def <u>ring</u> $(R, +, *)$
- $\rightarrow (R, +)$ is abelian group
- $\rightarrow$ $*$ is associative
- $\rightarrow$ distributes over $+$

$$a(b+c) = ab + ac$$
$$(a+b)c = ac + bc$$

def <u>commutative ring</u>
... $*$ is commutative

def <u>ring with unity</u> 1, multiplicative identity

def <u>field</u> ... $(R \setminus \{0\}, *)$ also an abelian group

---

examples $\mathbb{Z}$, $\mathbb{Z}[i] \subset \mathbb{C}$ are rings

$\mathbb{R}[x_1, \ldots, x_n]$ polynomials in n vars, coefs in $\mathbb{R}$

"endomorphisms" Let V be a vectorspace over field F

$$R = \mathrm{Hom}(V, V) = \{ f : V \to V \mid f \text{ is linear map} \}$$

$+$ $\quad (f+g)(x) := f(x) + g(x)$

$*$ $\quad (f*g)(x) := f(g(x))$ composition

linearity $\Rightarrow$ distributive law ⊛

⊛
$$\begin{aligned}(f*(g+h))(x) &:= f((g+h)(x)) \\ &= f(g(x)+h(x)) \\ (f*g + f*h)(x) &:= f(g(x)) + f(h(x))\end{aligned}$$

$$\begin{aligned}((f+g)*h)(x) &:= (f+g)(h(x)) \\ (f*h + g*h)(x) &:= f(h(x)) + g(h(x))\end{aligned}$$

matrix rings $\quad M_{n,n}(F) =$ matrices $n \times n$ over F

$+, *$ using matrix ops

same thing for finite dim V / F

generalize: free module over R

(module: sometimes partially modded out, doesn't happen for fields)

Group rings $\quad$ Let G be multiplicative group (finite or infinite)

R ~~comm~~ ring with unity

$$R[G] = \{ \text{finite sums } r_1 g_1 + \dots + r_e g_e \}$$

$$r_i \in R \quad g_i \in G$$

add, multiply as expressions using $*$ in R, G where r_i commute with g_j

compare

$$R[x_1, \dots, x_n] = \{ \text{finite sums } r_1 x^{a_1} + \dots + r_e x^{a_e} \}$$

$x = (x_1, \dots, x_n)$

$a_i = (a_{i1}, \dots, a_{in}) \in \mathbb{N}^n \quad \mathbb{N} = \{0, 1, \dots\}$

$x^{a_i} = x_1^{a_{i1}} \cdots x_n^{a_{in}}$ multinomial notation

$x^{a_i} * x^{a_j} = x^{(a_i + a_j)}$

How are these related?

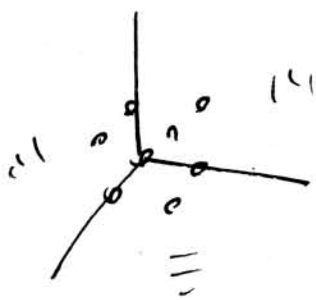
Let S be the semigroup $\{ x^{a_i} \mid a_i \in \mathbb{N}^n \}$

$(S, *)$ is $(\mathbb{N}^n, +)$ written multiplicatively

$R[S]$ is <u>same</u> construction as $R[G]$

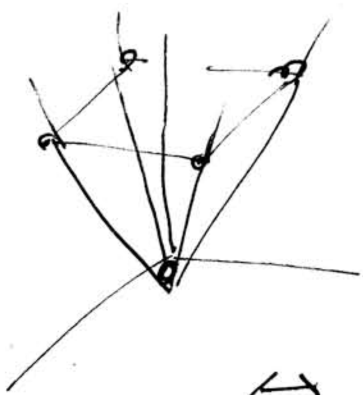
"toric algebra"

$R[S]$ is "polynomials" on lattice points in first orthant



(source of exponents)

can instead take any polyhedral cone



integer programming:

finding ~~solutions~~ integer solutions to linear inequalities

$\Leftrightarrow$ lattice points in polytopes

def
product R_1, R_2 rings

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

$$(a,b) + (c,d) = (a+c, b+d)$$

ops termwise $$(a,b) * (c,d) = (a*c, b*d)$$

dumb def? Linear algebra didn't work this way.

$(0,0)$ is identity for $+$

$(1,1)$ is identity for $*$

problem: $(1,0) * (0,1) = (0,0)$

$\boxed{0 \text{ factors unexpectedly}}$

Def integral domain is comm ring w/ unity ~~&~~ $1 \neq 0$

so $a \neq 0,\ b \neq 0 \Rightarrow ab \neq 0$

---

example: $(\mathbb{Z}/6\mathbb{Z}, +, *)$ $2 \cdot 3 = 0$ (6 is not prime)

$\mathbb{Z}/6\mathbb{Z}$ is same ring as $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

How do we say this? $f: R_1 \to R_2$

morphism
homomorphism
isomorphism

preserves ops of algebra
here, $+, *$

5.

$$f: \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

$$m \longmapsto (m \bmod 2,\ m \bmod 3)$$

always the case, if $f_1: R \to R_1$, $f_2: R \to R_2$ are homomorphisms

then $f_1 \times f_2: R \to R_1 \times R_2$ is homomorphism

(in product, factors don't interact at all)

so f is homomorphism

Kernel is $\{0\}$ ✓ injective,

6 elements each

$\Rightarrow$ ~~surjective~~ 1:1

---

if $f: R_1 \to R_2$ is 1:1 homomorphism then so is f^{-1}

0	0	0	0
1	1	1	7=1
2	0	2	8=2
3	1	0	3
4	0	1	4
5	1	2	11=5

$$f^{-1}: \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$$

(Chinese remainder theorem)

$$(m,n) \longrightarrow 3m + 4n \bmod 6$$

prime vs ~~ring~~ integral domain

generalize from $\mathbb{Z}$ to comm ring with unity

$$\left(\begin{array}{l} p \text{ prime} \Leftrightarrow \text{only factors are } 1, p \\ ab = p \Rightarrow a = \pm p \text{ or } b = \pm p \end{array} \right)$$

prepare for multiple generators by rewording using sets

I = all multiples of p, $I \subset \mathbb{Z}$

$$ab \in I \Rightarrow a \in I \text{ or } b \in I$$

now, I need not be multiples of single elem

can be ideal: closed under $+$
absorbing under $*$

$$a \in I, b \in I \Rightarrow a+b \in I$$
$$a \in \cancel{R}, b \in \underset{I}{\cancel{R}} \Rightarrow ab, \cancel{ba} \in I$$

say I is prime: $ab \in I \Rightarrow a \in I$ or $b \in I$

now take $I = \{0\} \subset R$

$$\boxed{\underset{\{0\}}{\underset{\parallel}{I}} \text{ is prime} \Leftrightarrow R \text{ is an integral domain}}$$

in general, we <u>quotient</u> by ideals (two-sided, if $ab \neq ba$)
what should our defn be?

<u>First isomorphism theorem</u>

Let $\phi : G \to G'$ hom w/ kernel K
$\gamma_K : G \to G/K$ canonical ~~iso~~ hom

exists unique $\mu : G/K \to \phi[G]$ so

$$\begin{tikzcd} G \arrow[rr, "\phi"] \arrow[dr, "\gamma_K"'] & & \phi[G] \subseteq G' \\ & G/K \arrow[ur, "\mu \text{ iso}"'] & \end{tikzcd}$$

$(*)$

what's the point: quotients appear as images of maps

we mod out by kernels of maps

pseudo-sphere
Cardano
1860's