b_2)x^2 + (0+b_3)x^3$

useful convention:

$\deg(0) = -\infty$

$\deg(a) = 0$ $\quad a \neq 0$

$\deg f(x)$ – largest n such that $a_n \neq 0$

Exercise 1) $\deg(f(x)+g(x)) \leq \max(\deg(f(x)), \deg(g(x)))$

If $\deg f \neq \deg g$ then $\deg(f+g)$ is the bigger of the two degrees.
what if $\deg f = \deg g$?

2) $\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$

For nice rings, have equality

$R = \mathbb{Z}/4$ $\qquad (1+2x)(3+2x) = 3+2x+6x+4x^2 = 3 \equiv -1 \pmod 4$

$\deg \quad 1 \quad 1 \qquad\qquad 0$

Assoc. of mult. in $R[x]$ and use distributivity

$$(ax^n\, bx^m)\, c x^k = a x^n (b x^m\, c x^k)$$

$$\| \qquad\qquad \|$$

$$abc\, x^{n+m+k}$$

$R \subset R[x]$ is a subring

$R \subset S$ ring

a subring: an abelian subgroup, contains 1 & closed under multiplication

$R^\times = \{a \in R \mid \exists b \ ab = ba = 1\}$ subgroup of invertible elements

$\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$

$M_n(\mathbb{R})^\times = GL_n(\mathbb{R})$ or $GL(n, \mathbb{R})$

$z \neq 0 \to z^{-1}$

$z = a + bi \quad z^{-1} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i$

Def A commutative ring R is called a **field** if $R^\times = R \setminus \{0\}$

That is, if every nonzero element of R is invertible ($R^\times$ is the largest possible).

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

(Soon we'll see that linear algebra can be done over any field).

$\mathbb{Z}$ is not a field

$\mathbb{Z}/n$ is sometimes a field

$n=7$ $\mathbb{Z}/7$ residues $0, 1, 2, 3, 4, 5, 6$

$2^{-1} = 4 \pmod 7$

$3^{-1} = 5 \pmod 7$

$2 \cdot 4 = 8 \equiv 1 \pmod 7$

$3 \cdot 5 = 15 \equiv 1 \pmod 7$

$6 \equiv -1 \pmod 7$

$(-1)^2 = 1$

invertible $\{1, 2, 3, 4, 5, 6\}$

$(\mathbb{Z}/7)^\times$

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

(will prove soon) $\mathbb{Z}/2, \mathbb{Z}/3, \mathbb{Z}/5, \mathbb{Z}/7, \mathbb{Z}/11$ fields

F common notation for a field

Let R, S be rings

Def A ring homomorphism $\alpha: R \to S$ is a map of sets such that

(1) $\alpha(a+b) = \alpha(a) + \alpha(b) \quad \forall a, b \in R$

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

(3) $\alpha(1) = 1$ α takes identity in R to identity in S.

Sometimes (3) is omitted. We keep it.

"Weak homomorphism": omit (3).

(nonunital homomorphism).

Properties: (1) says that α is additive $\Rightarrow$

$\alpha(0) = 0$, $\alpha(-a) = -\alpha(a)$.

(2) if a is invertible in R, $\alpha(a)$ is invertible in S.

$\Rightarrow \alpha$ induces a homomorphism of groups of invertible elements $R^* \to S^*$

$\mathbb{Z} \xrightarrow{\alpha} \mathbb{Q}$ $\quad \mathbb{Z}^* = \{\pm 1\}$ $\quad \{\pm 1\} \to \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$

(3) for any ring R $\exists$ a unique homomorphism $\mathbb{Z} \to R$

$1 \longmapsto 1$

$n \longmapsto n$

(4) Composition of homomorphisms $R_1 \xrightarrow{\alpha} R_2 \xrightarrow{\beta} R_3$ is a homomorphism $R_1 \xrightarrow{\beta\alpha} R_3$

Examples a) Inclusions of rings $R \subset S$ $\quad R \xhookrightarrow{\alpha} S$ $\quad \alpha(1) = 1$

b) $R \longrightarrow \{0\}$ zero ring 0.

c) $\mathbb{Z} \xrightarrow{\alpha} \mathbb{Z}/n$ $\quad a \longmapsto a + n\mathbb{Z}$ residue mod n / coset

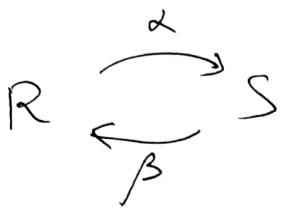
$\alpha(a+b) = a+b+n\mathbb{Z} = (a+n\mathbb{Z}) + (b+n\mathbb{Z})$ $\quad$ "$\bar{a}$"

$\alpha(ab) = ab+n\mathbb{Z} = (a+n\mathbb{Z})(b+n\mathbb{Z})$ matches definition of t.o. of cosets

$\alpha(1) = 1 \bmod(n)$ $\quad \alpha$ is a surjective homomorphism

Def A bijective homomorphism of rings $\alpha: R \to S$ is called an isomorphism of rings.

Equivalently, $\exists$ a homomorphism $\beta: S \to R$ such that $\beta\alpha = id_R$, $\alpha\beta = id_S$ (*)



$id_R: R \to R$ identity homomorphism

$id_R(a) = a \quad \forall a \in R$

id_R is an isomorphism

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

$\mathbb{C} \xrightarrow{\alpha} \mathbb{C}$ $\alpha(z) = \bar{z}$ complex conjugation is an isomorphism (automorphism of $\mathbb{C}$)

Exercise $\mathbb{Q}[\sqrt{2}] \xrightarrow{\alpha} \mathbb{Q}[\sqrt{2}]$ $\alpha(\sqrt{2}) = -\sqrt{2}$ $\alpha(a+b\sqrt{2}) = a-b\sqrt{2}$ an isomorphism (automorphism)

General principle / definition: (1) An isomorphism of objects is a bijection that respects all the structure.

(2) better: $\alpha: X \to Y$ is an isomorphism if $\exists \beta: Y \to X$ such that (*) holds

works for sets, vector spaces, groups, rings, etc..

isomorphism of sets (have the same cardinality)

isomorphism of vector spaces (have the same dimension)

isomorphism of groups, ..

Automorphisms of an object X constitute a group $Aut(X)$

Direct product of rings R_1, R_2 rings

$R_1 \times R_2$ Cartesian product of sets

$R_1 \times R_2 = \{ (a,b) \mid a \in R_1, b \in R_2 \}$

addition, multiplication term-wise

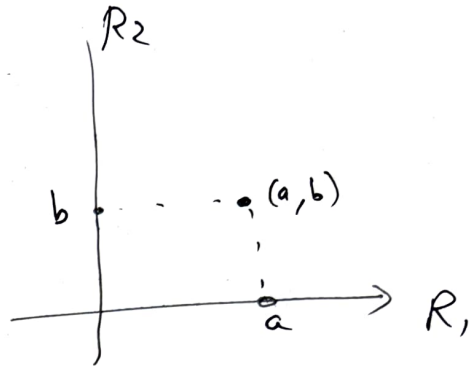
$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$

$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1, b_2)$

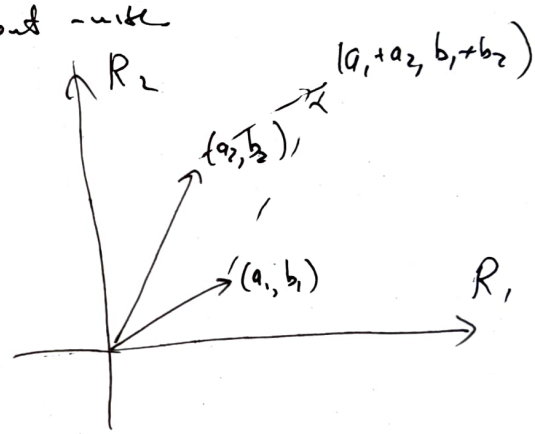
$(1,1)$ is identity

$(0,0)$ is zero

conceptually:



addition, multiplication component-wise



Exercise 1) $R_1 \times R_2$ is a ring

2) $R_1 \times R_2$ is commutative iff both R_1, R_2 are commutative

3) $R_1 \times R_2 \xrightarrow{\alpha} R_1$

$(a,b) \longmapsto a$

$\alpha((a,b)) = a$ "forget b" homomorphism

α is a homomorphism

$R_1 \times R_2 \xrightarrow{\beta} R_2$

$(a,b) \longmapsto b$ a homomorphism

"forget a" homomorphism

but $R_1 \longrightarrow R_1 \times R_2$

$a \longmapsto (a,0)$ is <u>not</u> a homomorphism. why?

Elements $(1,0)$, $(0,1)$ are special

$(1,0)^2 = (1,0)(1,0) = (1,0)$ itself $\quad (0,1)^2 = (0,1)$

$(1,1) = (1,0) + (0,1)$

---

e in R is called an <u>idempotent</u> if $e^2 = e$. $0, 1$ are idempotents

e in R is called an <u>idempotent</u> if $e^2 = e$.

0, 1 are idempotents. - Sometimes, a ring may have additional idempotents.

(a) In direct product $R_1 \times R_2$ $(1,0)$, $(0,1)$ are idempotents.

<u>Exercise</u> e is an idempotent $\longrightarrow$ $1-e$ is an idempotent.

Note that e and $(1-e)$ annihilate each other

$e(1-e) = e - e^2 = e - e = 0$

$(1-e)e = e - e^2 = 0$

In a comm. ring, only need to check on one side.

<u>complementary idempotents</u>

(b) In $\mathbb{Z}/6$ have usual idempotents 0, 1. Also

$3^2 = 9 \equiv 3 \pmod 6$ $\quad 4^2 = 16 \equiv 4 \pmod 6$.

$3 + 4 = 1$ complementary idempotents

(Secretly, that's due to $\mathbb{Z}/6 \cong \mathbb{Z}/2 \times \mathbb{Z}/3$ as rings).

(c) $M_n(\mathbb{R})$ projection operators P : $P^2 = P$

are idempotents