Noncommutative algebra

Lecturer: Daniel Smertnig

October 2, 2025

1. Basics and examples

1.1. Examples of noncommutative rings

Ring: $(R,+,\cdot,1,0)$ s.t. $(R,+,0)$ is an abelian group
$(R,\cdot,1)$ is a monoid
$a(b+c)=ab+ac$, $(b+c)a=ba+ca$

This course: always unital (with 1)
typically noncommutative (=nc)

$a\in R$ is right [left] invertible if $\exists b\in R.\ ab=1$ $[ba=1]$

right [left] zerodivisor if $\exists b\in R\setminus\{0\}.\ ba=0$ $[ab=0]$

nilpotent if $\exists n\in\mathbb{N}.\ a^n=0$

invertible/unit if right AND left invertible

$R^\times:=\{a\in R \mid a \text{ invertible}\}$ group of invertible elements/unit group

$a\in R$ is a zerodivisor if left OR right zerodivisor

R is a domain $\Leftrightarrow$ 0 is the only zerodivisor
$\Leftrightarrow R\neq \underline{0}=\{0\}$ and $\forall a,b\in R.\ ab=0\Rightarrow a=0 \vee b=0$

R is reduced $\Leftrightarrow$ R has no nonzero nilpotents
$\Leftrightarrow \forall a\in R.\ a^2=0\Rightarrow a=0$

Note: $\underline{0}$ is reduced

Examples:

1) Commutative rings ($\mathbb{Z}$, Fields, $K[x_1,\dots,x_n]$, ...)

2) $M_n(R)$ ... $n\times n$ matrices; nc if $n \geq 2$ or R nc

Subring of upper triangular matrices: $T_n(R) = \begin{bmatrix} R & R & \cdots & R \\ 0 & R & \cdots & R \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & R \end{bmatrix}$

$R = K$ Field : $A \cdot \underbrace{\mathrm{adj}(A)} = \det(A)\cdot I_n \in M_n(K)$

So: $A \in M_n(K)^\times \iff \det(A) \neq 0$ — adjugate of A/ classical adjoint of A

A zerodivisor $\iff \det(A) = 0$

3) Hamilton quaternions $\mathbb{H} := \mathbb{R}1 + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$
with $i^2 = -1$, $j^2 = -1$, $ij = -ji = k$ extended $\mathbb{R}$-linearly

$\left(\Rightarrow \quad i \to j \to k \to i \qquad jk = i = -kj, \quad ki = j = -ik, \quad k^2 = -1 \right)$

For $\alpha = a + bi + cj + dk$ $(a,b,c,d \in \mathbb{R})$, let $\bar{\alpha} := a - bi - cj - dk$

$\Rightarrow \alpha\bar{\alpha} = \bar{\alpha}\alpha = \underbrace{a^2 + b^2 + c^2 + d^2}_{\geq 0} =: \mathrm{nr}(\alpha) \in \mathbb{R}_{\geq 0}$

reduced norm

If $\alpha \neq 0 \Rightarrow \mathrm{nr}(\alpha)^{-1}\bar{\alpha}\alpha = 1 \Rightarrow \alpha \in \mathbb{H}^\times$

$\mathbb{H}$ is a division ring (= skew field; slovene: obseg)

4) $R = \begin{bmatrix} \mathbb{Z} & \mathbb{Z}/2\mathbb{Z} \\ 0 & \mathbb{Z} \end{bmatrix}$ here $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ is a left zerodivisor, but not right zerodivisor

$$\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & \bar{1} \\ 0 & 0 \end{bmatrix} = 0,$$

$$\begin{bmatrix} x & \bar{y} \\ & z \end{bmatrix}\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2x & \bar{y} \\ & z \end{bmatrix} \neq 0 \text{ unles } x = z = 0, \bar{y} = \bar{0}.$$

Remark: This type of ring is often used to produce counter examples.

5) Free k-algebras "nc versions of polynomial rings"

k commutative ring, X set: $R = k\langle X\rangle$ is the k-vector space of all nc polynomials in X (= formal k-linear combinations of words in X), e.g.

$$3x + 7xyz - 5\underbrace{xy}_{\text{different}} + 3\underbrace{yx}_{\text{different}} + 2yzx \in \mathbb{Z}\langle x,y,z\rangle$$

Coefficients commute with indeterminates, but indeterminates do not commute with each other.
$\Rightarrow k\langle X\rangle$ is a ring, product: k-linearly extend concatenation of words

universal property

<u>UP:</u> If R' is a ring, $\varphi: k \to Z(R')$ is a ring hom. (i.e. R' is a k-algebra), and $f: X \to R'$ is a map (of sets), then there exists a unique ring hom. $\bar{f}: k\langle X\rangle \to R'$ s.t. $\bar{f}|_X = f$, $\bar{f}|_k = \varphi$.
[$\Leftrightarrow \bar{f}$ is the unique k-algebra hom. s.t. $\bar{f}|_X = f$]

$$\begin{tikzcd}
X \arrow[r] \arrow[dr, "f"'] & k\langle X\rangle \arrow[d, dashed, "\exists!\,\bar{f}"] \arrow[dl, phantom, "\circlearrowleft"] \\
 & R
\end{tikzcd}$$

(as k-algebras)

(Every k-algebra is a holomorphic image of a free k-algebra.)

$X = \{x\}$: $k\langle x\rangle = k[x]$ (polynomial ring)

$|X| \geq 2$: We get something totally diffent from $k[x_1,\dots,x_n]$!
<u>E.g.</u>: $k\langle x,y\rangle$ contains a subring isomorphic to $k\langle z_i \mid i\in\mathbb{N}_0\rangle$

$$\varphi: \underbrace{k\langle z_i \mid i\in\mathbb{N}_0\rangle \hookrightarrow k\langle x,y\rangle}_{\text{monomorphism}}, \quad z_i \longmapsto xy^i$$

e.g. $\varphi(z_2z_3z_1) = xy^2\,xy^3\,xy$

6) Algebras defined by generators and relations:

If R is a k-algebra (every ring is a $\mathbb{Z}$-algebra), $(g_i)_{i\in I}$ is a system of generators

$\exists$ hom. $\varphi : k\langle x_i \mid i\in I\rangle \twoheadrightarrow R$, $x_i \mapsto g_i$

φ surjective $\Rightarrow R \cong k\langle x_i \mid i\in I\rangle / \ker\varphi$

If $F=(f_j)_{j\in J}$ generates the ideal $\ker\varphi$, then R is "generated over k by $(x_i)_{i\in I}$ subject to relations F"

- $k\langle x,y \mid xy-yx\rangle = k\langle x,y\rangle / \langle xy-yx\rangle \cong k[x,y]$

  $\hookrightarrow xy-yx$ being in the kernel means $xy=yx$

- $\mathbb{R}\langle x,y \mid x^2+1,\ y^2+1,\ xy+yx\rangle \cong \mathbb{H}$ $(x\mapsto i,\ y\mapsto j)$

- $k\langle x,y \mid xy-yx-1\rangle =: A_1(k)$ is the 1^{st} Weyl algebra

7) k field, $\operatorname{char} k = 0$, $R = A_1(k)$ generated over k by $\bar{x},\bar{y}$ subject to $\bar{x}\bar{y}-\bar{y}\bar{x}=1$.

Interpretation as differential operators on $k[y]$:
(this has applications in physics - quantum mechanics)

$$\Phi_0 : \begin{cases} k\langle x,y\rangle \longrightarrow \operatorname{End}_k(k[y]) \\ y \longmapsto M, \quad M(f) = yf \\ x \longmapsto \frac{d}{dy}, \quad D(f) = \frac{d}{dy} f \quad \text{(formally)} \end{cases}$$

$$\forall f \in k[y]: \ DM(f) = \frac{d}{dy}(yf) = \underbrace{\frac{d}{dy}y}_{=1}\cdot f + y\frac{d}{df}f = (1+MD)f$$

$\Rightarrow DM - MD = 1$, so $xy-yx-1 \in \ker(\Phi_0)$

$\Rightarrow \exists$ ring hom. $\Phi : A_1(k) \longrightarrow \operatorname{End}_k(k[y])$, $\bar{y}\mapsto M$, $\bar{x} \mapsto D$

Exercise: Φ is injective, so $A_1(k) \cong$ k-subalgebra of $\mathrm{End}_k(k[y])$ generated by M, D.

8) R ring, G group or (monoid), (semi) group ring:

$$R[G] := \bigoplus_{g\in G} Rg \quad \text{elements: finite formal sums } \sum_{g\in G} r_g g,\ r_g \in R$$

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) := \sum_{k\in G}\left(\sum_{\substack{g,h\in G\\ k=gh}} a_g b_h\right)k, \qquad \left[(a_g g)(b_h h) = a_g b_h gh\right]$$

<u>Special cases</u>: R commutative,

- G free monoid generated by a set X
  $\Rightarrow R[G]$ is the free R-algebra generated by X
- $G \cong \left(\mathbb{N}_0^{(I)}\right)$, say freely generated by $\{x_i \mid i\in I\}$, so elements of G are of the form $x_{i_1}^{n_{i_1}} \cdots x_{i_k}^{n_{i_k}}$, $i_1,\dots,i_k \in I$ pairwise distinct
  $\Rightarrow R[G] \cong$ polynomial ring

<u>Universal property</u>: If $f: R \longrightarrow R'$ is a ring hom., $\sigma: G \longrightarrow (R', \cdot, 1)$ is a monoid hom. s.t. $f(r)\sigma(g) = \sigma(g) f(r)$ for all $r\in R$, $g\in G$, then there exists a unique ring hom. $\bar{f}: R[G] \longrightarrow R'$ s.t. $\bar{f}|_R = f$, $\bar{f}|_G = \sigma$.

9) Skew polinomial rings / Ore extensions, R ring
a) $\sigma: R \longrightarrow R$ endomorphism
$R[x;\sigma]$ elements: finite formal (left) R-linear combinations of x^i, $i \geq 0$

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

$$fg := \sum_{i,j=0}^{n} a_i \sigma^i(b_j) x^{i+j} \,, \qquad \boxed{\forall a \in R.\ xa = \sigma(a) x}$$

Note: polynomials with coefficients on the right can be rewritten as

$$\sum x^i a_i = \sum \sigma^i(a_i) x^i,$$

but the converse only works if σ is surjective.

If σ not injective: $\exists b \in R \setminus \{0\}$, $\sigma(b) = 0$

$\Rightarrow \underset{\neq 0}{x} \cdot \underset{\neq 0}{b} = \underset{= 0}{\sigma(b)} x = 0 \Rightarrow x$ is a left zerodivisor, not right zerodivisor

<u>Lemma</u>: R domain, σ injective $\Rightarrow R[x, \sigma]$ domain, since then $\deg(fg) = \deg(f) + \deg(g) \in \mathbb{N}_0 \cup \{-\infty\}$.

b) Let σ be a derivation on R (i.e. $\sigma(a+b) = \sigma(a) + \sigma(b)$ and $\sigma(ab) = \sigma(a)b + a\sigma(b)$, i.e., Leibniz rule)

$R[x; \sigma]$ again has elements $\sum_i a_i x^i$, multiplication induced by $\forall a \in R.\ xa = ax + \sigma(a)$

<u>E.g.</u>
$$\begin{aligned} x^2 a = x(ax + \sigma(a)) &= (xa)x + x\sigma(a) \\ &= ax^2 + \sigma(a)x + \sigma(a)x + \sigma^2(a) \\ &= ax^2 + 2\sigma(a)x + \sigma^2(x) \end{aligned}$$

<u>E.g.</u> $R = k[y]$, k ring, $\delta = \frac{d}{dy}$

In $k[y][x; \sigma]$: $xy = yx + \delta(y) = yx + 1$

$\overset{\text{easy}}{\Longrightarrow} k[y][x;\sigma] \cong A_1(k)$

In particular, elements of $A_1(k)$ have a (unique) representation $\sum_{i,j} a_{ij} \bar{y}^i \bar{x}^j$, i.e., $\{\bar{y}^i \bar{x}^j \mid i,j \geq 0\}$ is a k-basis of $A_1(k)$
(but also $\{\bar{x}^j \bar{y}^i \mid i,j \geq 0\}$ is, $A_1(k) \cong k[x][y; -\frac{d}{dx}]$

c) <u>Mixed case</u>: R ring, $\sigma: R \to R$ endomorphism, $\delta: R \to R$ a σ-derivation (i.e., $\delta(a+b) = \delta(a) + \delta(b)$, $\delta(ab) = \delta(a)b + \sigma(a)b)$
$R[x; \sigma, \delta]$ ... same construction with $\forall a \in R. \, xa = \sigma(a)x + \delta(a)$

Why do we define it this way?
Suppose we want to define some multiplication on formal sums $f = \sum a_i x^i$, $g = \sum b_j x^j$ s.t. $\deg(fg) \leq \max\{\deg f, \deg g\}$.
In particular $x \cdot a \overset{!}{=} \sigma(a)x + \delta(a)$ with maps $\sigma, \delta: R \to R$

$$\Rightarrow xab = x(ab) = \sigma(ab)x + \delta(ab)$$
$$= (xa)b = (\sigma(a)x + \delta(a))b = \sigma(a)(\sigma(b)x + \delta(b)) + \delta(a)b$$
$$= \underbrace{\sigma(a)\sigma(b)}_{\overset{!}{=}\,\sigma(ab)} x + \underbrace{\sigma(a)\delta(b) + \delta(a)b}_{\overset{!}{=}\,\delta(ab)}$$

$\Rightarrow \sigma$ must be an endomorphism, δ a σ-derivation
(For additivity look at $x(a+b) = xa + xb$)

10) <u>Formal power series</u>: R ring, x indeterminate, $R[[x]] = \{a_0 + a_1 x + a_2 x^2 + \cdots \mid a_i \in R\}$.
Then $f \in R[[x]]^\times \Leftrightarrow a_0 \in R^\times$

<u>Laurent series</u>: $R((x)) := \{\sum_{i=-n}^{\infty} a_i x^i \mid a_i \in R\}$

invertible $\Leftrightarrow$ lowest coeff. invertible
$\Rightarrow$ if R is a division ring, so is $R((x))$.

Twisted versions:
- $R[x;\sigma]$ with $\sigma \in \mathrm{End}(R)$: $xa = \sigma(a)x$
- $R[x;\sigma]$ with $\sigma \in \mathrm{Aut}(R)$: $xa = \sigma(a)x$
  (now $x^{-1}a = \sigma^{-1}(a)x^{-1}$
  If R is a division ring $\Rightarrow$ $R((x;\sigma))$ is a div. ring

1.2. Noetherian/Artinian Modules and Rings

Definition: R ring. A (right) R-module is an abelian group $(M,+,0)$ together with „$\cdot$" $: M \times R \to M$ s.t. $\forall m,n \in M.\ \forall a,b \in R.$
- $m \cdot 1 = m$
- $(m+n)a = ma + na$
- $m(a+b) = ma + mb$
- $m(ab) = (ma)b$

Homomorphisms: $f: M \to N$, $f(m+m') = f(m) + f(m')$,
$f(ma) = f(m)a$

Mod-R is the category of all right R-modules

Remark: Left modules analogously, the opposite ring R^{op} has $(R^{op},+,0) = (R,+,0)$, but $\forall a,b \in R.\ a \cdot_{op} b = ba$.
Category of left R-modules: R-Mod

We can't turn a right module into a left module by just taking $\cdot$ on the other side: associativity wont work.

If M_R is a right R-module, it is a left R^{op}-module via $\underset{R^{op}}{a} \cdot m = m \cdot \underset{R}{a}$.

$[(a \cdot_{op} b)m = (ba)m = m(ba) = (mb)a = a(mb) = a(bm)]$

$\Rightarrow$ Mod-$R \cong R^{op}$-Mod (as categories)

⚠ in general: $R \not\cong R^{op}$; $R = R^{op} \Leftrightarrow R$ commutative

$\boxed{\text{We will default to right modules.}}$

<u>Remark</u>: The right R-module structure σ can be equivalently described by a ring hom:

$$\tilde{\sigma}: R^{op} \longrightarrow \mathrm{End}_{\mathbb{Z}}(M)$$

[Given σ, define $\tilde{\sigma}(a)(m) := \underset{:= \sigma(m,a)}{ma}$.
E.g. $\tilde{\sigma}(ab)(m) = mab = (\tilde{\sigma}(a)(m))b = \tilde{\sigma}(b)(\tilde{\sigma}(a)(m))$
$= (\tilde{\sigma}(b) \circ \tilde{\sigma}(a))m \Rightarrow \tilde{\sigma}(b \circ_{op} a) = \tilde{\sigma}(b) \circ \tilde{\sigma}(a)$.
Conversely, given $\tilde{\sigma}$, define $m \cdot a := \tilde{\sigma}(a)m$.]

left R-module structure $\cong$ ring. hom. $R \to \mathrm{End}_{\mathbb{Z}}(M)$

<u>Definition</u>: Let R be a commutative ring. An **R-algebra** is a ring A s.t. A is also an R-module and $\forall r \in R. \forall a,b \in A.\ r(ab) = (ra)b = a(rb)$.

<u>Equivalent data</u>: a ring hom. $\varepsilon: R \longrightarrow Z(A)$ center

[If A is an R-algebra, $r \mapsto r \cdot 1_A$ is such a hom.
Conversly, $r \cdot a := \varepsilon(r)a$ defines an R-module structure on A.]
multiplication in A

<u>Example</u>: $\mathbb{C}$, $\mathbb{H}$ are $\mathbb{R}$-algebras (of dimension 2 resp. 4)

$\mathbb{C} \hookrightarrow \mathbb{H}$ as subring (e.g. $i \mapsto i$) but i is not central.
$\Rightarrow \mathbb{H}$ is not a $\mathbb{C}$ algebra!

- R is commutative $\Rightarrow R\langle X\rangle, R[G], M_n(R)$ R-algebras, $R[x; \sigma, \delta]$ in general is not

- $\underline{\mathrm{Rng}} = \mathbb{Z}\text{-}\underline{\mathrm{Alg}}$ as categories

<u>Example</u> [Endomorphism rings]:
Let $M_R \in \mathrm{Mod}\text{-}R$,

$$\mathrm{End}(M_R) := \{ f : M_R \longrightarrow M_R \mid f \text{ R-module hom} \}$$

is a ring with multiplication $\circ$

+ pointwise

$$\left[\begin{aligned} \text{e.g. } (f\circ(g+h))(m) &= f((g+h)(m)) \overset{}{=} f(g(m)+h(m)) \\ \text{f hom} \quad &= f(g(m)) + f(h(m)) \\ &= (f\circ g + g\circ h)(m). \end{aligned}\right]$$

<u>Special cases</u>:

⚠ r on left

-) $M = R_R$: $\quad L : R \longrightarrow \mathrm{End}(R_R), \quad r \mapsto L_r, L_r(x) = rx$
$\Rightarrow L$ is an isomorphism

$$\left[\begin{aligned} &\text{Consider } x=1: 0 = L_r \Rightarrow 0 = L_r(1) = r\cdot 1 = r \Rightarrow r=0 \Rightarrow L \text{ inj.} \\ &\text{If } \varphi \in \mathrm{End}(R_R), \text{ then } \forall x \in R.\ \varphi(x) = \varphi(1\cdot x) = \varphi(1)\cdot x \\ &\Rightarrow \varphi = L_r, \text{ so } L \text{ is surjective} \qquad R \cong \mathrm{End}(R_R) \end{aligned}\right]$$

-) ⚠ $\mathrm{End}({}_R R) \cong R^{op}$ ← one reason why one might prefer right modules over left

•) $R = K$ a field, $V_K \cong K^n$ finite dimensional vec. space (f.d.)
$\Rightarrow \mathrm{End}(V_K) \cong M_n(K)$

•) K field, R f.d. K-algebra
$\Rightarrow R \cong \mathrm{End}(R_R) \subseteq \mathrm{End}(R_K) \cong M_n(K)$ (as K-algebras)
So every f.d. K-algebra embeds into a matrix ring.

Exercise: Find an embedding $\mathbb{H} \hookrightarrow M_4(\mathbb{R})$.
$(\mathbb{H} \hookrightarrow M_2(\mathbb{C}))$

1.2. Noetherian/Artinian modules and rings

R ring

October 9, 2025

Lemma 1.1: For $M \in \text{Mod-}R$, TFAE:
(a) Every $N_R \leq M_R$ is finitely generated.
(b) M satisfies the ascending chain condition (ACC) on submodules. I.e. if $M_1 \subseteq M_2 \subseteq \cdots$ are submodules, there exists $n_0 \geq 1$ s.t. $\forall n \geq n_0$. $M_n = M_{n_0}$.
(c) Every nonempty set Ω consisting of submodules of M has a maximal element.

Proof: (a) $\Rightarrow$ (b): $M' := \bigcup_{i \geq 1} M_i$ is a submodule of M,
$\exists m_1, \dots, m_k \in M'$: $M' = \langle m_1, \dots, m_k \rangle_R$ $(m_1R + \dots + m_kR)$ by (a)
$\Rightarrow \exists n_0 \geq 0$: $m_1, \dots, m_k \in M_{n_0} \Rightarrow M' \subseteq M_{n_0} \subseteq M_n \subseteq M'$ $\forall n \geq n_0$
$\Rightarrow M_n = M_{n_0}$

(b) $\Rightarrow$ (c): Suppose not. Then $\forall N \in \Omega\ \exists N' \in \Omega.\ N \subsetneq N'$.
Choose $N_0 \in \Omega$ arbitrary. Recursively, $\forall i \geq 0$, choose $N_{i+1} \in \Omega$ s.t. $N_i \subsetneq N_{i+1}$ $\lightning$

(c) $\Rightarrow$ (a): Let $N \leq M$ and $\Omega := \{N' \leq N : N' \text{ is f.g}\}$.
Then $0 \in \Omega \Rightarrow \Omega \neq \emptyset$. So $\exists N_0 \in \Omega$ that is maximal.
If $N_0 \subsetneq N$, then $\exists x \in N \setminus N_0$, and $N_0 + xR \supsetneq N_0$ but
$N_0 + xR \in \Omega$ ↯
So N is f.g. $\blacksquare$

<u>Definition</u>: (1) $M \in \text{Mod-}R$ is noetherian if it satisfies the conditions in Lemma 1.1.
(2) R is right [left] noetherian if R_R [${}_RR$] is noetherian.
(3) R is noetherian if it is right and left noetherian.

<u>So</u>: R right noetherian $\Leftrightarrow$ every right ideal is f.g.

<u>Example</u>: $\mathbb{Z}$ is noetherian; R noetherian $\Rightarrow R[x_1, \dots, x_n]$ noetherian (Hilbert's basis theorem).

·) Free algebras in ≥ 2 variables are not noetherian
E.g. $F = k\langle x, y\rangle \Rightarrow \sum_{i \geq 0} x^i y$ is direct (exercise), hence not f.g.

·) $R = k(x)[y; \sigma]$ with $\sigma(f/g) = \frac{f(x^2)}{g(x^2)}$ is left noetherian, not right noetherian (Exercise: left PID by polynomial division; but $\sum_{i \geq 0} y^i xy R$ is direct).

Proposition 1.2: Let $\sigma \in \mathrm{Aut}(R)$, δ a derivation. If R is right [left] noetherian, then $R[x; \sigma, \delta]$ is right [left] noetherian.

Proof omitted, like commutative Hilbert's basis theorem (i.e. for left noetherian: given $L \leq_R R$ consider the left ideals $L_n \leq_R R$ consisting of leading coeffs. of polynomials of degree $\leq n$ in L + zero).

Lemma 1.3: For $M \in \text{Mod-}R$ TFAE:
(a): M satisfies the *descending chain condition* (DCC) on submodules i.e., for every chain $M_1 \supseteq M_2 \supseteq \cdots$ of submodules, there exists n_0 s.t. $\forall n \geq n_0.\ M_{n_0} = M_n$.
(b) Every non-empty set consisting of submodules of M has a minimal element.

Proof: (a) $\Rightarrow$ (b): Analogous to L 1.1. (b) $\Rightarrow$ (c).
(b) $\Rightarrow$ (a): Let $M_1 \supseteq M_2 \supseteq \cdots$ be a descending chain, $\Omega := \{M_i \mid i \geq 1\}$ has a minimal element M_{n_0}
$\Rightarrow \forall n \geq n_0.\ M_{n_0} = M_n$. $\square$

Definition: (1) $M \in \text{Mod-}R$ is *artinian* if it satisfies the conditions in Lemma 1.3
(2) R is *right [left] artinian* if R_R [${}_RR$] is artinian.
(3) R is *artinian* if it is right and left artinian.

Example: • Division rings are artinian, $\mathbb{Z}/n\mathbb{Z}$ is artinian, $\mathbb{Z}$ is not artinian ($\mathbb{Z} \supseteq 2\mathbb{Z} \supseteq 4\mathbb{Z} \supseteq 8\mathbb{Z} \supseteq \cdots$)

• $\begin{bmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{bmatrix}$ is right noetherian not left noetherian | $\begin{bmatrix} \mathbb{Q} & \mathbb{C} \\ & \mathbb{C} \end{bmatrix}$ is right artinian not left artinian

Exercise from Lam.

Lemma: (1) Let $M \in \text{Mod-}R$, $N \leq M$. Then
M is noetherian [artinian] $\Leftrightarrow$ N and M/N are noet. [artinian]
(2) Let $M_1, \ldots, M_n \in \text{Mod-}R$. Then $\bigoplus_{i=1}^{n} M_i$ is noetherian [artinian] $\Leftrightarrow \forall i$: M_i is noetherian [artinian].

(1) restated: if $0 \to N \to M \to \underset{\cong M/N}{L} \to 0$ is SES (short exact sequence) then M is noetherian [artinian] $\Leftrightarrow$ N, L are noetherian [artinian].

Proof: (1) For artinian; noetherian is dual.

($\Rightarrow$): If $N_1 \supseteq N_2 \supseteq \cdots$ is a chain of submodules of N, then this is also a chain of submodules of M, so it stabilizes.

Suppose $L_1 \supseteq L_2 \supseteq \cdots$ are submodules of M/N. Then $L_i = M_i+N/N$ with M_i submodules of M.,

$$M_1 + N \supseteq M_2 + N \supseteq \cdots$$

so $\exists i_0 \forall i > i_0.\ M_i = M_{i_0} \Rightarrow M_i + N = M_{i_0} + N \Rightarrow L_i = L_{i_0}$.

($\Leftarrow$): Let $M_1 \supseteq M_2 \supseteq \cdots$ be submodules of M.

Both chains $M_1 \cap N \supseteq M_2 \cap N \supseteq \cdots$ and $M_1+N/N \supseteq M_2+N/N \supseteq \cdots$ stabilize.

$\Rightarrow \exists i_0 \forall i \geq i_0.\ M_i \cap N = M_{i_0} \cap N$ and $M_i+N/N = M_{i_0}+N/N$
$\Rightarrow M_i + N = M_{i_0} + N$

Claim: $M_i = M_{i_0}$

$m' \in M_i, n \in N$

($\subseteq$): ✓ ($\supseteq$): Let $m \in M_{i_0} \Rightarrow m \in M_{i_0} + N = M_i + N$, so $m = m' + n$

$\underset{M_i \subseteq M_{i_0}}{\Rightarrow} n = m - m' \in M_{i_0}$ and also $n \in N \underset{M_{i_0} \cap N = M_i \cap N}{\Rightarrow} n \in M_i \Rightarrow m = \underset{\in M_i}{m'} + \underset{\in M_i}{n} \in M_i$

(2) By (1) and induction, because there is a S.E.S.

$$0 \longrightarrow \bigoplus_{i=1}^{n-1} M_i \longrightarrow \bigoplus_{i=1}^{n} M_i \longrightarrow M_n \longrightarrow 0$$

▨

2. Semisimple Modules and Rings (Wedderburn-Artin Theory)

2.1. Simple rings

$M \in \text{Mod-}R$ is cyclic if $\exists m \in M.\ M = mR$
$\Leftrightarrow \exists$ epimorphism $\varphi: R_R \twoheadrightarrow M_R$
$[(\Rightarrow): r \longmapsto mr,\quad (\Leftarrow): \varphi: R_R \twoheadrightarrow M_R,\quad M = \varphi(R) = \underset{\overset{\shortparallel}{m}}{\varphi(1)} R]$
$\Leftrightarrow M \cong R/I$ for a right ideal $I \leq R_R$
$[(\Rightarrow): R/\ker\varphi \cong M,\quad (\Leftarrow): R \to R/I,\ r \mapsto r+I$ is an epi$]$

<u>Definition</u>: $M \in \text{Mod-}R$ is simple/irreducible if $M \neq \underline{0}$ and M has no proper nonzero submodule.

<u>Example</u>: •) The simple $\mathbb{Z}$-modules are $\mathbb{Z}/p\mathbb{Z}$, p prime.
•) $R = k$ field: k_k is (up to isomorphism) the unique simple module
•) k field, $R = M_d(k)$, $V = k^{1\times d}$ (row vectors) with R, acting on the right. V is simple: for any $0 \neq v, w \in V.\ \exists A \in M_d(k)$ s.t. $vA = w$. So $vR = V \quad \forall v \in V \setminus \{0\}$.

<u>Proposition 2.1</u>: For $M \in \text{Mod-}R$, TFAE:
(a) M is simple.
(b) $M \neq \underline{0}$ and $\forall m \in M \setminus \{0\}.\ M = mR$. In particular: M is cyclic.
(c) $M \cong R/I$ for a maximal right ideal.

<u>Proof</u>: <u>(a) => (b)</u>: $M \neq 0$ by definition of a simple ring.
Let $0 \neq m \in M$, $\underline{0} \neq mR \underset{\text{submodule}}{\leq} M_R \Rightarrow mR = M$.

<u>(b) => (c)</u>: Let $0 \neq m \in M$. Let $\varphi: R_R \overset{(b)}{\twoheadrightarrow} M_R$, $r \mapsto mr$.
$I := \ker(I) =:$ ann(m) ... annihilator of m

$\Rightarrow M \cong R/I$ with I a right ideal. If I is not maximal, $\exists x \in R.\ I \subsetneq I + xR \subsetneq R$. Then $f(x) \neq 0$, and the cyclic module $f(x)R$ is a proper submodule of M. $\nrightarrow$
why?

!! $I+xR/I \leq R/I$ $\quad f(x)R = m\underbrace{xR}_{\subsetneq R}$!

$\underline{(c) \Rightarrow (a)}$: Since $R/I \cong M$, the submodules of M are in bijection with right ideals J for which $I \subseteq J \subseteq R$. Since $J = I$ or $J = R$, M is simple. ▨
(I maximal)

Lemma 2.2 [Schur's Lemma]: Let $M, N \in \text{Mod-}R$ be simple. If $f \in \text{Hom}(M, N)$, then $f = 0$ or f is an isomorphism. In particular: $\text{End}(M_R)$ is a division ring.

$\underline{\text{Proof}}$: $\ker f \leq M$, $\text{im } f \leq N$, so $\ker f \in \{0, M\}$, $\text{im} f \in \{0, N\}$.
If $f \neq 0$ then $\ker f \neq M$, $\text{im} f \neq 0$.
$\Rightarrow \ker f = 0$, $\text{im} f = N \Rightarrow f$ is an iso. ▨

$\underline{\text{Remark}}$: If M, N are simple, either $M \cong N$ or $\text{Hom}(M, N) = 0$.

$\underline{\text{Recall}}$: A field k is algebraically if every nonconstant $f \in k[x]$ has a root in k.
$\Leftrightarrow$ Every $f \in k[x] \setminus k$ factors into linear factors.
$\Leftrightarrow$ If L/k is a finite field extension, then $L = k$.

Lemma 2.3: A field k is algebraically closed $\Leftrightarrow$
If $D \supseteq k$ is a fin. dim division algebra (i.e. div. ring and fin. dim. k-algebra), then $D = k$.

$\underline{\text{Proof}}$: ($\Leftarrow$): If L/k is a finite field ext., it is a fin. dim. div. alg. $/k$.

($\Rightarrow$): Let $a \in D$. Since $k \subseteq Z(D)$, $k(a)/k$ is a field extension.
$\dim_k k(a) \leq \dim_k D < \infty \underset{k \text{ alg. closed}}{\Longrightarrow} k(a) = k \Rightarrow a \in k$.

Corollary 2.4: Suppose k is an alg. closed field, R k-algebra, M a simple R-module s.t. $\dim_k(M) < \infty$. Then $\operatorname{End}(M_R) = k$ (canonically).

<u>Proof:</u> $k \hookrightarrow \operatorname{End}(M)$ via scalar mult.: $\lambda \in k \longmapsto (m \mapsto m\lambda)$
$\operatorname{End}(M_R) \subseteq \operatorname{End}(M_k) \cong M_d(k)$ for $d = \dim_k(M)$, so $\operatorname{End}(M_R)$ is a fin.-dim. k-algebra and a division ring (L 1.2).
$\underset{k \text{ alg. closed}}{\Longrightarrow} \operatorname{End}(M_R) = k$. $\square$

<u>Example:</u> If R is a fin. dim. $\mathbb{C}$-algebra (e.g. $R = \mathbb{C}[G]$ with G finite), $\operatorname{End}(M_R) \cong \mathbb{C}$ for all simple R-modules.

2.2. Composition series

<u>Definition:</u> Let $M \in \text{Mod-}R$. A composition series for M is a chain of submodules

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$$

s.t. M_i/M_{i-1} is simple for $1 \leq i \leq n$.
We call n the length of the chain.

<u>Example:</u>
- $(\mathbb{Z}/12\mathbb{Z})_{\mathbb{Z}}$ has a composition series:

$$0 = \underbrace{{}^{12\mathbb{Z}}/_{12\mathbb{Z}} \subsetneq {}^{6\mathbb{Z}}/_{12\mathbb{Z}}}_{\mathbb{Z}/2\mathbb{Z}} \underbrace{\subsetneq \frac{2\mathbb{Z}}{12\mathbb{Z}}}_{\mathbb{Z}/3\mathbb{Z}} \underbrace{\subsetneq {}^{\mathbb{Z}}/_{12\mathbb{Z}}}_{\mathbb{Z}/_{12}\mathbb{Z}}$$

- $\mathbb{Z}_{\mathbb{Z}}$ does not have a composition series
(between $n\mathbb{Z} \supsetneq 0$, we can always insert $mn\mathbb{Z}$, $m \geq 1$) ${}^{n\mathbb{Z}}/_{0}$ not simple

Lemma 2.5 [Modular Law]: Let $M \in \text{Mod-}R$, $A, B, C \leq M_R$ s.t. $B \subseteq A$. Then $A \cap (B+C) = \underset{(A\cap B)}{\overset{\shortparallel}{B}} + (A \cap C)$.

Proof: ($\supseteq$): $B \subseteq A \cap (B+C)$ and $(A\cap C) \subseteq A \cap (B+C)$ ✓

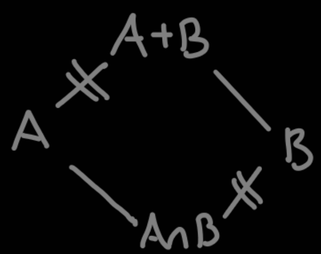
($\subseteq$): Let $a = b + c$, with $a \in A$, $b \in B$, $c \in C$.

$\Rightarrow c = a - b \in A \Rightarrow a = \underset{B}{\underset{\Uparrow}{b}} + \underset{A\cap C}{\underset{\Uparrow}{c}} \in B + (A \cap C)$.

Recall: If $A, B \leq M_R$ ($M \in \text{Mod-}R$), then

One of the isomorphism theorems.

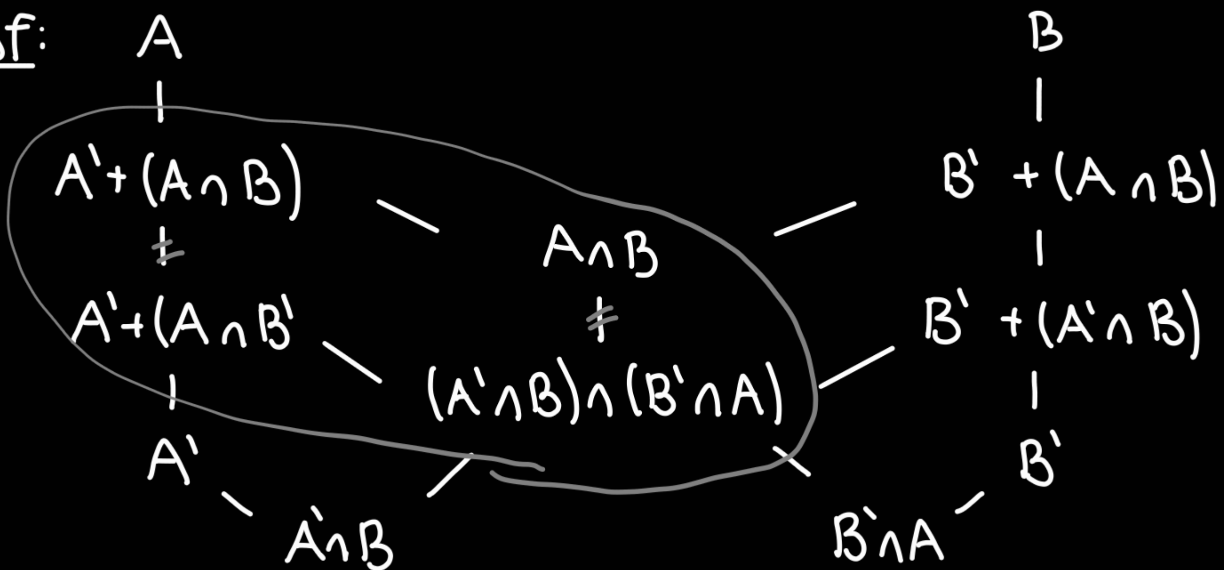
$$A+B/A \cong B/A\cap B.$$



Lemma 2.6 [Zossenhaus]: Let $A' \leq A$, $B' \leq B$ be submodules of some $M \in \text{Mod-}R$. Then

$$\frac{(A\cap B) + A'}{(A\cap B') + A'} \cong \frac{(A\cap B) + B'}{(A'\cap B) + B'}$$

Proof:



Note: ·) $A' + \cancel{(A\cap B')} + (A\cap B) = A' + (A \cap B)$

·) $(A\cap B) \cap (A' + (A\cap B')) \underset{A\cap B' \subseteq A\cap B}{\overset{L.2.5}{=}} (\cancel{A} \cap B \cap A') + (A\cap B')$

$= (B \cap A') + (A \cap B')$

$$\Rightarrow \frac{A' + (A \cap B)}{A' + (A \cap B')} \underset{\text{From above}}{\cong} \frac{A \cap B}{(B \cap A') + (A \cap B')} \underset{\text{symmetry}}{\cong} \frac{B' + (A \cap B)}{B' + (A' \cap B)} \qquad \blacksquare$$

Definition: Two chains of submodules $0 = A_0 \leq A_1 \leq \cdots \leq A_m = M$, $0 = B_0 \leq B_1 \leq \cdots \leq B_n$ are equivalent (or isomorphic) if $m = n$ and there is a permutation $\sigma : [n] \to [n]$ s.t.

$$A_i / A_{i-1} \cong B_{\sigma(i)} / B_{\sigma(i)-1} \quad \forall i.$$

Theorem 2.7 [Schreier refinement theorem]: Let $M \in \text{Mod-}R$. Any two chains $0 = A_0 \leq A_1 \leq \cdots \leq A_m = M$, $0 = B_0 \leq B_1 \leq \cdots \leq B_n = M$ have equivalent refinements.

Proof: For $1 \leq i \leq m$, $1 \leq j \leq n$:
$$A_{i,j} := (A_i \cap B_j) + A_{i-1}$$
$$B_{j,i} := (A_i \cap B_j) + B_{j-1}$$

$\to \{A_{ij} : j\}$ refines $A_{i-1} \leq A_i$, $\{B_{j,i} : i\}$ refines $B_{j-1} \leq B_j$.

$$A_i = A_{i,n} \geq A_{i,n-1} \geq \cdots \geq A_{i,1} \geq A_{i,0} = A_{i-1}$$
$$B_j = B_{j,m} \geq B_{j,m-1} \geq \cdots \geq B_{j,1} \geq B_{j,0} = B_{j-1}$$

Now: $$A_{i,j} / A_{i,j-1} \cong \frac{(A_i \cap B_j) + A_{i-1}}{(A_i \cap B_{j-1}) + A_{i-1}}$$

$$\overset{L2.6}{\cong} \frac{(A_i \cap B_j) + B_{j-1}}{(A_{i-1} \cap B_j) + B_{j-1}} \cong B_{j,i} / B_{j,i-1}$$

$\Rightarrow$ The refinements are equivalent. $\blacksquare$

October 16, 2025

Corollary [Jordan-Hölder Theorem]: Any two composition series of a module M_R are equivalent.

Proof: Let $\underline{0} = A_0 \subsetneq A_1 \subsetneq \dots \subsetneq A_m$, $\underline{0} = B_0 \subsetneq B_1 \subsetneq \dots \subsetneq B_n = M$ be composition series. By Theorem 2.7 they have equivalent refinements $\{A_{i,j}\}$, $\{B_{j,i}\}$. Some factors $A_{i,j}/A_{i,j-1}$, $B_{j,i}/B_{j,i-1}$ may be zero, but the nonzero ones correspond to the composition factors of the respective series. The nonzero factors must be paired with the nonzero in the equivalence, and the chain follows. $\boxtimes$

Definition: Let $M \in \text{Mod-}R$. The length of M, $\ell(M) \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ is the length of a composition series if one exists, $\ell(M) = \infty$ otherwise. M has finite length if $\ell(M) < \infty$.

Lemma 2.9: Let $M \in \text{Mod-}R$. TFAE:

(a) M has a composition series.
(b) $\ell(M) < \infty$
(c) M is noetherian and artinian

Proof: (a) $\Leftrightarrow$ (b) by definition

(a) $\Rightarrow$ (c): Let $\underline{0} = A_1 \subsetneq A_2 \subsetneq \dots \subsetneq A_n = M$ be a composition series. If $B_1 \subsetneq B_2 \subsetneq \dots \subsetneq B_{m-1}$ is any chain of submodules, then $m \leq n$ by Theorem 2.7. In particular, there are no infinite ascending or descending chains.

(c) $\Rightarrow$ (a): Recursive definition of A_i: $A_0 := \underline{0}$.
Suppose we have $A_0 \subsetneq A_1 \subsetneq \dots \subsetneq A_{i-1}$ s.t. A_j/A_{j-1} is simple $\forall 1 \leq j \leq i-1$. If $A_{i-1} = M$, this is a composition series.
If $A_{i-1} \subsetneq M$, the set $\Omega = \{A \leq M_R : A_{i-1} \subsetneq A_i\}$ has a minimal element A_i (by artinianity), so A_i/A_{i-1} is simple.
This process stops after finitely many steps by noetherianity. $\boxtimes$

2.3. Semisimple Modules

Recall: If $M \in \text{Mod-}R$, and $(M_i)_{i\in I}$ is a family of submodules, then $\sum_{i\in I} M_i$ is the smallest submodule of M containing all M_i.
Elements: $\sum_{i\in I} m_i$ with $m_i \in M_i$, finitely many m_i nonzero.

$\sum_{i\in I} M_i$ is direct (an internal direct sum) if $\forall i \in I$.

$$M_i \cap \sum_{j\in I\setminus\{i\}} M_j = \underline{0}$$

Then $\sum_{i\in I} M_i \cong \bigoplus_{i\in I} M_i$ (external direct sum)

Definition: $M \in \text{Mod-}R$ is semisimple (= completely reducible) if it is a direct sum of simple modules.

Examples: ·) simple modules are semisimple

·) If D is a division ring, each D-module V has a basis $(e_i)_{i\in I}$, i.e. $V = \sum_{i\in I} e_i D$ (direct) with $e_i D$ simple, so every D-module is semisimple.

·) $\underline{0}$ is semisimple, not simple (empty direct sum)

·) $\mathbb{Z}_{\mathbb{Z}}$ is not semisimple, $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (p prime) is semisimple, $\mathbb{Z}/p^2\mathbb{Z}$ is not.

·) D division ring, $M_n(D) = S_1 \oplus \cdots \oplus S_n$ with $S_i = E_{ii} M_n(D)$ (matrices where all entries outside the i-th row are zero).
S_i is simple as right $M_n(D)$-module, so $M_n(D)_{M_n(D)}$ is semisimple.

Lemma 2.10: If $M = \sum_{i\in I} M_i$ with simple $M_i \leq M$, and $N \leq M$, there exists $I' \subseteq I$ s.t. $M = N \oplus \bigoplus_{i\in I'} M_i$.

Proof: Let $\Omega := \{ J \subseteq I \mid N + \sum_{j\in J} M_j$ is direct$\}$.
Then $\Omega \neq \emptyset$ since $\emptyset \in \Omega$. If $\Omega' \subseteq \Omega$ is a chain w.r.t. $\subseteq$, then $J' := \bigcup_{J\in\Omega'} J \in \Omega$. [If not, there exists $n + \sum_{j\in J'} m_j = 0$, not all $m_j = 0$, but only finitely many nonzero. So this is actually supported on some $J \in \Omega'$ ↯.]
Zorn's lemma $\Rightarrow$ Ω has a maximal element I'

Let $M' := \sum_{i\in I'} M_i$. Claim: $M = N + M'$

$\forall i \in I.\ M_i \cap (N + M') \in \{0, M_i\}$ by simplicity.
But $M_i \cap (N + M') = 0$ ↯ I' maximal in Ω, so
$M_i \cap (N + M') = M_i \Rightarrow M_i \leq N + M'$
$\Rightarrow M = N + \sum_{i\in I} M_i \leq N + M'$ ▨

Lemma 2.11: Let $0 \neq M \in$ Mod-R. Suppose that for every $N \leq M$ there exists $K \leq M$ s.t. $M = N \oplus K$. Then M contains a simple submodule.

Proof: The assumption also holds for all $M' \leq M$:
If $N \leq M'$, $\exists K: M = N \oplus K$. Then $M' = N \oplus (K \cap M')$ (because $N \subseteq M'$!)

Thus w.r.t. $M = mR$, $m \neq 0$. By Zorn's lemma, there exists $N \leq M$ s.t. N is maximal with $m \notin N$. By assumption, there exists K s.t. $M = N \oplus K$. If $0 \neq K' \leq K$, then $N \oplus K' \ni m$ by maximality of N. Then $M = N \oplus K'$, hence $K' = K$. Thus, K is simple. ▨

Theorem 2.12: For $M \in \text{Mod-}R$ TFAE:
(a) M is semisimple
(b) M is a sum of simple modules.
(c) For every $N \leq M$, there exists $L \leq M$ s.t. $M = L \oplus N$.

Proof: (a) $\Rightarrow$ (b) ✓
(b) $\Rightarrow$ (c) Let $M = \sum_{i \in I} M_i$ with M_i simple.
$\overset{2.10}{\Rightarrow} \exists I' \subseteq I.$ $M = N \oplus \bigoplus_{i \in I} M_i$. Take $L := \bigoplus_{i \in I'} M_i$.

(c) $\Rightarrow$ (a): Let N be the sum of all simple submodules of $M \Rightarrow M = N \oplus L$ for some $L \leq M$. L also satisfies (c) but cannot contain a simple submodule. Thus $L = 0$ by L2.11. ◪

Corollary: Quotients and submodules of semisimple modules are semisimple.

Proof: For quotients use 2.12(b) (images of simple modules are simple or 0). For submodules use 2.12(c) [& proof of L2.11]. ◪

Remark: (1) If $M = M_1 \oplus \cdots \oplus M_k$ with simple M_i, then the M_i are unique up to isomorphism & order, since $0 \subsetneq M_1 \subsetneq M_1 \oplus M_2 \subsetneq \cdots \subsetneq M_1 \oplus \cdots \oplus M_k$ is a composition series with composition factors $M_1, \dots, M_k$.

(2) Endomorphism Rings: Suppose $M_R \cong M_1 \oplus \cdots \oplus M_k$.
Let $\varepsilon_i : M_i \longrightarrow M$ be the cannonical embedding, $\pi_i : M \to M_i$ the canonica projection, so $m = \sum_{i=1}^{k} \varepsilon_i(\pi_i(m))$ $\forall m \in M$.
If $f \in \operatorname{End}(M_R)$, then $f(m) = \sum_{i,j=1}^{k} \varepsilon_i \circ \underbrace{\pi_i \circ f \circ \varepsilon_j}_{=: f_{ij}} \circ \pi_j(m)$

with $\varphi_{i,j}: M_j \longrightarrow M_i$.

Then $\mathrm{End}(M_R) \longrightarrow \bigoplus_{i,j=1}^{k} \mathrm{Hom}(M_j, M_i)$, $\varphi \longmapsto [\varphi_{ij}]_{i,j=1}^{k}$ (*)

is an isomorphism of abelian groups.

If $\varphi, \psi \in \mathrm{End}(M)$, then (easy exercise):

$$(\psi \circ \varphi)_{ij} = \sum_{l=1}^{k} \psi_{il} \circ \varphi_{lj},$$

so considering the RHS to be formal matrices, (*) is a ring isomorphism.

Proposition 2.14: Let M_R be semisimple of finite length, say $M \cong M_1^{n_1} \oplus \cdots \oplus M_n^{n_k}$ with M_i simple, $M_i \not\cong M_j$ for $i \neq j$. Then $\underset{\uparrow \text{module}}{\mathrm{End}(M)} \cong \underset{\uparrow \text{matrix ring } M_{n_1}(D_1)}{M_{n_1}(D_1)} \times \cdots \times M_{n_k}(D_k)$ with $D_i := \mathrm{End}(M_i)$ division rings.

Proof: $\mathrm{End}(M) \underset{(*)}{\cong} \bigoplus_{i,j=1}^{k} \mathrm{Hom}(M_j^{n_j}, M_i^{n_i})$

since $\mathrm{Hom}(M_j, M_i) = 0$ for $i \neq j$ L2.2 $= \bigoplus_{i=1}^{k} \mathrm{End}(M_i^{n_i})$

$\underset{(*)}{\cong} \bigoplus_{i=1}^{k} M_{n_i}(\mathrm{End}(M_i))$

$\mathrm{End}(M_i)$ is a divison ring by L2.2. ▨

2.4 Semisimple Rings:

Definition: A ring R is (right) semisimple if R_R is a semisimple module.

Remark: Later: right semisimple $\Leftrightarrow$ left semisimple.

Examples: •) D div. ring is semisimple, as is $M_n(D)$.

•) R_1, R_2 semisimple $\Rightarrow R_1 \times R_2$ semisimple
[If M is an $R_1 \times R_2$ module, then $M = M_1 \oplus M_2$ with $M_i \in \text{Mod-}R_i$.]

•) $\mathbb{Z}$ is not semisimple

•) $\mathbb{Z}/n\mathbb{Z}$ semisimple $\Leftrightarrow$ n squarefree $\Leftrightarrow \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r\mathbb{Z}$,
p_i pairwise distinct

Recall: If M, N, K are R-modules:

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} K \longrightarrow 0 \quad \text{is SES}$$

$\Leftrightarrow \ker f = 0$, $\operatorname{im} f = \ker g$, $\operatorname{im} g = 0$

(1) The SES is split exact if

$\exists f' : N \to M.\ f' \circ f = \mathrm{id}_M$

$\Leftrightarrow \exists g' : K \to K.\ g \circ g' = \mathrm{id}_K$

$\Leftrightarrow \exists \varphi : N \xrightarrow{\sim} M \oplus K$ s.t.

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d, "\mathrm{id}_M"] & N \arrow[r] \arrow[d, "\varphi"] & K \arrow[r] \arrow[d, "\mathrm{id}_K"] & 0 \\
0 \arrow[r] & M \arrow[r] & M \oplus K \arrow[r] & K \arrow[r] & 0
\end{tikzcd}$$

commutes

$m \longmapsto (m, 0)$

$(m, k) \longmapsto k$

(2) P_R is projective if every SES $0 \to M \to N \to P \to 0$ splits

(3) I_R is injective if every SES $0 \to I \to N \to K \to 0$ splits.

Theorem 2.15: Let $R \in \mathrm{Rng}$. TFAE:
(a) R is right semisimple.
(b) All SES in Mod-R split.
(c) All $M \in$ Mod-R are semisimple.
(d) All f.g. $M \in$ Mod-R are semisimple.
(e) All cyclic $M \in$ Mod-R are semisimple.

Proof: (b)$\Rightarrow$(c): Let $N \leq M$. Then $0 \to N \to M \to M/N$ is split exact by (b), so $M = N \oplus K$ with $K \cong M/N$. $\overset{T.2.12(c)}{\Rightarrow}$ M semisimple.

(c) $\Rightarrow$ (d) $\Rightarrow$ (e) ✓ (e) $\Rightarrow$ (a): R_R is cyclic.

(a) $\Rightarrow$ (c): R_R semisimple $\Rightarrow R_R^{(I)}$ semisimple for all index sets I. Every module M_R is a quotient of some free module $R_R^{(I)}$, hence semisimple [C2.13].

(c) $\Rightarrow$ (b): Let $0 \to M \xrightarrow{f} N \xrightarrow{g} K \to 0$ be exact.
N semisimple $\Rightarrow N = f(M) \oplus K'$ with $K' \leq N$ [T 2.12]
Define $f': N \to M$ by $N \underset{proj.}{\twoheadrightarrow} f(M) \xrightarrow{f^{-1}} M$. Then $f' \circ f = \mathrm{id}_M$. ▨

Corollary 2.16: If R_R is right semisimple, then
$R_R = M_1^{n_1} \oplus \cdots \oplus M_k^{n_k}$ with simple pairwise nonisomorphic $M_i \in$ Mod-R.
In particular, R_R has finite length and only finitely many simple modules $M_1, \dots, M_k$.

Proof: We know $R_R = \bigoplus_{i \in I} M_i$ with simple M_i. But $R_R = 1 \cdot R_R$ is cyclic, and there is a finite $I_0 \subseteq I$ s.t. $1 \in \bigoplus_{i \in I_0} M_i \Rightarrow R_R = \bigoplus_{i \in I_0} M_i$. ▨

Remark: Similarly, if M_R is semisimple:
M_R f.g. $\Leftrightarrow M \cong M_1 \oplus \cdots \oplus M_n$, M_i simple $\Leftrightarrow \ell(M) < \infty$.

Corollary 2.17: TFAE:
(a) R is right semisimple
(b) Every $M \in \text{Mod-}R$ is projective.
(c) Every $M \in \text{Mod-}R$ is injective.

Proof: (a)$\Leftrightarrow$(b) and (a)$\Leftrightarrow$(b) both follow from T2.15 (b) ▨

If D_i div. ring, then $M_{n_i}(D_i)$ is semisimple. Finite products of semisimple rings are semisimple, so $M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ is semisimple.

Theorem 2.18 [Wedderburn-Artin]: If R is right semisimple, then $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ with D_i division rings, $n_i \geq 1$, where k and $(D_1, n_1), \dots, (D_k, n_k)$ are uniquely determined (up to order and isomorphism) and R has exactly k simple modules $S_1, \dots, S_k$ up to isomorphism. Also $D_i \cong \text{End}(S_i)$.

October 23, 2025

Proof: Existance: $R_R \overset{C2.16}{=} S_1^{n_1} \oplus \cdots \oplus S_k^{n_k}$ with simple S_i, $S_i \not\cong S_j$ if $i \neq j$
$\Phi: R \longrightarrow \text{End}(R_R)$, $r \mapsto \Phi_r$, $\Phi_r(x) = rx$ is a ring hom
$\overset{P2.14}{\Rightarrow} R \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ with $D_i \cong \text{End}(S_i)$.

Uniqness: of simple modules: $S \in \text{Mod-}R$ simple
$\Rightarrow \exists$ epi $f: S_1^{n_1} \oplus \cdots \oplus S_n^{n_k} \twoheadrightarrow S$
$\Rightarrow S$ is a composition factor of R_R
$\Rightarrow S \cong S_i$ for some i.

of matrix rings: Suppose $R \cong M_{m_1}(E_1) \times \cdots \times M_{m_e}(E_e)$, E_i division rings, $m_i \geq 1$ $\Rightarrow M_{m_i}(E_i) \cong V_i^{m_i}$ with V_i simple in $\text{Mod-}M_{m_i}(E_i)$.
$\Rightarrow V_1, \dots, V_e$ are nonisomorphic simple R-modules
[with $V_i M_{m_j}(E_j) = 0$ $\forall i \neq j$]

$\Rightarrow R_R = V_1^{m_1} \oplus \cdots \oplus V_\ell^{m_\ell}$

Uniqness of composition series (after renumbering):

$k = \ell$, $S_i \cong V_i$, $n_i = m_i$ $\forall i$

$D_i = \mathrm{End}(S_i) \cong \mathrm{End}(V_i) \cong E_i$ $\square$

Remark: Analogous statement holds for left semisimple, but now $D_i \cong \mathrm{End}(S_i)^{op}$, because $\mathrm{End}({}_R R) \cong R^{op}$.

Corollary: R right semisimple $\Leftrightarrow$ R left semisimple

$\Rightarrow$ We say: R is *semisimple* (without left, right)

Definition: A ring R is *simple* if $R \neq \underline{0}$ and it has no nonzero proper ideal.
(two sided)

Example: $\cdot)$ $M_n(D)$, D div. ring (then $M_n(D)$ is also artinian).

$\cdot)$ $A_1(k)$, k field, char $k = 0$, is simple (exercise)

So: R semisimple $\Longrightarrow$ $R = R_1 \times \cdots \times R_k$ with R_i simple artinian.

⚠ R simple ring $\not\Rightarrow$ R_R simple module
(not even R_R semisimple, $A_1(k)$)

Proposition: If R is a ring s.t. $R = R_1 \times \cdots \times R_k = R_1' \times \cdots \times R_\ell'$ with R_i, R_j' simple $\Rightarrow k = \ell$, $R_i = R_i'$ after renumbering ($=$, not just $\cong$).

Proof: $R_i, R_j' \trianglelefteq R$ (ideal) and $R_i R = R_i$, $R_j' R = R_j'$

$R_i = (R_i R_1') \times \cdots \times (R_i R_\ell') \Rightarrow R_i R_j' \in \{\underline{0}, R_i\}$ since R is simple and $R_i R_j' \trianglelefteq R_i$

$0 \neq R_i \Rightarrow \exists j : R_i R_j' = R_i$, also $R_i R_j' \trianglelefteq R_j' \Rightarrow R_i R_j' = R_j' \Rightarrow R_i = R_j'$ $\square$

2.5. Simple artinian rings

Definition: Let $M \in \text{Mod-}R$.

(1) The annihilator of M is $\operatorname{ann}(M) := \{r \in R \mid Mr = 0\}$
$= \{r \in R \mid \forall m \in M.\ mr = 0\}$.

(Note: $\operatorname{ann}(R) \trianglelefteq R$).

(2) M is faithful if $\operatorname{ann}(M) = 0$, otherwise unfaithful.

(3) R is right primitive if it has a faithful simple right R-modules. (right prim $\neq$ left primitive)
↳ hard to show

[Suppose R is commutative: M_R simple module $\Rightarrow M_R \cong R/I$, I maximal ideal of R $\Rightarrow \operatorname{ann}(M) = I$.
If R is (right) primitive $\Rightarrow 0$ is the annihilator of some (R/I), $I \trianglelefteq R$ maximal $\Rightarrow 0$ max. ideal of R $\Rightarrow 0, R$ are the only ideals of R ($\Leftrightarrow R$ simple) $\Rightarrow R$ field].
This is why this notion does not show up in the com. setting.

Theorem 2.21: TFAE for a ring R:
(a) R is simple artinian
(b) R is simple and has a minimal nonzero right ideal
(c) R is right primitive and right artinian
(d) R is semisimple with unique simple module up to iso.
(e) $R \cong M_n(D)$, D div. ring, $n \geq 1$

Proof: (a) $\Rightarrow$ (b): $R \neq 0$, so $\Omega = \{0 \neq I_R \leq R_R\} \neq \emptyset$
By right artinianity, Ω has a minimal element.

(b) $\Rightarrow$ (c): Let I_R be a minimal nonzero right ideal.

Then $1 \notin \mathrm{ann}(I_R) \trianglelefteq R \Rightarrow \mathrm{ann}(I_R) = 0 \Rightarrow I_R$ faithful, simple

trick For every $r \in R$, $\varphi_r : I_R \to rI_R$, $x \mapsto rx$ has $\ker \varphi \in \{0, I_R\}$
$\Rightarrow rI_R$ simple or $rI_R = 0$

by simplicity $R_R = RI$

$\Rightarrow R_R = \sum_{r \in R} rI$ is a sum of simple modules $\Rightarrow R_R$ semisimple
$\Rightarrow R_R$ is artinian

<u>(c) ⇒ (d)</u>: Let $M_R \in$ Mod-R be faithful, simple.
Consider $\mathcal{F} = \{f : R_R \to M_R^n \mid n \geq 0, f$ R-hom$\}$. Since R is left artinian $\{\ker(f) \mid f \in \mathcal{F}\}$ has a minimal element.
Pick $f \in \mathcal{F}$ with $\ker(f)$ minimal.

<u>Claim</u>: $\ker f = 0$

[Suppose not. Let $0 \neq r \in \ker f$. $\mathrm{ann}(M) = 0 \Rightarrow \exists m \in R.\ mr \neq 0$.
Define $\hat{f} : R \to M^n \oplus M$ $\Rightarrow \ker \hat{f} \subsetneq \ker f$ ↯ contradiction minimality
$x \mapsto (f(x), mx)$]

So $f : R_R \hookrightarrow M_R^n$, M_R^n semisimple $\overset{T2.12}{\Rightarrow} M_R^n \cong R_R \oplus K_R$
$\overset{C2.13}{\Longrightarrow} R_R$ semisimple, $R_R \cong M_R^m$ for some $m \leq n$.

<u>(d) ⇒ (e)</u>: [T 2.18]

<u>(e) ⇒ (a)</u>: ✓ (exercises, fin. dim $\rightsquigarrow$ artinian) ▨

right art $\not\Rightarrow$ left art
right primitive $\not\Rightarrow$ left primitive

$\left.\begin{array}{l}\text{right artinian} \\ + \text{right primitive}\end{array}\right\} \Rightarrow$ left art, left prim

Remark 1) $D \cong \mathrm{End}(V_R)$ with V_R the unique simple right R-module, but $D \cong \mathrm{End}({}_RW)^{op}$ with ${}_RW$ the unique simple left module.

2) R simple artinian $\Leftrightarrow$ R simple right artinian $\Leftrightarrow$ R simple left artinian
$\Updownarrow$ $\Updownarrow$
R right prim, right art $\Leftrightarrow$ R left prim, left art

2.6. Maschke's Theorem

Let $(G,\cdot)$ be a group. Fix a field K. A representation of G is a group hom. $\rho: G \to GL(V)$ with V a K-vector space. If $\dim V = n < \infty$, $GL(V) \cong GL_n(K)$ (non-canonically, by chosing a basis).

Representations are useful in studying groups (finite & infinite).
$\rightsquigarrow$ Representation Theory of Groups

If $\rho: G \to GL(V)$, $\sigma: G \to GL(W)$ are representations, a homomorphism is a K-linear $T: V \to W$ s.t. $T(\rho(g)v) = \sigma(g)Tv$.
$\Rightarrow$ Repr. form a category.

Proposition 2.22: G group, K field. There is a category equivalence:

$$\{\text{Repr of } G\} \longleftrightarrow \{\text{(left) } K[G]\text{-modules}\}$$

Sketch: A $K[G]$-module structure on an abelian group $(M,+)$ corresponds to a ring hom. $\rho: K[G] \to \mathrm{End}(M_{\mathbb{Z}})$.
"$\longleftarrow$": A $K[G]$ module M is a k-vector space $(\rho|_K)$
"$\longmapsto$": A repr. $\rho: G \to GL(V_k)$ gives rise to a monoid hom

$$\rho: (G,\cdot) \longrightarrow (\mathrm{End}(V_k), \circ).$$

ring

Using the UP of $K[G]$, this extends to a K-alg hom.
$\tilde{\rho}: K[G] \longrightarrow \mathrm{End}(V_K)$. $\square$

The irred. repr. $\cong$ simple modules
completely reducible repr $\cong$ semisimple modules

Theorem 2.23 [Maschke]: If G is a finite group then $K[G]$ is semisimple $\Leftrightarrow \operatorname{char} K \nmid |G|$.
In particular: $\mathbb{C}[G]$ is semisimple.

Proof: ($\Leftarrow$): Let $I_{K[G]} \leq K[G]$ be a right ideal.
We show: the SES $0 \longrightarrow I \hookrightarrow K[G] \xrightarrow{\pi} \underbrace{K[G]/I}_{:=V} \longrightarrow 0$
of $K[G]$-module splits [T 2.12(c)].
Since it splits as a SES of K-vector spaces
$\exists \varphi \in \operatorname{Hom}(V_K, K[G]_K)$ s.t. $\pi \circ \varphi = \mathrm{id}_V$.
$\operatorname{char} K \nmid |G| \Rightarrow |G| \in K^\times$
Define: $\tilde{\varphi}(v) := \frac{1}{|G|} \sum_{g \in G} \varphi(vg)g^{-1}$.

$\tilde{\varphi}$ is a $K[G]$-hom: K-linear ✓

$$\tilde{\varphi}(\underset{V}{v}\,\underset{G}{h}) = \frac{1}{|G|} \sum_{g \in G} \varphi(vhg)g^{-1} = \frac{1}{|G|} \sum_{g \in G} \varphi(vg)g^{-1}h$$

$g' := hg \Rightarrow g = h^{-1}g' \Rightarrow g^{-1} = (g')^{-1}h$

$\pi \circ \tilde{\varphi} = \mathrm{id}$: $\quad \pi \circ \tilde{\varphi} = \frac{1}{|G|} \sum_{g \in G} \underbrace{(\pi \circ \varphi)(vg)}_{vg} g^{-1} = v$

($\Rightarrow$): For $f = \sum_{g \in G} a_g g \in K[G]$, define $\varepsilon(f) = \sum_{g \in G} a_g$ (augementation map)

$I := \ker(\varepsilon)$ (augementation ideal)

We show: $I \cap J \neq 0$ for any nonzero right ideal $J \trianglelefteq K[G]$
Then $0 \to I \hookrightarrow K[G] \xrightarrow{\varepsilon} K \to 0$ is non split, hence $K[G]$ is not semisimple.

Let $0 \neq x = \sum_{g \in G} a_g g \in J$

Case 1: $\varepsilon(x) = 0 \Rightarrow x \in I \cap J$

Case 2: $\varepsilon(x) \neq 0$ Let $s := \sum_{g \in G} g \Rightarrow \varepsilon(s) = |G| \cdot 1_K = 0_K \Rightarrow s \in I$

$$\underset{I \cap J}{xs} = \left(\sum_{g \in G} a_g g\right)\left(\sum_{h \in G} h\right) = \sum_{g \in G} a_g \underbrace{\sum_{h \in G} gh}_{s} = \underset{K^\times}{\varepsilon(x)} \cdot s \neq 0$$

∎

Proposition 2.24: If $|G| = \infty$, then $K[G]$ is not semisimple.

Proof: Consider again the augmentation map $\varepsilon : K[G] \longrightarrow K$, augmentation ideal I. Suppose $K[G]$ is semisimple

$$0 \longrightarrow I \hookrightarrow K[G] \xrightarrow{\varepsilon} K \rightarrow 0 \quad \text{splits}$$

Let $\varphi : K \to K[G]$ s.t. $\varepsilon \circ \varphi = id_K$, φ $K[G]$-hom.

$\Rightarrow 0 \neq \varphi(1) =: f = \sum_{g \in G} a_g g$ with finitely many $a_g \neq 0$
(but at least one)

Let $h \in G$ s.t. $a_h \neq 0$
$K[G]$-module structure on K: $\forall g \in G \; \exists \lambda_g \in K.\ 1_K \cdot g = \lambda_g$

$$\left.\begin{aligned} \Rightarrow \varphi(g) &= \varphi(\lambda_g) = \varphi(1)\lambda_g = f\lambda_g \\ \varphi(g) &= f(1)g \qquad\qquad\quad = fg \end{aligned}\right\} \Rightarrow \forall g \in G.\ fg = f\lambda_g \neq 0$$

$\Rightarrow \forall g \in G.$ hg appears in support of f ↯ only finitely many $a_g \neq 0$ ∎

3. Jacobson Radical

<u>Definition</u>: Let $M \in \text{Mod-}R$, $X \subseteq M$ subset. We define the annihilator of X, $\operatorname{ann}(M) := \{r \in R \mid \forall x \in X.\ xr = 0\}$.

This is a right ideal.

$$\operatorname{ann}(\underset{\overset{\cap}{M}}{m}) := \operatorname{ann}(\{m\}), \quad \operatorname{ann} X = \bigcap_{x \in X} \operatorname{ann}(x)$$

If $X_R \leq M_R$, then $\operatorname{ann}(X_R) \trianglelefteq R$.

<u>Definition</u>: $I \trianglelefteq R$ is right primitive if $I = \operatorname{ann}(M_R)$, $M \in \text{Mod-}R$ simple.
[$\Leftrightarrow$ R/I is a right primitive ring]

<u>Example</u>: ·) $I \trianglelefteq R$ maximal $\Rightarrow$ I (right) primitive
[By Zorn's lemma, I is contained in a maximal right ideal J $\Rightarrow$ $(R/J)_R$ simple, $\operatorname{ann}(R/J) \supseteq I$ [$RI = J$]
$\Rightarrow \operatorname{ann}(R/J) = I$]

·) If R commutative: I primitive $\Leftrightarrow$ I maximal

[$I = \operatorname{ann}(R/J)$, $J_R \leq R_R$ maximal, J two-sided $\Rightarrow RJ \subseteq J$
$\Rightarrow J \subseteq \operatorname{ann}(R/J) \Rightarrow J = \operatorname{ann}(R/J) = I$.]

<u>Definition</u>: The Jacobson radical of R is

$$J(R) := \bigcap_{\substack{I \trianglelefteq R \\ I \text{ right primitive}}} I = \bigcap_{\substack{M_R \in \text{Mod-}R \\ \text{simple}}} \operatorname{ann}(M_R)$$

$J(R) = \mathcal{J}(R) = \operatorname{rad} R$

Note: $J(R) \trianglelefteq R$ and $J(R) \subsetneq R$ unless $R \neq 0$.

[**Properness:** If $R \neq 0$, there exists a max. right ideal $I \neq R \Rightarrow \operatorname{ann}(\underbrace{R/I}_{\neq 0}) \subsetneq R$]

Lemma 3.1: $\overset{A}{J(R)} = \overset{B}{\bigcap} \{ J \mid J_R \leq R_R \text{ maximal right ideal} \}$
$\overset{C}{=} \{ r \in R \mid \forall x \in R.\ 1 - rx \text{ is right invertible} \}$
$\overset{D}{=} \{ r \in R \mid \forall x, y \in R.\ 1 - xry \text{ is invertible} \}$

Note: Since the final condition is left/right symmetric, we also get the corresponding statements on the left.

E.g. $$J(R) = \bigcap_{\substack{I \trianglelefteq R \\ I \text{ left primitive}}} I$$

Proof: **$(A \subseteq B)$:** Let $J_R \leq R_R$ be maximal, $r \in J(R)$.
Claim: $r \in J$
R/J is a simple right R-module $\overset{r \in J(R)}{\Longrightarrow} (1+J) r = r + J = 0 + J$
$\Rightarrow r \in J$.

$(B \subseteq C)$: $\forall$ maximal $J_R \leq R_R$, $rx \in J \Rightarrow 1 - rx \notin J$ (otherwise $1 \in J$)
$\Rightarrow (1-rx)R$ is not contained in any max right ideal
$\Rightarrow (1-rx)R = R \Rightarrow \exists y \in R.\ 1 = (1-rx)y$.

$(C \subseteq A)$: Suppose $r \in C$. $Mr \neq 0$ for some simple module M.
$\Rightarrow \exists m \in M.\ mr \neq 0 \overset{M \text{ simple}}{\Longrightarrow} M = mrR \Rightarrow \exists x \in R.\ m = mrx$
$\Rightarrow m(1-rx) = 0 \underset{1-rx \text{ right invertible}}{\Rightarrow} m = 0$ ↯

$(C = D)$: $D \subseteq C$ ✓

C ⇒ D: Let $r \in \overset{=C}{J(R)}$, $x, y \in R$.

Show: $1 - xry \in R^\times$

$xr \in J(R) \overset{C=A}{\Rightarrow} \exists z \in R : (1 - \underbrace{xr}_{\in J(R)} y) z = 1 \Rightarrow z$ is left invertible

$z = 1 - \underbrace{(-xryz)}_{\in J(R)} \overset{C=A}{\Rightarrow} z$ is right invertible

$\Rightarrow z \in R^\times \Rightarrow 1 - xry \in R^\times$ ☒

Corollary 3.2: $J(R)$ is the largest ideal I s.t. $1 + I \subseteq R^\times$.

Examples: 1) $J(\mathbb{Z}) = 0$, $J(\mathbb{Z}/p^n\mathbb{Z}) = p\mathbb{Z}/p^n\mathbb{Z}$ $(n \geq 1)$

2) If $\prod_{i \in I} R_i$ is a product $\Rightarrow J(\prod_{i \in I} R_i) = \prod_{i \in I} J(R_i)$

3) R simple $\Rightarrow J(R) = \underline{0}$

4) R semisimple $\Rightarrow J(R) = \underline{0}$

5) $J(M_n(R)) = M_n(J(R))$ [Exercise]

October 30, 2025