**def** ring \((R, +, \cdot)\) 
- \((R, +)\) is abelian group
- \(\cdot\) is associative
- \(\cdot\) distributes over +

\[ a(b+c) = ab + ac \]
\[ (a+b)c = ac + bc \]

**def** commutative ring
- \(\cdot\) is commutative

**def** ring with unity \(1\), multiplicative identity

**def** field \((R, \cdot, +)\) 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.,
\(\text{coeffs in } \mathbb{R}\)

"endomorphisms" Let \(V\) be a vectorspace over field \(F\)
\[ R = \text{Hom}(V, V) = \{ f: V \to V \mid f \text{ is linear map} \} \]

+ \((f+g)(x) := f(x) + g(x)\) 
* \((f \circ g)(x) := f(g(x))\) composition

Linearity \(\Rightarrow\) distributive law \(\oplus\)
\[ (f \circ (g + h))(x) = f((g + h)(x)) \]
\[ = f(g(x) + h(x)) \]
\[ (f \circ g + f \circ h)(x) = f(g(x)) + f(h(x)) \]

\[ ((f + g) \circ h)(x) = (f + g)(h(x)) \]
\[ (f \circ h + g \circ h)(x) = F(h(x)) + g(h(x)) \]
matrix rings $M_{n \times n}(F) = \text{matrices } n \times n \text{ over } F$

$\text{plus, times using matrix ops}$

same thing for finite dim $V \nrightarrow F$

generalize: free module over $R$

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

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

$R$ ring with unity

$R[G] = \left\{ \text{finite sums } \sum_{i} r_i g_i \mid r_i \in R, g_i \in G \right\}$

add, multiply as expressions using $\ast$ in $R, G$

where $r_i$ commute with $g_j$

compare

$R[x_1, \ldots, x_n] = \left\{ \text{finite sums } \sum_{i} r_i x^{a_i} \mid r_i \in R, a_i \in \mathbb{N}^n \right\}$

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

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

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

$x^{a_i} \ast x^{a_j} = x^{(a_i + a_j)}$
How are these related?

Let $S$ be the semigroup $\prod x_a \mid a_i \in \mathbb{N}^3$

$(S, \cdot)$ is $(\mathbb{N}_0^3)$ written multiplicatively

$R[S]$ is the same construction as $R[G]$

"torn 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

$\iff$ lattice points in polytopes
Product \( R_1, R_2 \) rings

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

ops termwise

\((a, b) + (c, d) = (a + c, b + d)\)
\((a, b) \ast (c, d) = (a \ast c, b \ast d)\)

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

\((0, 0)\) is identity for +
\((1, 1)\) is identity for *

Problem: \((1, 0) \ast (0, 1) = (0, 0)\)

0 factors unexpectedly

Def integral domain is comm. ring w/ unity & \( l \neq 0 \)
so \( a \neq 0, b \neq 0 \) \( \Rightarrow ab \neq 0 \)

Example: \((\mathbb{Z}/6\mathbb{Z}, +, \cdot)\) \( 2 \cdot 3 = 0 \) (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?

- Morphism
- Homomorphism
- Isomorphism

F: \( R_1 \rightarrow R_2 \)

Preserves ops of algebra here, +, \( \ast \)
\[ f: \mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \]
\[ m \mapsto (m \mod 2, m \mod 3) \]

always the case, if \( f_1: R \rightarrow R_1 \) are homomorphisms \( f_2: R \rightarrow R_2 \), then \( f_1 \times f_2: R \rightarrow R_1 \times R_2 \) is homomorphism (in product, factors don't interact at all)

so \( f \) is homomorphism

Kernel is \( \{0\} \times \{0\} \) \& injective, 6 elements each \Rightarrow bijection 1:1

\[
\begin{array}{c|cccc}
0 & 0 & 0 & 0 & 0 \\
1 & 1 & 2 & 1 & 0 \\
2 & 0 & 1 & 2 & 0 \\
3 & 1 & 0 & 1 & 2 \\
4 & 2 & 1 & 0 & 1 \\
5 & 0 & 2 & 1 & 0 \\
\end{array}
\]

\[
f^{-1}: \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z}
\]
\[(m,n) \rightarrow 3m + 4n \mod 6\]

(Chinese remainder theorem)
prime vs integral domain

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

\[
\begin{align*}
\text{prime } &\Rightarrow \text{ only factors are } 1, p \\
abla p &\Rightarrow a = \pm p \text{ or } b = \pm p
\end{align*}
\]

prepare for multiple generators by rewording using sets

\[I = \text{all multiples of } p, \ I \subset \mathbb{Z}\]

\[ab \in I \Rightarrow a \in I \text{ or } b \in I\]

now, I need not be multiples of single elem

can be ideal: closed under + absorbing under *

\[a \in I, b \in I \Rightarrow a+b \in I\]

\[a \in \mathbb{R}, b \in I \Rightarrow ab, b \in I\]

say I is prime: \(ab \in I \Rightarrow a \in I \text{ or } b \in I\)

now take \[I = \mathbb{Z}/\mathbb{Z} \subset R\]

I is prime \(\Leftrightarrow R \text{ is an integral domain}\)
in general, we quotient by ideals (two-sided, if $a \neq b$)
what should our def be?

First isomorphism theorem

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

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

$G \xrightarrow{\phi} \phi[G] \subseteq G'$

$\gamma_K \xrightarrow{\mu \ iso} G/K$

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

we mod out by kernels of maps

pseudo-sphere
Cardano
1860's