Rings $(R, +, \cdot)$

(1) $(R,+)$ abelian group, 0, $(-a)+a=0$
(2) $\cdot$ is associative, has identity 1 $\quad 1\cdot a = a \cdot 1 = a$ (unital rings)
(3) distributivity $(a+b)c = ac+bc \quad a(b+c) = ab+ac$

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, M_n(R), \mathbb{Z}[\frac{1}{n}], \mathbb{Z}/n$

$M_n(R)$: matrices; R: ring; $\mathbb{Z}/n$: residues mod n

Commutative rings: $ab = ba \quad \forall a,b \in R$ $\qquad$ $M_n(R)$ not commutative

Ring of polynomials $R[x]$

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

x - formal variable

a_0 constants
$a_0 + a_1 x$ linear
$a_0 + a_1 x + a_2 x^2$ quadratic
$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots$

$f(x) \in R[x]$
polynomial with coefficients in R

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

$a_0 + a_1 x + \ldots + a_n x^n$ $\quad$ degree n if $a_n \neq 0$

How to turn $R[x]$ into a ring? Need addition, multiplication of polynomials

addition should be term-wise

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

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

convenient to pad $f(x), g(x)$ by zeros for uniform definition

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

In this example
$\deg f = 2$, $\deg g = 3$
$\deg(f+g) = 3$.

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

$f(x) = a_0 + a_1 x + a_2 x^2 \rightsquigarrow f = (a_0, a_1, a_2, 0, 0, 0, \dots)$

append infinity-many zeros

$g(x) = b_0 + b_1 x + b_2 x^2 + b_3 x^3 \rightsquigarrow g = (b_0, b_1, b_2, b_3, 0, 0 \dots)$

$f(x) = a_0 + a_1 x + \dots + a_n x^n \rightarrow f = (a_0, a_1, \dots, a_n, 0, 0, \dots)$ last non-zero element

$g = (b_0, b_1, \dots \quad b_m, 0, 0 \dots)$ fin. many nonzero elements

$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2 \dots \dots, 0, 0 \dots)$

eventually all zeros

$f(x) = \sum_{i=0}^{n} a_i x^i \quad , g(x) = \sum_{j=0}^{m} b_j x^j$

$f(x) + g(x) = \sum_{i=0}^{\max(n,m)} (a_i + b_i) x^i$ append zeros to either a's or b's.

<u>Exercise</u> Addition turns $R[x]$ into an abelian group.

$f(x) = 0$ additive identity. $0 + g(x) = g(x)$. term-wise addition

<u>How to multiply?</u> Should have $x^n \cdot x^m = x^{n+m}$.

Then extend using distributive laws

$(a_0 + a_3 x^3) x^2 = a_0 x^2 + a_3 x^5$ example

$(a_0 + a_1 x + \dots + a_n x^n)(b_0 + b_1 x + \dots + b_m x^m) =$

$a_0 b_0 + a_0 b_1 x + \dots a_0 b_m x^m + a_1 b_0 x + \dots + a_n b_m x^{n+m}$

$a_n x^n$ - a monomials.

$$\Big(\underbrace{\sum_{i=0}^{n} a_i x^i}_{f(x)}\Big)\Big(\underbrace{\sum_{j=0}^{m} b_j x^j}_{g(x)}\Big) = \sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j x^{i+j} =$$

set $k = i+j$

it ranges from 0 to $n+m$

k, i fixed $\rightarrow j = k-i$

$$= \sum_{k=0}^{n+m}\Big(\sum_{i=0}^{k} a_i b_{k-i}\Big)x^k =$$

$$= \sum_{k=0}^{n+m}\Big(\sum_{i+j=k} a_i b_j\Big)x^k$$

Exercise: write this down for $n=2$, $m=3$ and think through the form of coefficients of x^k and what these sums look like

$k=4$: $a_0b_4 + a_1b_3 + a_2b_2 + a_3b_1 + a_4b_0$

$k+1$ terms (5 terms)

why is multiplication associative? $(fg)h \overset{?}{=} f(gh)$

$f(x) = \sum_i a_i x^i \qquad g(x) = \sum b_j x^j \qquad h(x) = \sum c_k x^k$

$$(fg)h = \sum_{\ell}\Big(\sum_{i+j+k=\ell}(a_ib_j)c_k\Big)x^{\ell}$$

$a_i x^i \cdot b_j x^j \cdot c_k x^k \rightsquigarrow a_i b_j c_k\, x^{i+j+k}$

$$f(gh) = \sum_{\ell}\Big(\sum_{i+j+k=\ell} a_i(b_jc_k)\Big)x^{\ell}$$

$$a_i x^i\, b_j x^j\, c_k x^k \xrightarrow{(ab)c} (a_ib_j)x^{i+j}\, c_k x^k \longrightarrow (a_ib_jc_k)\,x^{i+j+k}$$

$$\|$$

$$a_i x^i\, b_j x^j\, c_k x^k \xrightarrow{a(bc)} a_i x^i (b_jc_k)x^{j+k} \longrightarrow (a_ib_jc_k)\,x^{i+j+k}$$

$(a_ib_j)c_k = a_i(b_jc_k)$

true for monomials, then distributivity

Exercise 1) R is a subring of $R[x]$, $R \subset R[x]$, of constant polynomials.

2) $R[x]$ is commutative iff (if and only if) R is.

(anyway, we'll study only commutative rings for most of this course)

Noncommutative rings have even higher complexity. You've spent an entire semester course (linear algebra) studying elements of matrix rings $M_n(\mathbb{R})$, $M_n(\mathbb{C})$ and some variations ($n \times m$ matrices, linear maps $V \to W$ between different vector spaces) + elements there + applications

Group of invertible elements of a ring

$$R^* = \{a \in R : \exists b,\ ab = ba = 1\} \qquad b = a^{-1}$$

Prop R^* is a group under multiplication

1) Contains 1, $1^{-1} = 1$ $\quad 1 \cdot 1 = 1$.

2) if $a_1, a_2 \in R^* \Rightarrow \exists b_1, b_2$ $\quad a_1 b_1 = b_1 a_1 = 1$ $\quad a_2 b_2 = b_2 a_2 = 1$

$a_1 a_2 \rightsquigarrow b_2 b_1$ $\qquad a_1 a_2 b_2 b_1 = a_1 b_1 = 1$

$\qquad b_2 b_1 a_1 a_2 = b_2 a_2 = 1$

3) if $a \in R^*$ take b, declare it a^{-1}.

why is b unique? Use result that the inverse in a group is unique or prove

R^* is not all of R, $0 \notin R^*$ (unless we take the zero ring $R = \{0\}$)

Examples 1) $\mathbb{Z}^* = \{\pm 1\}$

2) $\mathbb{Q}^*$ - all nonzero rationals, $\left(\frac{n}{m}\right)^{-1} = \frac{m}{n}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$

3) $\mathbb{R}^*$ - all nonzero reals, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$

4) $\mathbb{C}^*$ - all nonzero complex numbers, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$

5) $M_n(\mathbb{R})^* = GL_n(\mathbb{R})$ or $GL(n, \mathbb{R})$ - invertible $n \times n$ matrices

Examples 2), 3), 4) above are special (all nonzero elements are invertible)

Def A commutative ring R is called a field if $R^* = R \setminus \{0\}$,
That is, if every nonzero element of R is invertible

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

(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

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

Invertible $\{1, 2, 3, 4\}$

$(\mathbb{Z}/5)^* = \{1, 2, 3, 4\}$

$2 \cdot 3 = 6 \equiv 1 \pmod 5$

$4 = -1 \pmod 5$

$(-1)(-1) = 1$

$2^{-1} = 3 \pmod 5$

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

(try to prove, will discuss soon)

$\mathbb{Z}/2, \mathbb{Z}/3, \mathbb{Z}/5, \mathbb{Z}/7, \mathbb{Z}/11 \ldots$ fields.

common notation for a field: F

Let R, S be rings

<u>Def</u> A ring homomorphism $\alpha : R \to S$ is a map (or function) from set R to set S 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) $\alpha(1) = 1$ $\quad$ α takes identity in R to identity in S.

In some books (3) is omitted.
we keep it.

<u>Exercise</u> 1) With (1), (2), (3) above, α is additive (a homomorphism of abelian groups $(R,+) \to (S,+)$).
1) $\Rightarrow \alpha(0) = 0$

2) if a is invertible in R, $\alpha(a)$ is invertible in S.
$\Rightarrow$ α induces a homomorphism of groups $R^{*} \to S^{*}$ of inv. elements.

3) Composition of homomorphisms $R_1 \xrightarrow{\alpha} R_2 \xrightarrow{\beta} R_3$
$\beta\alpha : R_1 \to R_3$ is a homomorphism.

<u>Examples</u> a) Inclusions of rings $R \subset S$ $\quad R \xhookrightarrow{\alpha} S$ $\quad \alpha(1) = 1$..

b) $R \to \{0\}$ ← zero ring.

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

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

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

$\alpha(1) = 1 \mod (n)$

α is a surjective homomorphism. <u>Not</u> an isomorphism

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

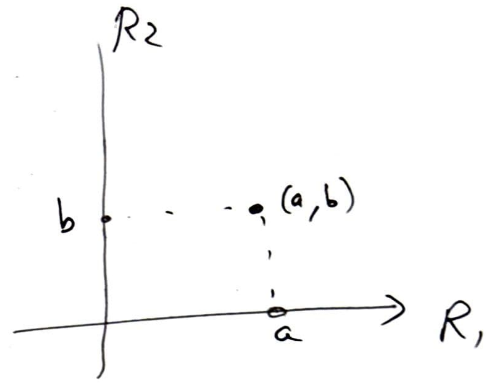
$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$

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

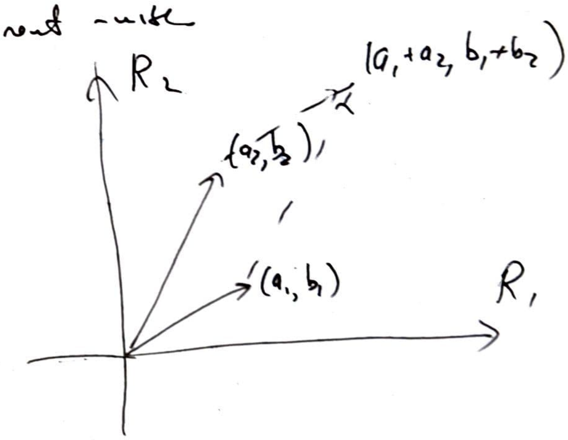
$(1, 1)$ is identity

$(0, 0)$ 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 __not__ a homomorphism. why?

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

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

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

e in R is called an idempotent 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 $\rightarrow$ $1-e$ 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 commu. ring, only need to check on one side.

<u>complementary idempotents</u>

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

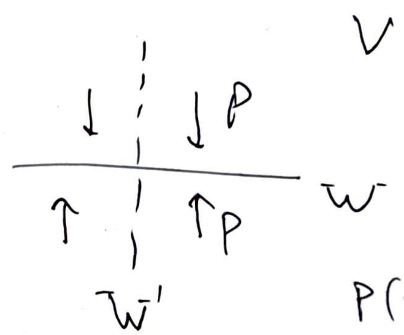
$3^2 = 9 \equiv 3 \pmod 6$ $\quad$ $4^2 = 16 \equiv 4 \pmod 6$.

$3 + 4 = 1$ $\quad$ complementary idempotents

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

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

are idempotents



$P(w') = 0$

$P(w) = w$

$\forall w \in W$