

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 ($\neq nc$)

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

R is a domain $\Leftrightarrow 0$ is the only zero divisor
 $\Leftrightarrow R \neq \underline{0} - \{0\}$ 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: $T_n(R) = \begin{bmatrix} R & R & \cdots & R \\ 0 & R & \cdots & R \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & R \end{bmatrix}$

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

So: $A \in M_n(K)^*$ $\Leftrightarrow \det(A) \neq 0$ adjugate of A /
 A zero divisor $\Leftrightarrow \det(A) = 0$ classical adjoint of A

3) Hamilton quaternions $H := \mathbb{R}1 + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$

with $i^2 = -1$, $j^2 = -1$, $ij = -ji = k$ extended \mathbb{R} -linearly

$$\left(\Rightarrow i \begin{smallmatrix} \curvearrowright j \\ \curvearrowright k \end{smallmatrix} \quad jk = i = -kj, \quad ki = j = -ik, \quad k^2 = -1 \right)$$

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

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

reduced norm

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

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 zero divisor,
but not right zero divisor

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

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

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.

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

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

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

[$\Leftrightarrow \bar{f}$ is the unique k -algebra hom. s.t. $\bar{f}|_X = f$]

$$\begin{array}{ccc} X & \xrightarrow{\quad} & k\langle X \rangle \\ & \searrow f & \downarrow \exists! \bar{f} \\ & & R \end{array} \quad (\text{as } k\text{-algebras})$$

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

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

$|X| \geq 2$: We get something totally different from $k[x_1, \dots, x_n]$!

E.g.: $k\langle x, y \rangle$ contains a subring isomorphic to $k\langle z_i | i \in \mathbb{N}_0 \rangle$

$$f: k\langle z_i | i \in \mathbb{N}_0 \rangle \xhookrightarrow{\text{monomorphism}} k\langle x, y \rangle, z_i \mapsto x y^i$$

$$\text{e.g. } f(z_2 z_3 z_1) = x y^2 x y^3 x y$$

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. $f: k\langle x_i \mid i \in I \rangle \rightarrow R$, $x_i \mapsto g_i$
 f surjective $\Rightarrow R \cong k\langle x_i \mid i \in I \rangle / \ker f$

If $F = (f_j)_{j \in J}$ generates the ideal $\ker f$, 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 $xy - yx$
- $R\langle x, y \mid x^2 + 1, y^2 + 1, xy + yx \rangle \cong \mathbb{H} \quad (x \mapsto i, y \mapsto j)$
- $k\langle x, y \mid xy - yx - 1 \rangle =: A_1(k)$ is the 1st Weyl algebra

\exists k field, $\text{char } k = 0$, $R = A_1(k)$ 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)

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

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

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

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

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

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

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

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

Special cases: R commutative,

- G free monoid generated by a set X
 $\Rightarrow R[G]$ is the free R -algebra generated by X
- $G \cong (N_0^{(I)})$, say freely generated by $\{x_i \mid i \in I\}$, so elements of G are of the form $x_{i_1}^{n_1} \cdots x_{i_k}^{n_k}$, $i_1, \dots, i_k \in I$ pairwise distinct
 $\Rightarrow R[G] \cong$ polynomial ring

Universal property: If $f: R \rightarrow R'$ is a ring hom.,
 $\sigma: G \rightarrow (R', \cdot, 1)$ 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. $\bar{f}: R[G] \rightarrow R'$ s.t. $\bar{f}|_R = f, \bar{f}|_G = \sigma$.

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

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

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

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: $\exists b \in R \setminus \{0\}, \sigma(b) = 0$

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

Lemma: 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 $\forall a \in R. \quad xa = ax + \sigma(a)$

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

$$\text{E.g. } R = k[y], \quad k \text{ ring}, \quad \delta = \frac{d}{dy}$$

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

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

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 $\{\bar{x}^i \bar{y}^j \mid i, j \geq 0\}$ is, $A_1(k) \cong k[x][y; -\frac{d}{dx}]$)

c) Mixed case: R ring, $\sigma: R \rightarrow R$ endomorphism, $\delta: R \rightarrow R$ 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 $x \cdot a = \sigma(a)x + \delta(a)$ with maps $\sigma, \delta: R \rightarrow R$

$$\Rightarrow xab = x(ab) = \sigma(ab)x + \delta(ab)$$

$$\begin{aligned} &= (xa)b = (\sigma(a)x + \delta(a))b = \underbrace{\sigma(a)(\sigma(b)x + \delta(b))}_{\overset{\text{II}}{\sigma(ab)}} + \underbrace{\delta(a)b}_{\overset{\text{II}}{\delta(ab)}} \\ &= \underbrace{\sigma(a)\sigma(b)}_{\overset{\text{II}}{\sigma(ab)}} x + \underbrace{\sigma(a)\delta(b) + \delta(a)b}_{\overset{\text{II}}{\delta(ab)}} \end{aligned}$$

$\Rightarrow \sigma$ must be an endomorphism, δ a σ -derivation

(For additivity look at
 $x(a+b) = xa + xb$)

10) Formal power series: R ring, x indeterminate,

$$R[[x]] = \{a_0 + a_1x + a_2x^2 + \dots \mid a_i \in R\}.$$

Then $f \in R[[x]]^\times \Leftrightarrow a_0 \in R^\times$

Laurent series: $R((x)) := \left\{ \sum_{i=-n}^{\infty} a_i x^i \mid a_i \in R \right\}$

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

Twisted versions:

• $R[[x; \sigma]]$ with $\sigma \in \text{End}(R)$: $xa = \sigma(a)x$

• $R[[x; \sigma]]$ with $\sigma \in \text{Aut}(R)$: $xa = \sigma(a)x$
(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 " σ ": $M \times R \rightarrow M$ 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: $f: M \rightarrow N$, $f(m+m') = f(m) + f(m')$,
 $f(ma) = f(m)a$

$\text{Mod-}R$ is the category of all right R -modules

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

Category of left R -modules: $R\text{-Mod}$

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

IF M_R is a right R -module, it is a left R^{op} -module via $\overset{\uparrow}{R^{\text{op}}} \cdot m = m \cdot \overset{\uparrow}{R}$.

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

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

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

We will default to right modules.

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

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

$$\left[\begin{array}{l} \text{Given } \sigma, \text{ define } \tilde{\sigma}(a)(m) := ma. \\ \text{E.g. } \tilde{\sigma}(ab)(m) = mab = (\tilde{\sigma}(a)m)b = \tilde{\sigma}(b)(\tilde{\sigma}(a)(m)) \\ = (\tilde{\sigma}(b) \circ \tilde{\sigma}(a))m \Rightarrow \tilde{\sigma}(b \circ_{\text{op}} a) = \tilde{\sigma}(b) \circ \tilde{\sigma}(a). \\ \text{(Conversely, given } \tilde{\sigma}, \text{ define } m \cdot a := \tilde{\sigma}(a)m. \end{array} \right]$$

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

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

Equivalent data: a ring hom. $\varepsilon: R \rightarrow Z(A)$ \nwarrow center

$$\left[\begin{array}{l} \text{If } A \text{ is an } R\text{-algebra, } r \mapsto r \cdot 1_A \text{ is such a hom.} \\ \text{Conversely, } r \cdot a := \varepsilon(r)a \text{ defines an } R\text{-module structure on } A. \\ \qquad \qquad \qquad \text{multiplication in } A \end{array} \right]$$

Example: \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
- Rng = \mathbb{Z} -Alg as categories

Example [Endomorphism rings]:

Let $M_R \in \text{Mod-}R$,

$$\text{End}(M_R) := \left\{ f: M_R \rightarrow M_R \mid f \text{ R-module hom} \right\}$$

is a ring with multiplication \circ

$$\left[\begin{array}{l} \text{e.g. } (f \circ (g+h))(m) = f((g+h)(m)) \stackrel{\downarrow + \text{ pointwise}}{=} f(g(m)+h(m)) \\ \quad \quad \quad f \text{ hom} \stackrel{\curvearrowleft}{=} f(g(m)) + f(h(m)) \\ \quad \quad \quad = (f \circ g + g \circ h)(m). \end{array} \right]$$

Special cases:

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

\triangleleft r on left

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

- $\triangleleft \text{End}(RR) \cong R^{\text{op}}$ \leftarrow ^{↑ one reason why one might}
 $\text{prefer right modules over left}$

-) $R = K$ a field, $V_K \cong K^n$ finite dimensional vec. space
 $\Rightarrow \text{End}(V_K) \cong M_n(K)$ (f.d.)
-) K field, R f.d. K -algebra
 $\Rightarrow R \cong \text{End}(R_R) \subseteq \text{End}(R_K) \cong M_n(K)$ (as K -algebras)
So every f.d. K -algebra embeds into a matrix ring.

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

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 $M_1 \subseteq M_2 \subseteq \dots$ 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)
 $\Rightarrow \exists n_0 \geq 0: m_1, \dots, m_k \in M_{n_0} \Rightarrow M' \subseteq M_{n_0} \subseteq M_n \subseteq M' \quad \forall n \geq n_0$
 $\Rightarrow M_n = M_{n_0}$.

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

(c) \Rightarrow (a): Let $N \subseteq M$ and $\Omega := \{N' \subseteq N : N' \text{ is f.g.}\}$.

Then $\Omega \neq \emptyset \Rightarrow \Omega \neq \emptyset$. So $\exists N_0 \in \Omega$ that is maximal.
If $N_0 \subset N$, then $\exists x \in N \setminus N_0$, and $N_0 + xR \supseteq N_0$ but
 $N_0 + xR \in \Omega \quad \nsubseteq$
So N is f.g.



Definition: (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 [R_L] is noetherian.
(3) R is noetherian if it is right and left noetherian.

So: R right noetherian \Leftrightarrow every right ideal is f.g.

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

Proposition 1.2: Let $\sigma \in \text{Aut}(R)$, 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 $L \trianglelefteq_R R$ consider the left ideals $L_n \trianglelefteq_R R$ consisting of leading coeffs. of polynomials of degree $\leq n$ in $L + \text{terms}$).

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 $M_1 \supseteq M_2 \supseteq \dots$ 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 $M_1 \supseteq M_2 \supseteq \dots$ be a descending chain, $L := \{M_i \mid i \geq 1\}$ has a minimal element M_{n_0} ,
 $\Rightarrow \forall n \geq n_0. M_{n_0} = M_n$. □

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 [R_L] 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 ($\mathbb{Z} \supseteq 2\mathbb{Z} \supseteq 4\mathbb{Z} \supseteq 8\mathbb{Z} \supseteq \dots$)

• $\begin{bmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{bmatrix}$ is right noetherian $\left| \begin{bmatrix} \mathbb{Q} & \mathbb{C} \\ \mathbb{C} & \mathbb{C} \end{bmatrix}$ is right artinian
not left noetherian 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 $M_1, \dots, M_n \in \text{Mod-}R$. Then $\bigoplus_{i=1}^n M_i$ is noetherian [artinian]
 $\Leftrightarrow \forall i: M_i$ is noetherian [artinian].

(1) restated: if $0 \rightarrow N \rightarrow M \rightarrow L \xrightarrow{\cong M/N} 0$ is SES then
 M is noetherian [artinian] $\Leftrightarrow N, L$ are noetherian [artinian].

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

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

Suppose $L_1 \supseteq L_2 \supseteq \dots$ are submodules of M/N . Then $L_i = \frac{M_i + N}{N}$ with M_i submodules of M .

$$M_1 + N \supseteq M_2 + N \supseteq \dots$$

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

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

Both chains $M_1 \cap N \supseteq M_2 \cap N \supseteq \dots$ and

$\frac{M_1 + N}{N} \supseteq \frac{M_2 + N}{N} \supseteq \dots$ stabilize.

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

Claim: $M_i = M_{i_0}$

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

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

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

$$M_{i_0} \cap N = M_i \cap N$$

$$\overbrace{M_{i_0}}^{\uparrow} \quad \overbrace{M_i}^{\uparrow}$$

(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 $\exists m \in M. M = mR$

$\Leftrightarrow \exists \text{ epimorphism } \varphi: R_R \rightarrowtail M_R$

$$[(\Leftarrow): r \mapsto mr, (\Leftarrow): \varphi: R_R \rightarrowtail M_R, M = \varphi(R) = \overset{m}{\underset{i}{\oplus}} R]$$

$\Leftrightarrow M \cong R/I$ for a right ideal $I \leq R_R$

$$[(\Leftarrow): R_{/\ker \varphi} \cong M, (\Leftarrow): R \xrightarrow{\cong} R/I, r \mapsto r+I \text{ is an epi}]$$

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

Example: •) 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, $R = \text{Md}(k)$, $V = k^{1 \times d}$ (row vectors) with R , acting on the right. V is simple: for any $0 \neq v, w \in V. \exists A \in \text{Md}(k)$ s.t. $vA = w$. So $vR = V \quad \forall v \in V \setminus \{0\}$.

Proposition 2.1: For $M \in \text{Mod-}R$, TFAE:

(a) M is simple.

(b) $M \neq 0$ and $\forall m \in M \setminus \{0\}. M = mR$. In particular: M is cyclic.

(c) $M \cong R/I$ for a maximal right ideal.

Proof: (a) \Rightarrow (b): $M \neq 0$ by definition of a simple ring.

Let $0 \neq m \in M$, $0 \neq mR \leq M_R \Rightarrow mR = M$.

(b) \Rightarrow (c): Let $0 \neq m \in M$. Let $\varphi: R_R \rightarrowtail M_R$, $r \mapsto mr$.

$I := \ker(I) =: \text{ann}(m)$... 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 . ~~why?~~

$$\text{!! } I + xR / I \leq R / I \quad f(x)R = \underbrace{m_x R}_{\not\subseteq R} !$$

(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. \blacksquare

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.

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. \blacksquare

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

Recall: A field k is algebraically closed 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 $D=k$.

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.
 $\dim_k k(a) \leq \dim_k D < \infty \xrightarrow{k \text{ alg. closed}} k(a) = k \Rightarrow a \in k$.

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 $\text{End}(M_R) = k$ (canonically).

Proof: $k \hookrightarrow \text{End}(M)$ via scalar mult.: $\lambda \in k \mapsto (m \mapsto \lambda m)$
 $\text{End}(M_R) \subseteq \text{End}(M_k) \cong M_d(k)$ For $d = \dim_k(M)$, so $\text{End}(M_R)$ is a fin.-dim. k -algebra and a division ring (L1.2).
 $\xrightarrow[k \text{ alg. closed}]{} \text{End}(M_R) = k$. □

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

2.2. Composition series

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

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

s.t. M_i/M_{i-1} is simple for $1 \leq i \leq n$.

We call n the **length** of the chain.

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

$$\Omega = \underbrace{\mathbb{Z}/12\mathbb{Z}}_{\mathbb{Z}/2\mathbb{Z}} \subsetneq \underbrace{\mathbb{Z}/6\mathbb{Z}}_{\mathbb{Z}/3\mathbb{Z}} \subsetneq \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\mathbb{Z}/12\mathbb{Z}} \subsetneq \mathbb{Z}/12\mathbb{Z}$$

• \mathbb{Z}/\mathbb{Z} does not have a composition series
(between $n\mathbb{Z} \not\equiv \Omega$, we can always insert $m\mathbb{Z}$, $m \geq 1$) $\frac{n\mathbb{Z}}{0}$ simple

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

$$(A \cap B)$$

Proof: (2): $B \subseteq A \cap (B+C)$ and $(A \cap C) \subseteq A \cap (B+C)$ ✓

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

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

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

One of the
isomorphism
theorems.

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

$$\begin{array}{ccccc} & & A+B & & \\ & \diagdown & & \diagup & \\ A & & & & B \\ & \diagup & & \diagdown & \\ & A \cap B & & & \end{array}$$

Lemma 2.6 [Zassenhaus]: 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:

$$\begin{array}{ccccc} & A & & B & \\ & | & & | & \\ & A' + (A \cap B) & & B' + (A \cap B) & \\ & \neq & & & \\ & A' + (A \cap B') & & B' + (A' \cap B) & \\ & | & & | & \\ & A' & & B' & \\ & \diagdown & & \diagup & \\ & A \cap B & & B \cap A & \\ & \diagup & & \diagdown & \\ & (A' \cap B) \cap (B' \cap A) & & & \end{array}$$

Note: •) $\cancel{A' + (A \cap B')} + (A \cap B) = A' + (A \cap B)$
•) $(A \cap B) \cap (A' + (A \cap B')) \stackrel{\text{L2.5}}{=} \cancel{(A \cap B \cap A')} + (A \cap B')$

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

$$\Rightarrow \frac{A' + (A \cap B)}{A' + (A \cap B')} \stackrel{\text{from above}}{\cong} \frac{A \cap B}{(B \cap A') + (A \cap B')} \stackrel{\text{symmetry}}{\cong} \frac{B' + (A \cap B)}{B' + (A' \cap B)} \quad \square$$

Definition: Two chains of submodules $\underline{Q} = A_0 \leq A_1 \leq \dots \leq A_m = M$, $\underline{Q}' = B_0 \leq B_1 \leq \dots \leq B_n = M$ are equivalent (or isomorphic) if $m=n$ and there is a permutation $\sigma: [n] \rightarrow [m]$ 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 $\underline{Q} = A_0 \leq A_1 \leq \dots \leq A_m = M$, $\underline{Q}' = B_0 \leq B_1 \leq \dots \leq B_n = M$ have equivalent refinements.

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

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

$$A_i = A_{i,n} \geq A_{i,n-1} \geq \dots \geq A_{i,1} \geq A_{i,0} = A_{i-1}$$

$$B_j = B_{j,m} \geq B_{j,m-1} \geq \dots \geq B_{j,1} \geq B_{j,0} = B_{j-1}$$

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

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

\Rightarrow The refinements are equivalent. \square

October 16, 2025

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

Proof: Let $\underline{Q} = A_0 \leq A_1 \leq \cdots \leq A_m$, $\underline{Q} = B_0 \leq B_1 \leq \cdots \leq B_n = M$ 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. \square

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 $\underline{Q} = A_1 \leq A_2 \leq \cdots \leq A_n = M$ be a composition series. If $B_1 \leq B_2 \leq \cdots \leq B_{m-1}$ 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 : $A_0 := \underline{Q}$.

Suppose we have $A_0 \leq A_1 \leq \cdots \leq A_{i-1}$ 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 $\Omega = \{A \subseteq M_R : A_{i-1} \leq A\}$ 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. \square

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 $\forall i \in I$.

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

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.

•) $\underline{\Omega}$ 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, $M_n(D) = S_1 \oplus \dots \oplus S_n$ with $S_i = \{ \text{matrices where all entries outside the } i\text{-th row are zero} \}$.
 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. $M = N \oplus \bigoplus_{i \in I \setminus I'} M_i$.

Proof: Let $\Omega := \{J \subseteq I \mid N + \sum_{j \in J} M_j \text{ is direct}\}$. 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 $J \in \Omega' \setminus J'$.] Zorn's lemma $\Rightarrow \Omega$ has a maximal element I'

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

$\forall i \in I. M_i \cap (N + M') \in \{\emptyset, M_i\}$ by simplicity.

But $M_i \cap (N + M') = \emptyset$ $\Leftrightarrow I'$ 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 $\emptyset \neq M \in \text{Mod-}R$. 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 $N \leq M'$!).

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.

$\underset{2.10}{\Rightarrow} \exists I' \subseteq I. M = N \oplus \bigoplus_{i \in I'} M_i$. 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. \square

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]. \square

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

(2) Endomorphism Rings: Suppose $M_R \cong M_1 \oplus \dots \oplus M_k$. Let $\varepsilon_i : M_i \rightarrow M$ be the canonical embedding, $\pi_i : M \rightarrow M_i$ the canonical projection, so $m = \sum_{i=1}^k \varepsilon_i(\pi_i(m)) \quad \forall m \in M$. If $f \in \text{End}(M_R)$, then $f(m) = \sum_{i,j=1}^k \varepsilon_i \circ \pi_i \circ f \circ \varepsilon_j \circ \pi_j(m) \stackrel{\text{def}}{=} t_{ij}$

with $\ell_{i,j} : M_j \rightarrow M_i$.

Then $\text{End}(M_R) \xrightarrow{\text{(*)}} \bigoplus_{i,j=1}^k \text{Hom}(M_j, M_i)$, $\varphi \mapsto [\ell_{ij}]_{i,j=1}^k$ (1)

is an isomorphism of abelian groups.

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

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

so considering the RHS to be formal matrices, (1) is a ring isomorphism.

Proposition 2.14: Let M_R be semisimple of finite length, say $M \cong M_1^{n_1} \oplus \cdots \oplus M_k^{n_k}$ with M_i simple, $M_i \neq M_j$ for $i \neq j$. Then $\text{End}(M) \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ with $D_i = \text{End}(M_i)$ division rings. ^{module} ^{matrix ring $M_{n_i}(D_i)$}

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

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

$$\xrightarrow{\text{(*)}} \bigoplus_{i=1}^k M_{n_i}(\text{End}(M_i))$$

$\text{End}(M_i)$ is a division 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 $\Leftrightarrow \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \times \dots \times \mathbb{Z}/p_r\mathbb{Z}$,
 p_i pairwise distinct

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

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

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

(1) The SES is **split exact** if

$$\exists f': N \rightarrow M. f' \circ f = \operatorname{id}_M$$

$$\Leftrightarrow \exists g': K \rightarrow N. g \circ g' = \operatorname{id}_K$$

$$\Leftrightarrow \exists \varphi: N \rightarrow M \oplus K \text{ s.t.}$$

$$0 \rightarrow M \rightarrow N \rightarrow K \rightarrow 0$$
$$\downarrow \operatorname{id}_M \quad \downarrow \varphi \quad \downarrow \operatorname{id}_K \quad \text{commutes}$$

$$0 \rightarrow M \rightarrow M \oplus K \rightarrow K \rightarrow 0$$

$$m \mapsto (m, 0)$$

$$(m, k) \mapsto k$$

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

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

Theorem 2.15: Let $R \in \text{Rng}$. TFAE:

- (a) R is right semisimple.
- (b) All SES in $\text{Mod-}R$ split.
- (c) All $M \in \text{Mod-}R$ are semisimple.
- (d) All f.g. $M \in \text{Mod-}R$ are semisimple.
- (e) All cyclic $M \in \text{Mod-}R$ are semisimple.

Proof: (b) \Rightarrow (c): Let $N \leq M$. Then $0 \rightarrow N \rightarrow M \rightarrow M/N$ is split exact by (b), so $M = N \oplus K$ with $K \cong M/N$. $\xrightarrow{\text{T.2.12(c)}}$ 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 $0 \rightarrow M \xrightarrow{f} N \xrightarrow{g} K \rightarrow 0$ be exact.
 N semisimple $\Rightarrow N = f(M) \oplus K'$ with $K' \leq N$ [T 2.12]
Define $f': N \rightarrow M$ by $N \xrightarrow{\text{proj.}} f(M) \xrightarrow{f^{-1}} M$. Then $f \circ f' = \text{id}_M$. \blacksquare

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 $M_i \in \text{Mod-}R$.
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. $1 \in \bigoplus_{i \in I_0} M_i \Rightarrow R_R = \bigoplus_{i \in I_0} M_i$. \blacksquare

Remark: Similarly, if M_R is semisimple:

M_R f.g. $\Leftrightarrow M \cong M_1 \oplus \cdots \oplus M_n$, M_i simple $\Leftrightarrow l(M) < \infty$.

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 (c) both follow from T2.15 (b) \blacksquare

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 $D_i \cong \text{End}(S_i)$.

C2.16

[October 23, 2025]

Proof: Existence: $R_R = S_1^{\oplus n_1} \oplus \cdots \oplus S_k^{\oplus n_k}$ with simple S_i , $S_i \neq S_j$ if $i \neq j$.
 $\Phi: R \rightarrow \text{End}(R_R)$, $r \mapsto \Phi_r$, $\Phi_r(x) = rx$ is a ring hom
 $\xrightarrow{\text{P2.14}} R \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ with $D_i \cong \text{End}(S_i)$.

Uniqueness of simple modules: $S \in \text{Mod-}R$ simple
 $\Rightarrow \exists \text{ epi } f: S_1^{\oplus n_1} \oplus \cdots \oplus S_k^{\oplus n_k} \longrightarrow S$
 $\Rightarrow S$ 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, $m_i \geq 1 \Rightarrow M_{m_i}(E_i) \cong V_i^{\oplus n_i}$ with V_i simple in $\text{Mod-}M_{m_i}(E_i)$.
 $\Rightarrow V_1, \dots, V_e$ are nonisomorphic simple R -modules
 $[\text{with } V_i M_{m_j}(E_j) = 0 \quad \forall i \neq j]$

$$\Rightarrow R_R = V_1^{m_1} \oplus \cdots \oplus V_e^{m_e}$$

Uniqueness of composition series (after renumbering):

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

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



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

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

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

Definition: A ring R is simple if $R \neq 0$ 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, $\text{char } k = 0$, is simple (exercise)

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

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

Proposition: If R is a ring s.t. $R = R_1 \times \cdots \times R_k = R'_1 \times \cdots \times R'_e$ with R_i, R'_j simple $\Rightarrow k = l$, $R_i = R'_i$ after renumbering ($=$, not just \cong).

Proof: $R_i, R'_j \trianglelefteq R$ and $R_i R = R_i, R'_j R = R'_j$
 $R_i = (R_i R'_1) \times \cdots \times (R_i R'_e) \Rightarrow R_i R'_j \subseteq \{0, R'_j\}$ 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 $R_i R'_j \subseteq R'_j \Rightarrow R_i R'_j = R'_j \Rightarrow R_i = R'_j$



2.5. Simple artinian rings

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

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

(Note: $\text{ann}(R) \leq R$).

(2) M is **Faithful** if $\text{ann}(M) = 0$, otherwise **unfaithful**.

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

[Suppose R is commutative: M_R simple module $\Rightarrow M_R \cong R/I$,
 I maximal ideal of $R \Rightarrow \text{ann}(M) = I$.

If R is (right) primitive $\Rightarrow 0$ is the annihilator of some (R/I) ,
 $I \triangleleft R$ maximal $\Rightarrow 0$ max. ideal of $R \Rightarrow 0, R$ are the only ideals
of R ($\Rightarrow R$ 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 $\Omega = \{\Omega \neq I_R \trianglelefteq R_2\} \neq \emptyset$

By right artinianity, Ω has a minimal element.

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

Then $1 \notin \text{ann}(I_R) \leq R \Rightarrow \text{ann}(I_R) = 0 \Rightarrow I_R$ faithful, simple
 trick For every $r \in R$, $\ell_r: I_R \rightarrow rI_R$, $x \mapsto rx$ has $\ker \ell_r \subseteq \{0, I_R\}$
 $\Rightarrow rI_R$ 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

(c) \Rightarrow (d): Let $M_R \in \text{Mod-}R$ be faithful, simple.

Consider $\mathcal{F} = \{f: R_R \rightarrow M_R^n \mid n \geq 0, f \text{ R-hom}\}$. 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.

Claim: $\ker f = 0$

Suppose not. Let $0 \neq r \in \ker f \cdot \text{ann}(M) = 0 \Rightarrow \exists m \in R, mr \neq 0$.

Define $\tilde{f}: R \rightarrow M^n \otimes M$ $\Rightarrow \ker \tilde{f} \subsetneq \ker f$ $\xrightarrow{\text{contradiction}}$ minimality

$x \mapsto (f(x), mx)$

$\xrightarrow{\text{c.u.}} f: R_R \hookrightarrow M_R^n$, M_R^n semisimple $\xrightarrow{T2.12} M_R^n \cong R_R \oplus K_R$
 $\xrightarrow{\text{c.u.}} R_R$ semisimple, $R_R \cong M_R^m$ for some $m \leq n$.

(d) \Rightarrow (e): [T 2.18]

(e) \Rightarrow (a): ✓ (exercises, fin.dim \Rightarrow artinian) □

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

right artinian } \Rightarrow left art
 right primitive } \Rightarrow left primitive

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

2) R simple artinian $\Leftrightarrow R$ simple right artinian $\Leftrightarrow R$ simple left artinian

\Downarrow \Uparrow
 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. $\varrho: G \rightarrow GL(V)$ with V a K -vector space. If $\dim V = n < \infty$, $GL(V) \cong GL_n(K)$ (non-canonically, by choosing a basis).

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

If $\varrho: G \rightarrow GL(V)$, $\sigma: G \rightarrow GL(W)$ are representations, a homomorphism is a K -linear $T: V \rightarrow W$ s.t. $T(\varrho(g)v) = \sigma(g)Tv$.
= 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. $\ell: K[G] \rightarrow \text{End}(M_K)$.

" \hookleftarrow ": A $K[G]$ module M is a K -vector space ($\ell|_K$)

" \hookrightarrow ": A repr. $\varrho: G \rightarrow GL(V_K)$ gives rise to a monoid hom

$$\ell: (G, \cdot) \longrightarrow (\text{End}(V_K), \circ).$$

\cong ring

Using the VP of $K[G]$, this extends to a K -alg hom.

$$\tilde{\varrho}: K[G] \rightarrow \text{End}(V_K).$$

□

The irred. repr. \cong simple modules

completely reducible repr \cong semisimple modules,

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

Proof: (\Leftarrow): Let $I_{K[G]} \leq K[G]$ be a right ideal.

We show: the SES $0 \rightarrow I \hookrightarrow K[G] \xrightarrow{\pi} \overbrace{K[G]/I}^{\cong V} \rightarrow 0$ of $K[G]$ -module splits [T 2.12(c)].

Since it splits as a SES of K -vector spaces

$\exists \ell \in \text{Hom}(V_K, K[G]_K)$ s.t. $\pi \circ \ell = \text{id}_V$.

$\text{char } K \nmid |G| \Rightarrow |G| \in K^\times$

Define: $\tilde{\ell}(v) := \frac{1}{|G|} \sum_{g \in G} \ell(vg) g^{-1}$.

$\tilde{\ell}$ is a $K[G]$ -hom: K -linear \checkmark

$$\tilde{\ell}(vg) = \frac{1}{|G|} \sum_{g \in G} \ell(vkg)^{-1} g = \frac{1}{|G|} \sum_{g \in G} \ell(vg) g^{-1} k$$

$v \in V$ $g \in G$
 $g' := hg \Rightarrow g = h^{-1}g' \Rightarrow g^{-1} = (g')^{-1}k$

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

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

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

We show: $I \cap J \neq 0$ for any nonzero right ideal $J \trianglelefteq K[G]$

Then $0 \rightarrow I \hookrightarrow K[G] \xrightarrow{\varepsilon} K \rightarrow 0$ 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 $s := \sum_{g \in G} g \Rightarrow \varepsilon(s) = |G| \cdot 1_K = 0_K \Rightarrow s \in I$

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



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

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

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

Let $f: K \rightarrow K[G]$ s.t. $\varepsilon \circ f = \text{id}_K$, f $K[G]$ -hom.

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

Let $h \in G$ s.t. $a_h \neq 0$

$K[G]$ -module structure on K : $\forall g \in G \exists \lambda_g \in K. 1_K \cdot g = \lambda_g$

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

$\Rightarrow \forall g \in G. hg \text{ appears in support of } f \Leftrightarrow \text{only finitely many } a_g \neq 0$ \blacksquare

3. Jacobson Radical

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

This is a right ideal.

$$\text{ann}(M) := \text{ann}(\{m\}), \quad \text{ann } X = \bigcap_{x \in X} \text{ann}(x)$$

If $X_R \subseteq M_R$, then $\text{ann}(X_R) \trianglelefteq R$.

Definition: $I \trianglelefteq R$ is right primitive if $I = \text{ann}(M_R)$, $M \in \text{Mod-}R$ simple.

[$\Leftrightarrow R/I$ is a right primitive ring]

Example: $\cdot) I \trianglelefteq R$ maximal $\Rightarrow I$ (right) primitive

[By Zorn's lemma, I is contained in a maximal right ideal $J \Rightarrow (R/J)_R$ simple, $\text{ann}(R/J) \supseteq I$ [$RI = J$]
 $\Rightarrow \text{ann}(R/J) = I$]

$\cdot) \text{If } R \text{ commutative: } I \text{ primitive} \Leftrightarrow I \text{ maximal}$

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

Definition: The Jacobson radical of R is

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

$$J(R) = J(R) = \text{rad } R$$

Note: $J(R) \triangleq R$ and $J(R) \subseteq R$ unless $R \neq 0$.

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

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

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 $\overset{r \in J(R)}{\Rightarrow} (1+J)r = r + J = 0 + J$
 $\Rightarrow r \in J$.

($B \subseteq C$): \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 .
 $\Rightarrow \exists m \in M. mr \neq 0 \overset{M \text{ simple}}{\Rightarrow} M = mrR \Rightarrow \exists x \in R. m = mrx$
 $\Rightarrow m(1-rx) = 0 \Rightarrow m = 0$ ↴
↑
 $1-rx$ right invertible

($C = D$): $D \subseteq C \vee$

C ⊆ D: Let $r \in J(R)$, $x, y \in R$.

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

$xr \in J(R) \stackrel{C}{\subseteq} \exists z \in R : (1 - \underbrace{xyz}_{\in J(R)})z = 1 \Rightarrow z$ is left invertible

$z = 1 - (-xyz) \stackrel{C=A}{\Rightarrow} z$ is right invertible

$\Rightarrow z \in R^\times \Rightarrow 1 - xy \in R^\times$ □

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 $\Rightarrow J\left(\prod_{i \in I} R_i\right) = \prod_{i \in I} J(R_i)$

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

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

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

October 30, 2025

Definition: R is semiprimitive/Jacobson semisimple/ J -semisimple if $J(R)$.

Lemma 3.3: If $I \trianglelefteq R$, $I \subseteq J(R)$, then $J(R/I) = J(R)/I$.

In particular $J(R/J(R)) = \{0\}$.

Proof: Clear, using $J(R) = \bigcap \{\bar{I} \mid \bar{I} \trianglelefteq_R \text{ maximal}\}$ □

Proposition 3.4: 1) R and $R/J(R)$ have the same simple modules.
2) $r \in R$ is [right] invertible ($\Rightarrow r + J(R) \in \overline{R} := R/J(R)$ is [right] invertible).

Recall: If $I \triangleleft R$, there is a bijection

$$\{M \in \text{Mod-}R \mid I \subseteq \text{ann}(M)\} \longleftrightarrow \text{Mod-}^R/I$$

" \mapsto ": $m(R+I) := mr$ (works because $MI=0$)

" \leftarrow ": $mr := m(r+I)$

Respects submodules, morphisms, etc. (category isomorphism)

Proof: (1) By the remark on $\text{Mod-}^R/I$ & definition of $J(R)$.

2) (\Leftarrow): \checkmark

(\Leftarrow): $r + J(R)$ right invertible

$$\Rightarrow \exists s \in R. 1 + J(R) = (r + J(R))(s + J(R)) = rs + J(R)$$

$$\Rightarrow \exists x \in J(R). 1 - rs - x \Leftrightarrow rs = 1 + x \stackrel{\text{L3.1}}{=} \exists y. r(sy) = 1.$$

$$\stackrel{\text{L3.1}}{=} \exists y. r(sy) = 1.$$

3.1 Nil and Nilpotent Ideals

Definition: A right ideal $I \subseteq R$ is:

• **nilpotent** if $\exists n \geq 0. I^n = 0$ ($\forall a_1, \dots, a_n \in I. a_1 \cdots a_n = 0$).

• **nil** if every element of I is nilpotent [$\forall a \in I. \exists n \geq 0. a^n = 0$].

Nilpotent \Rightarrow nil, but

Example: In $\mathbb{Z}[x_1, x_2, \dots]/(x_1, x_2^2, x_3^3, \dots)$, $I = (\bar{x}_1, \bar{x}_2, \bar{x}_3, \dots)$ is nil, but not nilpotent.

Δ a, b nilpotent $\not\Rightarrow a+b$ nilpotent

$$\text{E.g. } M_2(\mathbb{K}): \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Remark: Easy to prove: $I, J \triangleleft R$ nilpotent $\Rightarrow I+J$ nilpotent

Open Conjecture (Köthe Conjecture): $I, J \triangleleft R$ nil $\Rightarrow I+J$ nil.

Lemma 3.5: If $I \trianglelefteq R_R$ is nil, then $I \subseteq J(R)$.

Proof: Let $x \in I \Rightarrow \forall r \in R. xr$ nilpotent, say $(xr)^n = 0$
 $\Rightarrow (1-xr)(1+xr + (xr)^2 + \dots + (xr)^{n-1}) = 1 - (xr)^n = 1$
 $\Rightarrow 1-xr$ is (right) invertible $\Rightarrow x \in J(R)$.

⚠ Not every nilpotent element is contained in $J(R)$.
E.g. $R = M_n(D)$, D div. ring $\Rightarrow J(R) = 0$, but there
are nilpotent matrices!

Theorem: If R is right artinian, $J(R)$ is nilpotent.
In particular: 1) $J(R)$ is the largest nilpotent right [left] ideal.
2) If $I \trianglelefteq R_R$ is nil, then I is nilpotent.

Proof: Suffices to show $J(R)$ nilpotent, then L3.5 gives (1) and (2)
The chain: $J(R) \supseteq J(R)^2 \supseteq J(R)^3 \supseteq \dots$ stabilizes
 $\Rightarrow \exists I \trianglelefteq R. I = J(R)^k$ for sufficiently large k . Note: $I^2 = I$

Claim: $I = 0$

Suppose $I \neq 0$. Let $A \trianglelefteq R_R$ be a right ideal minimal with
the property $AI \neq 0$ (exists, because R is right artinian).

Let $x \in A$ s.t. $xI \neq 0$.

$$\Rightarrow xI \cdot I = xI^2 = xI \underset{xI \subseteq A}{\neq} 0 \Rightarrow A = xI$$

$$\Rightarrow x = xy \text{ with } y \in I \underset{\substack{\in \\ J(R)}}{\Rightarrow} x(\underbrace{1-y}_{\in R^x}) = 0 \Rightarrow x = 0 \quad \blacksquare$$

3.2. Semisimple rings again

Lemma 3.7: A right ideal $I \trianglelefteq R_R$ is a direct summand of R_R
 $\Leftrightarrow I = eR$ with e idempotent.

Proof: (\Leftarrow): $\forall r \in R$. $r = er + (1-e)r$, so $R_R = eR + (1-e)R$

If $r \in R \setminus (1-e)R$, then $r = ex = (1-e)y$ ($x, y \in R$)

$$\Rightarrow er = e(ex) = ex = r, \text{ so } r = er = e(1-e)y = (e - e^2)y = 0$$

(\Rightarrow): Suppose $R_R = I_R \oplus J_R \Rightarrow 1 = e + \underbrace{(1-e)}_{\substack{\uparrow \\ \in J}} \text{ with } e \in [1 - ee]$

$$\Rightarrow e(1-e) = (1-e)e \in I \cap J = 0 \Rightarrow e(1-e) = 0 = (e-1)e = 0$$

$$\Rightarrow e = e^2$$

Finally: $\forall x \in I$. $x = ex + (1-e)x \Rightarrow x = ex$, so $I = eR$ □

Theorem 3.8: TFAE for a ring:

(a) R is semisimple

(b) R is semiprimitive ($J(R) = 0$) and right artinian.

(c) R is semiprimitive and satisfies the DCC on principal right ideals

Proof: (a) \Rightarrow (b): R_R has finite length, so it is right artinian.

$\exists I \subseteq R_R$. $R_R = J(R)_R \oplus I_R$ [T2.12 (c)] If $J(R) \neq 0$, then $I \subsetneq R$

\Rightarrow there exists a maximal right ideal $I \subseteq M \subsetneq R$

$\Rightarrow J(R) \subseteq M$. ↳

(b) \Rightarrow (c): \checkmark

(c) \Rightarrow (a): Note: (1) Every $0 \neq I \subseteq R_R$ contains a minimal nonzero right ideal [Take a minimal element of $\{xR \mid x \in I, xR \neq 0\}$ by DCC].

(2) Every minimal $0 \neq I \subseteq R_R$ is a direct summand of R_R .

[$I \neq 0$, but $J(R) = 0 \Rightarrow \exists$ maximal right ideal $M \subseteq R_R$ s.t.

$I \nsubseteq M \Rightarrow I + M = R$. Since I is simple, $I \cap M = 0$].

We now find $0 \neq A_1, \dots, A_n$ minimal right ideals s.t.

$R_R = A_1 \oplus \dots \oplus A_n$. Suppose A_1, \dots, A_{n-1} ($n \geq 1$) have been constructed s.t. $R_R = A_1 \oplus \dots \oplus A_{n-1} \oplus B_n$, $B_n \in R_R$. We can assume $B_n \neq 0$. Let $0 \neq A_n \subseteq B_n$ be minimal (by 1). Then $R_R = A_n \oplus C_n$ for some C_n (by 2) and

$$B_n = A_n \oplus \underline{(B_n \setminus C_n)} \quad (\text{because } A_n \subseteq B_n)$$

$$=: B_{n+1} \subsetneq B_n$$

This gives us A_n . Note $B_1 \supseteq B_2 \supseteq \dots$ is a chain of principal right ideals [L3.7], so by DCC it stabilizes. But this only happens when $B_n = 0$. □

Corollary 3.9: If R is right artinian (e.g. R is a f.d.-algebra over a field) then R semisimple $\Leftrightarrow J(R) = 0$.

Corollary 3.10: R right artinian $\Rightarrow R/J(R)$ semisimple and $J(R)$ nilpotent.

Strategy: Consider $\frac{J(R)^i}{J(R)^{i+1}}$ for $i=0,1,\dots$

Definition: R is **semiprimary** if $R/J(R)$ is semisimple and $J(R)$ is nilpotent.

So: right [left] artinian \Rightarrow semiprimary

Theorem [Hopkins-Levitzki]: If R is semiprimary and $M \in \text{Mod-}R$ TFAE:

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

Proof: (c) \Rightarrow (a), (b) by L2.9.

(a), (b) \Rightarrow (c): Let $n \geq 0$ s.t. $J(R)^n = 0$, $\bar{R} := R/J(R)$.

Consider $M \cong MJ(R) \cong MJ(R)^2 \cong \dots \cong MJ(R)^n = 0$.

It suffices to show $MJ(R)^i/MJ(R)^{i+1}$ has a composition series ($i=0, \dots, n-1$).

Now $\frac{MJ(R)^i}{MJ(R)^{i+1}}$ is a module over the semisimple \bar{R} , hence a direct sum of simple \bar{R} -modules. Since M is noetherian or artinian, so is $\frac{MJ(R)^i}{MJ(R)^{i+1}}$, so the direct sum is finite. Thus $MJ(R)^i/MJ(R)^{i+1}$ has a composition series as an \bar{R} -module, which is also a composition series as an R -module. □

Corollary 3.12: R right artinian $\Leftrightarrow R$ right noetherian and semiprimary

Proof: (\Leftarrow): By T3.11, R_R is right artinian.

(\Leftarrow): R right artinian $\Rightarrow R$ semiprimary L3.10

$\stackrel{3.11}{\Rightarrow} R_R$ is noetherian

In particular: R right artinian $\Rightarrow R$ right noetherian

Corollary 3.13: If R_R is right artinian and $M\text{-Mod-}R$ is finitely generated, then $l(M) < \infty$.

3.3 Nakayama's Lemma

Lemma 3.14 [Nakayama]: If $M \in \text{Mod-}R$ is f.g. and $M = MJ(R)$, then $M = 0$.

Proof: Let $M = \langle m_1, \dots, m_k \rangle_R$ with k minimal. If $k \geq 1$, we can write $m_k = m_1r_1 + \dots + m_{k-1}r_{k-1}$ with $r_i \in J(R)$.

$$\Rightarrow m_k(1-r_k) = m_1r_1 + \dots + m_{k-1}r_{k-1}$$

$$\Rightarrow m_k(1-r_k) \in \langle m_1, \dots, m_{k-1} \rangle_R$$

Since $1-r_k \in R^\times$, also $m_k \notin \langle m_1, \dots, m_{k-1} \rangle_R$ $\hookrightarrow k \text{ min.}$ \square

Corollary: If $M \in \text{Mod-}R$, $N \leq M_R$ s.t. M/N is f.g. and $M = N + J(R)$, then $M = N$.

Proof: Apply 3.14 to M/N .

Application: Let $M \in \text{Mod-}R$, then $\bar{M} = M/MJ(R)$ is annihilated by $J(R)$, so naturally an $\bar{R} := R/J(R)$ -module.

Corollary 3.16: If M is f.g. and $\{x_i\}_{i \in I}$ is a family in M s.t. $\{\bar{x}_i\}_{i \in I}$ generate \bar{M} (over \bar{R}), then $\{x_i\}_{i \in I}$ generates M .

Proof: Apply C1.15 to $N := \langle x_i \mid i \in I \rangle_R$.

If $f: M \rightarrow M'$ is an R -hom, then $f(M(J(R))) \subseteq M'J(R)$, so it induces $\bar{f}: \bar{M} \xrightarrow{f} \bar{M}' \quad (\text{Mod-}\bar{R})$

$$\begin{array}{ccc} & & \\ | & & | \\ \bar{M} & \xrightarrow{\bar{f}} & \bar{M}' \\ & & \end{array} \quad (\text{Mod-}\bar{R})$$

Corollary 3.17: If $M' \in \text{Mod-}R$ is f.g. and $f: M \rightarrow M'$ is s.t. $\bar{f}: \bar{M} \rightarrow \bar{M}'$ is surjective, then $f: M \rightarrow M'$ is surjective.

Proof: $\bar{f}(\bar{M}) = \bar{M}' \Rightarrow M' = f(M) + M'J(R) \Rightarrow M' = f(M)$ \square

3.4. Group Algebras (w/o proof)

K field. If G is infinite, then $K[G]$ is not semisimple [P2.24].

Theorem 3.18 [Amitsur]: Let K be a non-algebraic field extension of \mathbb{Q} . Then $K[G]$ is semiprimitive for any group. ($K = \mathbb{C}$... Rickart 1950; full theorem by Amitsur 1959).

For a proof: [Lam 01, (6.12)]

For fields of algebraic numbers (e.g. $K = \mathbb{Q}$), this is still open.

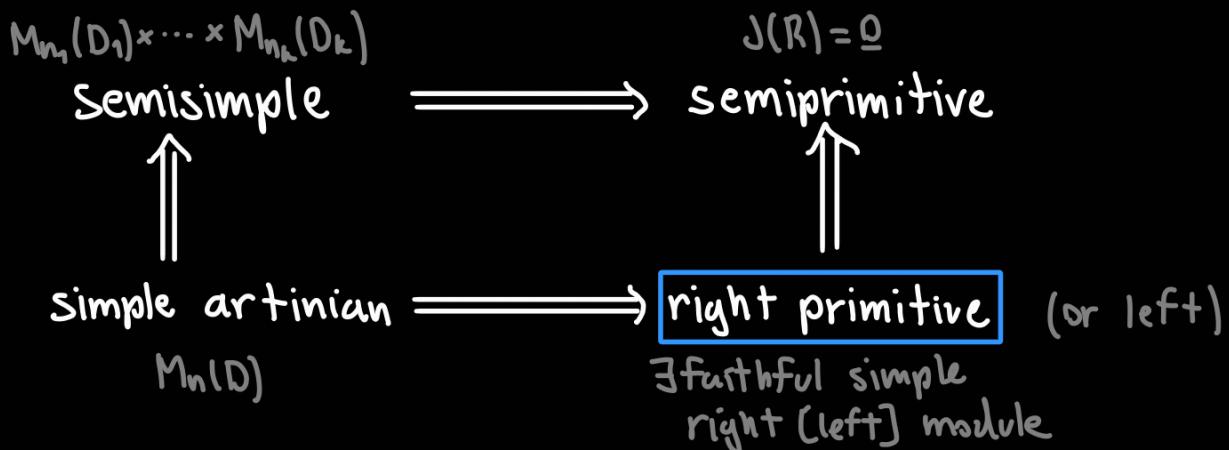
Difficult problems on group algebras (Kaplansky's conjectures, 50s): If G is torsion free:

- $K[G]$ is a domain (zero divisor conjecture) → open
- $K[G]$ does not contain non-trivial idempotents (idempotent conjecture) — open
- $K[G]$ contains only trivial units [$K[G]^{\times} = K^{\times}G$] (unit conjecture) — false

Gardam 2021: counterexample $K = \mathbb{F}_2$

2023: same counterexample with char $K = 0$

4. Structure of Primitive rings & Jacobson Density Theorem



Note: Semisimple, semiprimitive, simple artinian are left/right symmetric.

• left primitive \Leftrightarrow right primitive [Bergman 1964]

For any ring R , $R/J(R)$ is semi primitive.

Proposition 4.1: Every semi primitive ring R is a subdirect product of right primitive rings, i.e. $R \hookrightarrow \prod_{i \in I} R_i$ injective with R_i right primitive, and all projections $R \rightarrow R_i$ surjective

Proof: $\underline{Q} = J(R) = \bigcap_{\substack{M \in \text{Mod-}R \\ M \text{ simple}}} \text{ann}(M_R)$

$\Rightarrow R \hookrightarrow \prod_{\substack{M_R \text{ simple}}} R / \underbrace{\text{ann}(M)}_{\text{right primitive}}$, and $R \rightarrow R / \text{ann}(R)$ is surjective \blacksquare

Sometimes (rarely) a useful strategy: prove something for right primitive rings, lift it to subdirect products (\rightarrow semisimple rings), then modulo the Jacobson radical (\rightarrow arbitrary rings; usually hard or impossible).

M_R f.g., $M \Delta(R) = M \Rightarrow M = 0$

November 6, 2025

Example: $\mathbb{Z} \subseteq \mathbb{Q}_{\mathbb{Z}}$ $\mathbb{Q} = n\mathbb{Q} \quad \forall n \neq 0$

$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \mid p \nmid ab \right\}$ (p prime) ring (localization)

unique maximal ideal: $p\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid p \nmid b, p \mid a \right\}$

$\Rightarrow J(\mathbb{Z}_p) = p\mathbb{Z}_{(p)} \Rightarrow \mathbb{Q}_{\mathbb{Z}_{(p)}} = p\mathbb{Q} \quad \mathbb{Q} \text{ as } \mathbb{Z}_{(p)}\text{-mod}$

satisfies $\mathbb{Q}J(\mathbb{Z}_p) = \mathbb{Q}, \quad \mathbb{Q} \neq 0$

\Rightarrow The f.g. condition in Nakayama's lemma is necessary.

Example [A non-simple left-primitive ring]:

D div. ring, V_D vector space, $R := \text{End}(V_D)$ ($\cong_{\text{column finite}}^{\text{matrices}}$)

Then R acts on V from the left.

RV simple: If $v, w \in V \setminus \{0\}$, $\exists f \in R$. $f(v) = w$ [extend v to basis]

RV is faithful: If $f \in R$ is s.t. $\forall r \in V$. $f(rv) = 0 \Rightarrow f = 0$

So $\text{ann}(RV) = 0$.

$\Rightarrow R$ is left primitive

If $\dim V_D = \infty$, then R is not simple.

$I := \{f \in R \mid \dim(\text{im } f) < \infty\} \subseteq R$ (\cong matrices w. finitely many nonzero rows).

Definition: Let R, S be rings. An (R, S) -bimodule is a set M that is

-) a left R -module
-) a right S -module
-) $\forall r \in R, \forall s \in S, \forall m \in M. (rm)s = r(ms)$.

Examples: •) If R is commutative, every R module is an (R, R) -bimodule.

•) For arbitrary rings R : Let $M \in \text{Mod-}R$, $E := \text{End}(M_R)$. Then M is a left E -module ($\ell \cdot m := \ell(m)$ for $\ell \in E, m \in M$), and $\ell(mr) = \ell(m)r$, so M is an (E, R) -module.

•) If $R\text{-mod}$, $E := \text{End}(RM)$, then $RM_{E^{\text{op}}}$ is an (R, E^{op}) -bimodule: $m \cdot (\ell \circ_{\text{op}} \psi) = (\ell \circ_{\text{op}} \psi)m = (\psi \circ \ell)(m) = \psi(\ell)(m)$
 $\quad \quad \quad + (m \cdot \ell) = (m \cdot \ell) \cdot \psi$

Alternatively, view M as a left R -, left E -module subject to the actions commuting : $\ell(rm) = r\ell(m)$

- ⚠ If $M_R \in \text{Mod-}R$, then $R^{\text{op}}M \in R^{\text{op}}\text{-Mod}$ via $r \cdot m = mr$.
 In general this is not a bimodule structure!
 Suppose $(am)b - a(mb)$ differ i.g., e.g. if $\text{ann}(m) = 0$
 $\begin{matrix} " & " \\ m \cdot ab & mba \end{matrix}$ and $ab \neq ba$

4.1. The Jacobson Density Theorem

Definition: Let M be an (R, S) -bimodule, $E = \text{End}(M_S)$. Then R acts densely on M_S if $\forall f \in E, \forall m_1, \dots, m_k \in M, \exists r \in R, \forall i: r m_i = f(m_i)$.

[Note: $R \rightarrow E$, $r \mapsto (m \mapsto rm)$ is a ring hom.]

Lemma 4.2: If D is a division ring and V is an (R, D) -bimodule, then R acts densely on $V_D \Leftrightarrow \forall$ lin. ind. $(v_1, \dots, v_n) \in V^k$.
 $\forall (v'_1, \dots, v'_n) \in V^*$ $\exists r \in R$. $\forall i$. $r v'_i = v'_i$.

Proof: clear.

Corollary 4.3: If $\dim V_D = n < \infty$, then $\text{End}(V_D) \cong M_n(D)$ is the only subring of $\text{End}(V_D)$ that acts densely.

Proof: Trivially $E := \text{End}(V_0)$ acts densely.

Fix a D -basis (e_1, \dots, e_n) of V .

Suppose $R \subseteq E$ acts densely on V , let $f \in E$.

$$\Rightarrow \exists t \in R \forall 1 \leq i \leq n. t(e_i) = f(e_i) \Rightarrow t = f \in S. \quad \blacksquare$$

Theorem 4.4 [Jacobson Density Theorem/Chevalley-Jacobson Theorem]:

Let R be a ring, R^M a semisimple left R -module,
 $S = \text{End}(R^M)^{\text{op}}$. Then R acts densely on M_S .

A different proof from ours is presented in Bresar's book.

Lemma 4.5: $R^M \in \text{Mod-}R$ semisimple, $S = \text{End}(R^M)^{\text{op}}$,
 $E = \text{End}(M_S)$. Then every R -submodule of M is an
 E -submodule (& conversely).

Proof: E -submodules are R -submodules, because $R \rightarrow E$, $r \mapsto (m \mapsto rm)$
is a ring hom.

Let $RN \subseteq R^M$ be an R -submodule, and RN' s.t. $RM = RN \oplus RN'$ [T2.11(c)]

Define: $\Pi: R^M \rightarrow R^M$ s.t. $\Pi|_N = \text{id}$, $\Pi|_{N'} = 0$ (projection on N along N') $\Rightarrow \Pi \in S$.

E acts on M from the left : $f \cdot m = f(m)$, $E M_S$ is a bimodule

$$\forall f \in E \forall n \in N. f(n) = f(\Pi(n)) = f(n \cdot \Pi) \stackrel{\substack{\uparrow \\ \text{bimodule structure}}}{=} f(n) \cdot \Pi = \Pi(f(n))$$

So $f(N) \subseteq \Pi(M) = N \Rightarrow N$ is an E -submodule. \blacksquare

Proof of Theorem 4.4: $E := \text{End}(M_S)$. Let $f \in E$, $m_1, \dots, m_k \in M$.

Show: $\exists r \in R. \forall i. f(m_i) = r m_i$

$$R^{\tilde{M}} := R^{M^k} \quad (\text{semisimple})$$

matrix ring

$$\tilde{S} := \text{End}(R^{\tilde{M}}) = \text{End}(R^{M^k}) = M_k(\text{End}(R^M)^{\text{op}}) = M_k(S)$$

Define: $\tilde{f}: \tilde{M} \rightarrow \tilde{M}, (x_1, \dots, x_k) \mapsto (f(x_1), \dots, f(x_k))$

Claim: $\tilde{f} \in \text{End}(\tilde{M}_S)$:

Proof of claim: $\tilde{f}(x+y) = \tilde{f}(x) + \tilde{f}(y) \quad (\forall x, y \in \tilde{M})$

Let $x = (x_1, \dots, x_k) \in \tilde{M}$, $s \in (s_{ij})_{1 \leq i, j \leq k} \in \tilde{S}$, $s_{ij} \in S$

$$\Rightarrow (xs)_j = \sum_{i=1}^k x_i s_{ij}$$

$$\begin{aligned}\tilde{f}(xs) &= \tilde{f}\left(\sum_{i=1}^k x_i s_{i1}, \dots, \sum_{i=1}^k x_i s_{ik}\right) \\ &= \left(f\left(\sum_{i=1}^k x_i s_{i1}\right), \dots, f\left(\sum_{i=1}^k x_i s_{ik}\right)\right) \\ &= \left(\sum_{i=1}^k f(x_i) s_{i1}, \dots, \sum_{i=1}^k f(x_i) s_{ik}\right) \\ &= (f(x_1), \dots, f(x_k))s = \tilde{f}(x)s\end{aligned}$$

□ (claim)

Consider $R\tilde{C} := R(m_1, \dots, m_k) \leq_R \tilde{M}$

$\stackrel{\text{def}}{\Rightarrow} R\tilde{C}$ is an $\text{End}(\tilde{M}_S)$ -submodule of $R\tilde{M}$.

$\Rightarrow \tilde{f}(\tilde{C}) \leq \tilde{C} \Rightarrow \tilde{f}(m_1, \dots, m_k) = (f(m_1), \dots, f(m_k)) = r(m_1, \dots, m_k)$

for some $r \in R$. So $f(m_i) = rm_i \quad \forall i$.

■

Corollary 4.6: If additionally M_S is f.g., then $R \rightarrow \text{End}(M_S)$ is surjective.

Proof: Let $M_S = \langle m_1, \dots, m_k \rangle_S$. Let $f \in E := \text{End}(M_S)$.

Let $r \in R$ s.t. $f(m_i) \leq rm_i \quad \forall i$ [T 4.4].

If $m \in M$, then $m = \sum_{i=1}^k m_i s_i$ with $s_i \in S$.

$$\Rightarrow f(m) = f\left(\sum_{i=1}^k m_i s_i\right) = \sum_{i=1}^k f(m_i) s_i = \sum_{i=1}^k (rm_i) s_i \stackrel{(R,S)-\text{bimodule}}{\downarrow} \sum_{i=1}^k r(m_i s_i) = rm \quad \blacksquare$$

Most important case: RM simple $\Rightarrow S=D$ division ring, M_D D -vec. space, and $R \rightarrow \text{End}(M_D)$ maps R into a dense ring of linear operators on a vector space (here $D = \text{End}(RM)^{\text{op}}$).

Theorem [Structure Theorem For Left Primitive Rings]:

Let R be left primitive with faithful simple left R -module V and $D := \text{End}({}_R V)^{\text{op}}$. Then R embeds as a dense ring of linear operators, $R \hookrightarrow \text{End}(V_D)$, on the right D -vector space V . Further:

- (i) If R is left artinian, then $n = \dim V_D < \infty$ and $R \cong M_n(D)$.
- (ii) If R is not left artinian, then $\dim V_D = \infty$. For all $n \geq 1$, there is a subring $R_n \subseteq R$ and a surjective ring hom. $R_n \rightarrow M_n(D)$.

Remark: (i) recovers T2.21(c) \Rightarrow (e) with a different proof.

Proof: Since $\text{ann}({}_R V) = 0$, $R \hookrightarrow \text{End}(V_D)$ via left multiplication, R acts densely by 4.4.

Case 1: $n := \dim V_D < \infty$

Then $R \hookrightarrow \text{End}(V_D)$ is surjective [C4.6], so $R \cong \text{End}(V_D) \cong M_n(D)$. In particular, R is artinian.

Case 2: $\dim V_D = \infty$, choose D -lin. independent v_1, v_2, v_3, \dots

Let $W_n := \langle v_1, \dots, v_n \rangle$, $R_n := \{r \in R \mid rW \subseteq W\}$

$$I_n = \{r \in R \mid rW = 0\}$$

$\Rightarrow R_n \subseteq R$ is a subring, $I_n \subseteq R_n$

$R_n W_n \subseteq W_n \Rightarrow W_n$ is an R_n -module and $I_n = \text{ann}(R_n W)$

$\Rightarrow \varphi_n : R_n \rightarrow \text{End}(W_n) \cong M_n(D)$ is a ring hom. with $\ker \varphi_n = I_n$.

For any $w_1, \dots, w_n \in W_n$, $\exists r \in R$. $r v_i = w_i$ [T4.4]

$\stackrel{r \in R_n}{\Rightarrow} \varphi_n$ surjective

Claim: R is not left artinian

I_n is a left ideal of R

$\exists r \in R : r v_1 = \dots = r v_n = 0, r v_{n+1} \neq 0 \Rightarrow r \in I_n \setminus I_{n+1}$

$\Rightarrow I_1 \supseteq I_2 \supseteq \dots$



Corollary 4.8: R left primitive $\Leftrightarrow R$ isomorphic to a dense subring of linear operators on a right vector space over a division ring

(" \Leftarrow " easy, " \Rightarrow " T 4.7)

4.2. Application: Jacobson's Commutativity Theorem (after Herskin, Bell)

Theorem [Jacobson's Commutativity Theorem]: Let R be a ring. Suppose $\forall x \in R. \exists n = n(x) > 1. x^n = x$. Then R is commutative.

Motivation: In a boolean ring/algebra, always $x^2 = x$.
 $((\mathbb{Z}/2\mathbb{Z})^k \rightarrow X)$ set, $\mathcal{P}(X)$ powerset $X \cdot Y = X \cap Y$
 $X + Y = X \setminus Y \cup Y \setminus X$

Easy: If $x^2 = x \quad \forall x \in R \Rightarrow R$ commutative

$$1 = (-1)^2 = -1 \quad (x+y)^2 = x^2 + xy + yx + y^2 = \underset{x}{\cancel{x}} + \underset{y}{\cancel{y}} = xy$$

$$\Rightarrow XY + YX = 0 \stackrel{-1=1}{\Rightarrow} XY = YX$$

What if $x^3 = x \quad \forall x$?

Note: Every idempotent ($e^2 = e$) is central.

$$\left[\begin{array}{l} \text{Since } 0 = e(1-e) = (1-e)e. \quad \forall r \in R: \\ er(1-e) = (er(1-e))^3 = 0 \Rightarrow er = ere \\ (1-e)re = ((1-e)re)^3 = 0 \Rightarrow re = ere \end{array} \right] = e \in Z(R)$$

$$\cdot (r^2)^2 = r^4 = r^2 \Rightarrow \forall r \in R. \ r^2 \text{ idempotent} \Rightarrow r^2 \in Z(R)$$

$$\cdot 1+r = (1+r)^3 = 1+3r+3r^2+r^3 \Rightarrow 3r = -3r^2 \in \mathbb{Z}(R)$$

$$\cdot (1+r)^2, r^2 \in \mathcal{Z}(R) \rightarrow (1+r)^2 - 1 = r^2 \in \mathcal{Z}(R)$$

$$\Rightarrow r = 3r - 2r \in \mathcal{E}(R)$$

Lemma 4.10: If R is as in T4.9, then $J(R) = 0$.

Proof: Let $x \in J(R)$, $n > 1$ s.t. $x^n = x$.

$$\Rightarrow 0 = x - x^n = (\underbrace{1 - x^{n-1}}_{\in R^\times \text{ (n} \geq 2\text{)}})x \Rightarrow x = 0$$

□

So $R \hookrightarrow \prod_{I \text{ left primitive}}^{R/I}$, each R/I retains the assumption ideal of R

and it satisfies to prove [T4.9] for left primitive R .

Lemma 4.11: If R is as in T4.9, and left primitive, then R is a division ring.

Proof: By [T4.7], $R \hookrightarrow \text{End}(V_D)$ densely with D a division ring. We show $\dim V_D = 1$, then $R \cong \text{End}(D_D) \cong D$.

Suppose $v, w \in V_D$ are D -linearly independent.

$$\stackrel{\text{L4.4}}{\Rightarrow} \exists r \in R. rv = w, rw = 0$$

$$\Rightarrow \forall n \geq 1. r^n v = 0 \quad \downarrow r^{n(r)} = r$$

□

Lemma 4.12 [Herstein]: Let D be a division ring with $\text{char } D = p > 0$.

Suppose $a \in D \setminus Z(D)$ s.t. $a^{p^n} = a$ for some $n \geq 1$.

$$\Rightarrow \exists x \in D, i > 1. a^i \neq a \text{ and } xax^{-1} = a^i.$$

Theorem 4.13 [Wedderburn's "Little" Theorem]: Every finite division ring is a field.

Proofs of 4.12 and 4.13 later.

Proof of T4.9: By L4.10, L4.11, wlog $R = D$ is a division ring. In D , $(2 \cdot 1_D)^n = 2 \cdot 1_D$ for some $n > 1$, so $\text{char } D = p > 0$, p prime.

wlog $\mathbb{F}_p \leq D$ ($\mathbb{F}_p \subseteq Z(D)$ because everything commutes with scalars)

Suppose there exists $a \in D \setminus \mathbb{F}_p$. Then $\mathbb{F}_p[a] \leq D$ is a finite field (since $a^{p^n} - a = 0$) of char $p \Rightarrow \exists n \geq 1. a^{p^n} = a$. [Frobenius]

Let $x \in D$, $i > 1$ s.t. $a^i \neq a$, $xax^{-1} = a^i$ [L4.12]

Let $m > 1$ s.t. $x^m = x$.

Then $R := \mathbb{F}_p \langle a^k x^\ell \mid 0 \leq k \leq p^{n-1}, 0 \leq \ell \leq m \rangle$ is a finite subring of D

$$[(a^k x^\ell)(a^{k'} x^{\ell'})] = a^k (x^\ell a^{k'} x^{\ell'}) x^{\ell+\ell'} - a^{k+k'} i^{\ell} \cdot x^{\ell+\ell'} \in R$$

hence a division ring $\stackrel{T4.13}{\Rightarrow} D$ field $\Rightarrow x, a$ commute \hookrightarrow
↳ exercise class

November 13, 2025

Proof of 4.12: Define $\delta: D \rightarrow D$, $x \mapsto [a, x] := ax - xa$. δ is a derivation ($\delta(x+y) = \delta(x) + \delta(y)$, $\delta(xy) = \delta(x)y + x\delta(y)$) and K -linear for $K := \mathbb{F}_p[a]$ ($\delta(\lambda x) = \lambda \delta(x)$ for $\lambda \in K$).

$m \geq 1$ minimal s.t. $a^{p^m} = a \Rightarrow K \cong \mathbb{F}_{p^m}$ ($\mathbb{F}_{p^m} = \{c \in \bar{\mathbb{F}}_p \mid c^{p^m} = c\}$)

Claim: (1) $\delta^{p^n} = [a^{p^n}, x] \quad \forall x \in D, n \geq 1$

$$(2) \delta^{p^n} = \delta$$

Proof (1) $\delta^i(x) = \sum_{j=0}^i (-1)^{i-j} \binom{i}{j} a^j x a^{i-j}$ (combinatorial argument)

Now $p \mid \binom{p^n}{j}$ unless $j \in \{0, p^n\} \Rightarrow \delta^{p^n}(x) = a^{p^n} x - x a^{p^n}$.

(2) $a^{p^m} = a \Rightarrow \delta^{p^m}(x) = \delta(x)$.

□ (claim)

So $f(\delta) = 0$ with $f = t^{p^m} - t \in \mathbb{F}_p[t]$ (in $\text{End}_K(D)$)

$F = \prod_{b \in K} (t - b)$. Let $g = + (t - b_1)(t - b_2) \cdots (t - b_\ell)$ with ℓ minimal s.t. $g(\delta) = 0$.

$\delta \neq 0 \Rightarrow \ell \geq 1 \Rightarrow \delta(\delta - b_1) \cdots (\delta - b_{\ell-1}) \neq 0$

Let $v \in D$ s.t. $x := \delta(\delta - b_1) \cdots (\delta - b_{\ell-1}) v \neq 0$
 $\Rightarrow (\delta - b_\ell)x = 0$, so x is an eigenvector of S with eigenvalue
 $b := b_\ell \in K \Rightarrow ax - xa = bx \Rightarrow xa = (a - b)x \Rightarrow xax^{-1} = a - b$

Now, $a, a-b$ are elements of the finite field K of the same multiplicative order. Since K^\times is cyclic, they generate the same subgroup. $\Rightarrow a-b = a^i$ for some $i \geq 1$, $a \neq a^i$ since $b \neq 0$. \blacksquare

For $n \geq 1$, let $\mu_n(\bar{\mathbb{Q}}) := \{\zeta \in \bar{\mathbb{Q}} \mid \zeta^n = 1\}$ the n -th roots of unity, and $\mu_n^*(\bar{\mathbb{Q}}) := \{\zeta \in \mu_n(\bar{\mathbb{Q}}) \mid \zeta^m \neq 1 \text{ for } m|n, m \neq n\}$ the n -th primitive roots of unity. Then $|\mu_n(\bar{\mathbb{Q}})| = n$, $|\mu_n^*(\bar{\mathbb{Q}})| = \varphi(n)$, where φ is the Euler- φ -function. Define $\Phi_n(x) := \prod_{\zeta \in \mu_n^*(\bar{\mathbb{Q}})} (x - \zeta)$ the n -th cyclotomic polynomial.

Lemma 4.14: (1) If $m|n$, then $x^m - 1|x^n - 1$ in $\mathbb{Z}[x]$.
(2) $\Phi_n(x) \in \mathbb{Z}[x]$ and $\Phi_n(x) | x^n - 1$ in $\mathbb{Z}[x]$.

Proof: (1) $x^n - 1 = (x^m)^{n/m} - 1^{n/m} = (x^m - 1) \underbrace{\sum_{j=0}^{m-1} x^{mj}}_{\in \mathbb{Z}[x]}$

(2) If $m|n$, then $x^m - 1|x^n - 1$. Since $\mathbb{Z}[x]$ is a UFD, also $F := \text{lcm}(\{x^m - 1 \mid m|n, m \leq n\})$ divides $x^n - 1$.

$$\frac{x^n - 1}{F} = \prod_{\substack{\zeta \in \mu_n(\bar{\mathbb{Q}}) \\ m|n, m \neq n}} (x - \zeta) = \prod_{\substack{\zeta \in \mu_n^*(\bar{\mathbb{Q}})}} (x - \zeta) = \Phi_n(x)$$

Remark: Φ_n is irreducible.

Lemma 4.15 If D is a division ring and $K \subseteq L \subseteq D$ are subfields, then $[D : K] = [D : L][L : K]$.

$$\dim_K D$$

Proof: If $(e_i)_{i \in I}$ is an L -basis for D , and $(f_j)_{j \in J}$ is a K -basis for L , then $(e_i f_j)_{i \in I, j \in J}$ is a K -basis for D . □

Proof of T4.13: $Z(D) = F$ is a finite field

$\Rightarrow |F| = q$ with q a prime power

$\Rightarrow |D| = q^n$ with $n = \dim_F D$.

Class equation for D^* :

For $a \in D^*$, $C(a) := \{b \in D \mid ba = ab\} =: Z_D(a)$ (^{centralizer of a in D}) is a division ring.

$$|\{bab^{-1} \mid b \in D^*\}| = \frac{|D^*|}{|C(a)^*|}$$

$$\Rightarrow q^{n-1} = |D^*| = \underbrace{q^n - 1}_{\text{center}} + \sum_{i=1}^l \frac{|D^*|}{|C(a_i)^*|} = q^{n-1} + \sum_{i=1}^l \frac{q^{n-1}}{q^{m_i-1}}$$

where a_1, \dots, a_l represent the nontrivial conjugacy classes in D^* .

Here $|C(a_i)| = q^{m_i} - 1$ for $1 \leq m_i < n$ since $C(a_i)$ is a division ring with some $m_i = \dim_F C(a_i) < n$.

Note $\frac{x^{n-1}}{x^{m_i-1}} = \Phi_n(x) H_i(x)$ with $H_i \in \mathbb{Z}[x]$ ($\Phi_n(x) \in \mathbb{Z}[x]$)

$\Phi_n(x) \in \mathbb{Z}[x] \Rightarrow \Phi_n(q) \in \mathbb{Z}$ and (since $H_i(q) \in \mathbb{Z}$)

$$\Rightarrow \Phi_n(q) \mid \frac{q^{n-1}}{q^{m_i-1}}.$$

$\Rightarrow \Phi_n(q) \mid q-1$

But $\Phi_n(q) = \prod_{\zeta \in \mu_n^*(\bar{\mathbb{Q}})} (q - \zeta)$ and $|q - \zeta| > q-1$ if $\zeta \neq 1$.

So this is only possible if $n=1$ (otherwise $|\Phi_n(q)| > q-1 \Rightarrow D=F$ □)

Remark: Claim: K field $G \subseteq K^*$, G finite

Claim: G is cyclic ($G \cong \mathbb{Z}/n\mathbb{Z}$ for some n)

used in proof
of 4.12.

$$(G, \cdot) = (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_d\mathbb{Z}) \quad 1 \neq m_1 | m_2 | \cdots | m_d$$

$\Rightarrow \forall g \in G, g^{m_d} = 1 \Rightarrow \forall g \in G, g$ is a root of $x^{m_d} - 1$ in $K[x]$

$\Rightarrow |G| \leq m_d$

\vdots
 $m_1 \cdots m_d$

5. Tensor Products

R ring

Let $M_R \in \text{Mod-}R$, $RN \in R\text{-Mod}$, $X \in \underline{\text{Ab}} = \mathbb{Z}\text{-mod}$. A map $\varphi: M \times N \rightarrow X$ is **R-balanced** if $\forall m, m' \in M, \forall n, n' \in N, \forall r \in R:$

- $\varphi(m+m', n) = \varphi(m, n) + \varphi(m', n)$
- $\varphi(m, n+n') = \varphi(m, n) + \varphi(m, n')$
- $\varphi(mr, n) = \varphi(m, rn)$

The **tensor product** of M and N is an Abelian group $M \otimes_R N$ ($= M \otimes N$) together with an R -balanced map satisfying the following universal property: If $\varphi: M \times N \rightarrow X$ is R -balanced, there exists a unique group homomorphism ($= \mathbb{Z}$ -hom) $\bar{\varphi}: M \otimes_R N \rightarrow X$ s.t. $\varphi = \bar{\varphi} \circ \otimes$

$$\begin{array}{ccc} M \times N & \xrightarrow{\otimes} & M \otimes_R N \\ & \searrow \varphi & \downarrow \exists! \bar{\varphi} \\ & & X \end{array}$$

$(M \otimes_R N, \otimes)$ is unique up to unique iso:

If $(M \otimes N, \otimes)$ satisfies the same UP

$$\begin{array}{ccc} M \times N & \xrightarrow{\otimes} & M \otimes N \\ & \swarrow \bar{\otimes} \quad \uparrow \bar{\otimes} & \downarrow \bar{\otimes} \\ & & M \otimes N \end{array} \quad \text{but also} \quad \begin{array}{ccc} M \times N & \xrightarrow{\otimes} & M \otimes N \\ & \searrow \bar{\otimes} \quad \downarrow \bar{\otimes} \circ \bar{\otimes} & \downarrow \bar{\otimes} \\ & & M \otimes N \end{array}$$

uniqueness

$$\Rightarrow \text{id}_{M \otimes N} = \bar{\otimes} \circ \bar{\otimes}$$

$$\text{By symmetry: } \text{id}_{M \otimes N} = \bar{\otimes} \circ \bar{\otimes}.$$

Existence: Let F be a free \mathbb{Z} -module with basis

$\{e_{(m,n)} \mid m \in M, n \in N\}$. Let $K \leq_{\mathbb{Z}} F$ be generated by $\{(m, m', n, n') \in M \times M \times N \times N \mid m - m' \in N, n - n' \in M\}$:

$$e_{(m+n, n)} - e_{(m, n)} - e_{(m, n')}$$

$$\cdot e_{(m,n+m)} = e_{(m,m)} + e_{(m,n)}$$

$$\cdot e_{(mr,n)} = e_{(m,rn)}$$

Define $M \otimes_R N := F/K$, $\otimes : M \times N \longrightarrow M \otimes_R N$, $(m,n) \mapsto e_{(m,n)} + K =: m \circ n$

Check: \otimes is R -balanced, $M \otimes_R N$ satisfies the UP (using hom. thm.).

Elements of the form $m \circ n$ are **pure** (= elementary), general elements are $\sum_{i=1}^k m_i \circ n_i$, $m_i \in M$, $n_i \in N$.

If $f : M_R \longrightarrow M'_R$, $g : {}_R N \longrightarrow {}_R N'$ are module homomorphisms, then $(f,g) : M \times N \longrightarrow M' \otimes_R N'$, $(m,n) \mapsto f(m) \circ g(n)$ is R -balanced.

$[f(mr) \circ g(n) = f(m)r \circ g(n) = f(m) \circ rg(n) - f(m) \circ g(rn)]$, and it induces a unique $f \circ g : M \otimes_R N \longrightarrow M' \otimes_R N'$

$$m \otimes n \mapsto f(m) \circ g(n)$$

$\Rightarrow \otimes : \underline{\text{Mod}}\text{-}R \times R\text{-}\underline{\text{Mod}} \longrightarrow \text{Ab}$ is a functor.

! $f \circ g$ (symbol) also makes sense as an element of $\text{Hom}(M,M') \otimes \text{Hom}(N,N')$, but this is something different in general

Bimodules: If sM_R , ${}_RN_T$ are (S,R) resp. (R,T) - bimodules, then $sM_R \otimes_R {}_RN_T = {}_s(M \otimes_R N)_T$ is a (S,T) - bimodule via $s(m \circ n)t := (sm) \circ (nt)$.

Remark: (1) If M_R , ${}_RN$ are just modules, they are $\underline{\text{Mod}}\text{-}R$, $R\text{-}\underline{\text{Mod}}$ bimodules, so the previous case is a special case.
 (2) If R is commutative, every module is an (R,R) - bimodule, so for $M, N \in \underline{\text{Mod}}\text{-}R$, $M \otimes_R N$ is again an R - module.

$\Rightarrow \otimes$ is a functor $(S,R)\text{-}\underline{\text{Mod}} \times (R,T)\text{-}\underline{\text{Mod}} \longrightarrow (S,T)\text{-}\underline{\text{Mod}}$.

R commutative: $M, N, X \in R\text{-Mod}$

$f: M \times N \rightarrow R$ is R -bilinear if it is R -balanced &

$$f(rm, n) = rf(m, n) = f(m, rn) \quad \forall m \in M, \forall n \in N, \forall r \in R.$$

Then $M \otimes_R N$ satisfies the analogous UP wrt. R -bilinear maps:

$f: M \times N \rightarrow X$ R -bilinear $\Rightarrow \exists ! \bar{f} \in \text{Hom}(M \otimes_R N, X_R)$. $\bar{f} \circ \otimes = f$.

\otimes - Hom Adjunction:

Motivation/Comparison:

In Set: $\text{Hom}(A \times B, C) \cong \text{Hom}(A, \text{Hom}(B, C))$ (functorial in A, B, C)

$$\begin{aligned} f: A \times B &\rightarrow C \longmapsto (a \mapsto f_a: B \rightarrow C), & f_a(b) = f(a, b) \\ (a, b) &\mapsto (f(a))(b) \quad \longleftrightarrow \quad f \end{aligned}$$

$$f: C \rightarrow C', \text{Hom}(B, f'): \text{Hom}(B, C) \rightarrow \text{Hom}(B, C'), \quad g: C' \rightarrow C'' \quad (g \circ f)_* = g_* \circ f_*$$

$$\boxed{f: B \xrightarrow{\cong} B'}: \text{Hom}(B', C) \rightarrow \text{Hom}(B, C), \quad (j \circ \varphi)^* = f^* \circ \varphi^*$$

Two (bi)functors: $- \times - : \underline{\text{Set}} \times \underline{\text{Set}} \rightarrow \underline{\text{Set}}$
 $\text{Hom}(-, -) : \underline{\text{Set}}^{\text{op}} \times \underline{\text{Set}} \rightarrow \underline{\text{Set}}$

$$- \times B : \underline{\text{Set}} \rightarrow \underline{\text{Set}}, \quad \text{Hom}(B, -) : \underline{\text{Set}} \rightarrow \underline{\text{Set}}$$

$\textcircled{*}$: $- \times B$ is left adjoint to $\text{Hom}(B, -)$

($\Rightarrow - \times B$ commutes with colimits; $\text{Hom}(B, -)$ with limits)
(preserves)

For (bi)modules: First note: if M_R, N_R are modules

$\text{Hom}(M_R, N_R)$ is in general only an Abelian group.

[$(f_r)(m) = f(rm)$ does not work]. But:

• If $_S M_R$ is a bimodule, $\text{Hom}(_S M_R, N_R)_S$ is a right S -module
via $(f_S)(m) := f(sm)$. \curvearrowright contravariant

• If N_R is a (T, R) -bimodule, $\underline{\text{Hom}}(M_R, \underline{\text{Hom}}(N_R))$ is a left T -module via $(tf)(m) := f(m)$. $\xleftarrow[\mathbb{F}_N]{\text{covariant}}$

\otimes -Hom adjunction: $R M_S$ bimodule

- $\otimes_R M : \underline{\text{Mod}}-R \rightarrow \underline{\text{Ab}}$

$\text{Hom}_S(M_S, -) : \underline{\text{Mod}}-S \rightarrow \underline{\text{Ab}}$

are adjoint via $(X_R \in \text{Mod}-R, Y_S \in \text{Mod}-S)$

$$\begin{aligned} \text{Hom}_S(X_R \otimes_R M_S, Y_S) &\cong \text{Hom}_R(X_R, \text{Hom}(R M_S, X_S)_R) \\ f &\mapsto (x \mapsto f_x), \quad f_x(m) = f(x \otimes m) \\ x \otimes m &\mapsto g(x)(m) \end{aligned}$$

Proof: using UP.

Remark: If X is a (T, R) -bimodule, Y a (T', S) -bimodule, then the iso is an (T', T) -bimodule.

So: \otimes commutes with colimits (direct sum, cokernel)

If $A_R \xrightarrow{f} B_R \xrightarrow{g} C_R \rightarrow 0$ is exact, then so is $A \otimes_R M \rightarrow B \otimes_R M \rightarrow C \otimes_R M \rightarrow 0$, i.e. $- \otimes_R M$ is right exact

$$\begin{aligned} a \otimes m &\mapsto f(a) \otimes m \\ b \otimes m &\mapsto g(b) \otimes m \end{aligned}$$

(In general: $f: A_R \rightarrow B_R$ injective $\not\Rightarrow f \otimes M: A \otimes_R M \rightarrow B \otimes_R M$ injective.)

Proof sketch: First verify:

(i) $0 \rightarrow N_R \xrightarrow{f} M_R \xrightarrow{g} K_R \rightarrow 0$ exact

$\Leftrightarrow \forall X \in \text{Mod}-R : 0 \rightarrow \text{Hom}(X_R, N_R) \xrightarrow{f^*} \text{Hom}(X_R, M_R) \xrightarrow{g^*} \text{Hom}(X_R, K_R) \rightarrow 0$ exact

$$f_{*}(r) = f \circ r \quad g_{*}(r) = g \circ r$$

(ii) $N_R \xrightarrow{f} M_R \xrightarrow{g} K_R \rightarrow 0$ exact

$\Leftrightarrow \forall X \in \text{Mod}-R. 0 \rightarrow \text{Hom}(K_R, X_R) \xrightarrow{f^*} \text{Hom}(M_R, X_R) \xrightarrow{g^*} \text{Hom}(N_R, X_R) \rightarrow 0$ exact

$$g^*(r) = r \circ g \quad f^*(r) = f \circ r$$

(\Rightarrow): $\text{Hom}(X_R, -)$, $\text{Hom}(-, X_R)$: $(\text{Mod-}R)^{\text{op}} \rightarrow \widetilde{\text{Ab}}$ are left exact.

Now: $A_R \xrightarrow{f} B_R \xrightarrow{g} C_R \rightarrow 0$ exact, $RX \in R\text{-Mod}$

Consider $A \otimes_R X \xrightarrow{f \otimes \text{id}_X} B \otimes_R X \xrightarrow{g \otimes \text{id}_X} C \otimes_R X \rightarrow 0$ ($- \otimes_R X$)

Apply $\text{Hom}_{\mathbb{Z}}(-, Y)$, $Y \in \text{Ab}$

$$0 \rightarrow \text{Hom}_{\mathbb{Z}}(C \otimes_R X_{\mathbb{Z}}, Y_{\mathbb{Z}}) \rightarrow \text{Hom}_{\mathbb{Z}}(B \otimes_R X_{\mathbb{Z}}, Y_{\mathbb{Z}}) \rightarrow \text{Hom}_{\mathbb{Z}}(A \otimes_R X_{\mathbb{Z}}, Y_{\mathbb{Z}})$$

$\otimes\text{-Hom adj}$ $\downarrow z\text{-iso}$ \hookrightarrow $\downarrow s$ \hookrightarrow $\downarrow s$

$$0 \rightarrow \text{Hom}_R(RX, R\text{Hom}_{\mathbb{Z}}(C_R, Y)) \rightarrow \text{Hom}_R(RX, R\text{Hom}(B, Y)) \rightarrow \text{Hom}_R(RX, R\text{Hom}(A, Y))$$

$\stackrel{(ii), (iii)}{\Rightarrow}$ lower row is exact \Rightarrow upper row is exact $\stackrel{(ii)}{\Rightarrow}$ (*) is exact.