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: $T_n(R)=\begin{bmatrix} R & R & \cdots & R \\ 0 & R & \ddots & R \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & R \end{bmatrix}$

$R=K$ Field: $A\cdot \underbrace{\operatorname{adj}(A)}_{\text{adjugate of } A/\text{classical adjoint of } A} = \det(A)\cdot I_n \in M_n(K)$

So: $A\in M_n(K)^\times \Leftrightarrow \det(A)\neq 0$

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

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

$\left(\Rightarrow ijk=i=-kj,\ ki=j=-ik,\ k^2=-1\right)$

For $\alpha=a+bi+cj+dk$ $(a,b,c,d\in\mathbb{R})$, let $\bar{\alpha} := a-bi-cj-dk$
$\Rightarrow \alpha\bar{\alpha}=\bar{\alpha}\alpha=\underbrace{a^2+b^2+c^2+d^2}_{\geq 0} =: \operatorname{nr}(\alpha)\in\mathbb{R}_{\geq 0}$ reduced norm

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

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

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

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.

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

(different)

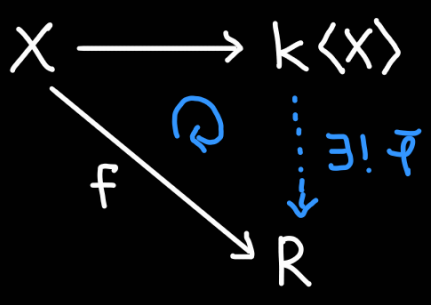
Coefficients commute with indeterminates, but indeterminates do not commute with each other.

$\Rightarrow k\langle X\rangle$ is a ring, product: k-linearly extend concatenation of words

(universal property)

UP: If R' is a ring, $\varphi: k \to Z(R')$ 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. $\bar{f}|_X = f$]



(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 $k[x_1,\dots,x_n]$!

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

$\varphi: k\langle z_i \mid i\in\mathbb{N}_0\rangle \hookrightarrow k\langle x,y\rangle$, $z_i \mapsto xy^i$ (monomorphism)

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. $f: k\langle x_i \mid i\in I\rangle \twoheadrightarrow R, \quad x_i \mapsto g_i$

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"

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

  ↳ $xy-yx$ being in the kernel means $xy=yx$

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

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

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

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

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

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

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:

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

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

Special cases: R commutative,

- G Free monoid generated by a set X
  $\Rightarrow R[G]$ is the Free R-algebra generated by X
- $G \cong \left(\mathbb{N}_0^{(I)}\right)$, say freely generated by $\{x_i \mid i \in I\}$, so elements of G are of the form $x_{i_1}^{n_1} \cdots x_{i_k}^{n_{i_k}}$, $i_1, \ldots, i_k \in I$ pairwise distinct
  $\Rightarrow R[G] \cong$ polynomial ring

Universal property: 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. $\overline{f}: R[G] \longrightarrow R'$ s.t. $\overline{f}|_R = f$, $\overline{f}|_G = \sigma$.

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, $i \geq 0$

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

$$fg := \sum_{i,j=0}^{n} a_i \sigma^i(b_j) x^{i+j},$$

$$\boxed{\forall a \in R.\ xa = \sigma(a)x}$$

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: $\exists b \in R \setminus \{0\}$, $\sigma(b) = 0$
$\Rightarrow x \cdot b = \sigma(b)\, x = 0 \Rightarrow x$ is a left zerodivisor, not right zerodivisor
($x \neq 0$, $b \neq 0$, $\sigma(b) = 0$)

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

E.g. $x^2 a = x(ax + \sigma(a)) = (xa)x + x\sigma(a)$
$= ax^2 + \sigma(a)x + \sigma(a)x + \sigma^2(a)$
$= ax^2 + 2\sigma(a)x + \sigma^2(x)$

E.g. $R = k[y]$, k ring, $\delta = \frac{d}{dy}$
In $k[y][x; \sigma]$: $xy = yx + \delta(y) = yx + 1$

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

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

c) Mixed case: 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 $x \cdot a \doteq \sigma(a)x + \delta(a)$ with maps $\sigma, \delta: R \to R$
$\Rightarrow xab = x(ab) = \sigma(ab)x + \delta(ab)$
$= (xa)b = (\sigma(a)x + \delta(a))b = \sigma(a)(\sigma(b)x + \delta(b)) + \delta(a)b$
$= \underbrace{\sigma(a)\sigma(b)}_{\sigma(ab)}\, x + \underbrace{\sigma(a)\delta(b) + \delta(a)b}_{\delta(ab)}$

$\Rightarrow \sigma$ 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,
$R[\![x]\!] = \{a_0 + a_1 x + a_2 x^2 + \cdots \mid a_i \in R\}$.
Then $f \in R[\![x]\!]^\times \iff a_0 \in R^\times$

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

invertible $\Leftrightarrow$ lowest coeff. invertible

$\Rightarrow$ if R is a division ring, so is $R((x))$.

Twisted versions:

- $R[[x;\sigma]]$ with $\sigma \in End(R)$: $xa = \sigma(a)x$
- $R[[x;\sigma]]$ with $\sigma \in Aut(R)$: $xa = \sigma(a)x$

(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 won't work.

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

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

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

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

We will default to right modules.

Remark: 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 $\tilde{\sigma}(a)(m) := \underbrace{ma}_{:=\sigma(m,a)}$.
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. $R \to \mathrm{End}_{\mathbb{Z}}(M)$

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. $\varepsilon: R \longrightarrow Z(A)$ (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.]
(a: multiplication in A)

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

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

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

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

is a ring with multiplication $\circ$

[e.g. $(f \circ (g+h))(m) = f((g+h)(m)) \overset{+ \text{ pointwise}}{=} f(g(m)+h(m))$
$\overset{F \text{ hom}}{=} f(g(m)) + f(h(m))$
$= (f \circ g + g \circ h)(m)$.]

Special cases:

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

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

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

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

- 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 $M \in \mathrm{Mod}\text{-}R$, TFAE:
(a) Every $N_R \subseteq M_R$ 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,
$\exists m_1, \dots, m_k \in M'$: $M' = \langle m_1, \dots, m_k \rangle_R$ $(m_1R + \cdots + m_kR)$ 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. $N_i \subsetneq N_{i+1}$ ↯

(c) $\Rightarrow$ (a): Let $N \subseteq M$ 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. ▨

Definition: (1) $M \in$ 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.

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 $\sum_{i \geq 0} y^i x y R$ 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 $L \trianglelefteq_R R$ consider the left ideals $L_n \trianglelefteq_R R$ 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}
$\Rightarrow \forall n \geq n_0.\ M_{n_0} = M_n$. ▨

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 [$_R R$] 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 $0 \to N \to M \to L \to 0$ ($L \cong M/N$) 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: $M_i = M_{i_0}$

($\subseteq$): ✓ (2): Let $m \in M_{i_0} \Rightarrow m \in M_{i_0} + N = M_i + N$, so $m = m' + n$ ($m' \in M_i, n \in N$)

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

(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 $\varphi: R_R \twoheadrightarrow M_R$
$[(\Rightarrow): r \mapsto mr,\ (\Leftarrow): \varphi: R_R \twoheadrightarrow M_R,\ M = \varphi(R) = \varphi(\overset{m}{\underset{ii}{1}})R]$
$\Leftrightarrow M \cong R/I$ for a right ideal $I \leq R_R$
$[(\Rightarrow): R/\ker\varphi \cong M,\ (\Leftarrow): R \to R/I,\ r \mapsto r+I$ 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, $R = M_d(k)$, $V = k^{1\times d}$ (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 $vR = V$ $\forall v \in V \setminus \{0\}$.

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 $0 \neq m \in M$, $0 \neq mR \leq M_R$ (submodule) $\Rightarrow mR = M$.

(b) $\Rightarrow$ (c): Let $0 \neq m \in M$. Let $\varphi: R_R \twoheadrightarrow M_R$, $r \mapsto mr$. ((b))
$I := \ker(I) =:$ 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 (why?) submodule of M. $\not\Rightarrow$

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

(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 $J = R$ (I maximal), M is simple. ▨

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. ▨

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

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 $D = k$.

Proof: ($\Leftarrow$): If L/k is a finite field ext., it is a Fin. dim. div. alg. $/k$.

($\Leftarrow$): 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 $\mathrm{End}(M_R) = k$ (canonically).

Proof: $k \hookrightarrow \mathrm{End}(M)$ via scalar mult.: $\lambda \in k \longmapsto (m \mapsto m\lambda)$
$\mathrm{End}(M_R) \subseteq \mathrm{End}(M_k) \cong M_d(k)$ For $d = \dim_k(M)$, so $\mathrm{End}(M_R)$ is a Fin.-dim. k-algebra and a division ring (L 1.2).
$\xRightarrow[k \text{ alg. closed}]{} \mathrm{End}(M_R) = k$. ▨

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

2.2. Composition series

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

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

$$0 = 12\mathbb{Z}/12\mathbb{Z} \subsetneq 6\mathbb{Z}/12\mathbb{Z} \subsetneq 2\mathbb{Z}/12\mathbb{Z} \subsetneq \mathbb{Z}/12\mathbb{Z}$$

$\mathbb{Z}/2\mathbb{Z}$ $\quad$ $\mathbb{Z}/3\mathbb{Z}$ $\quad$ $\mathbb{Z}/12\mathbb{Z}$

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

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

$(A \cap B)$

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

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

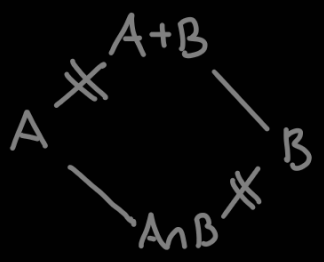
$\Rightarrow c = a - b \in A \Rightarrow a = b + c \in B + (A \cap C)$.

B $\quad A \cap C$

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

One of the isomorphism theorems.

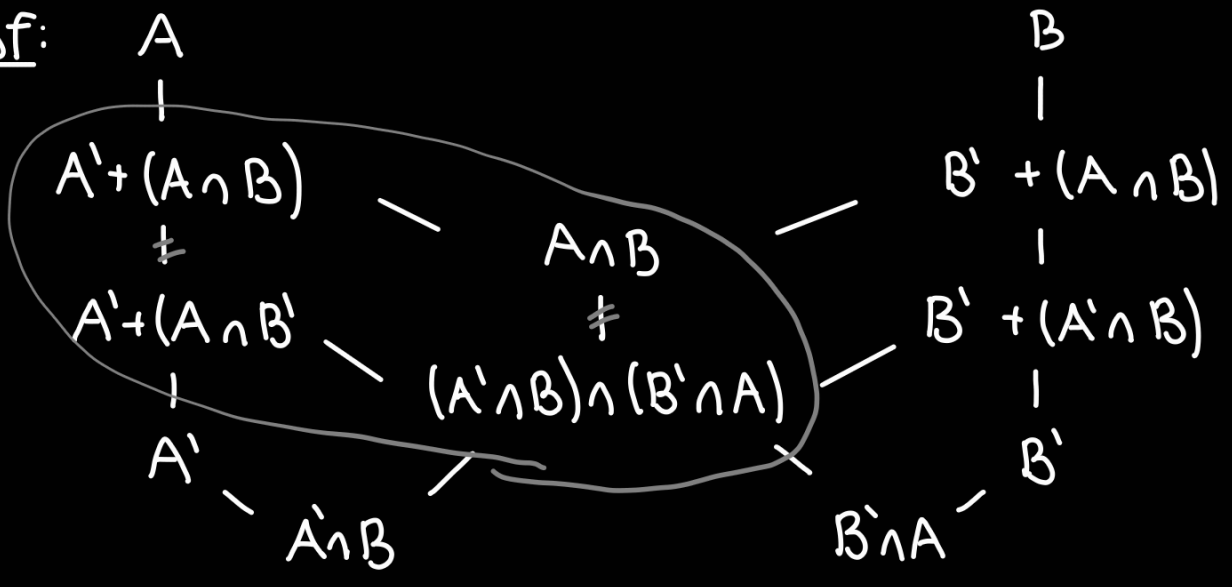
$$\frac{A+B}{A} \cong \frac{B}{A \cap B}.$$



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

• $(A \cap B) \cap (A' + (A \cap B')) \overset{L.2.5}{=} (A \cap B \cap A') + (A \cap B')$

$A \cap B' \leq A \cap B$

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

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

(From above; symmetry)

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 $M\in$ 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 $0 = A_0 \leq A_1 \leq \cdots \leq A_m$, $0 = B_0 \leq B_1 \leq \cdots \leq B_n = M$ 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. ▨

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 $0 = A_1 \leq A_2 \leq \cdots \leq A_n = M$ 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: $A_0 := 0$.
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 $A_{i-1} \leq M$, the set $\Omega = \{A \leq M_R : A_{i-1} \leq A_i\}$ 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. ▨

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.

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

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

$\forall i \in I.\ M_i \cap (N + M') \in \{0, M_i\}$ 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 $0 \neq M \in \text{Mod-}R$. 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 $N \oplus K'$ $\exists m$ 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 $M_1, \ldots, M_k$.

(2) **Endomorphism Rings**: Suppose $M_R \cong M_1 \oplus \cdots \oplus M_k$.
Let $\varepsilon_i : M_i \longrightarrow M$ be the canonical 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 $f \in \text{End}(M_R)$, then $f(m) = \sum_{i,j=1}^{k} \varepsilon_i \circ \pi_i \circ f \circ \varepsilon_j \circ \pi_j(m)$, where $f_{ij} := \pi_i \circ f \circ \varepsilon_j$.

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):

$$(\psi \circ \varphi)_{ij} = \sum_{\ell=1}^{k} \psi_{i\ell} \circ \varphi_{\ell j},$$

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

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

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

$$\exists f' : N \to M.\ f' \circ f = id_M$$

$$\Leftrightarrow \exists g' : K \to K.\ g \circ g' = id_K$$

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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & N & \longrightarrow & K & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id_M} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle id_K} & & \\ 0 & \longrightarrow & M & \longrightarrow & M \oplus K & \longrightarrow & K & \longrightarrow & 0 \end{array} \quad \text{commutes}$$

$m \longmapsto (m, 0)$

$(m, k) \longmapsto k$

(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 $K \cong M/N$. $\overset{\text{T. 2.12(c)}}{\Rightarrow}$ 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 $N \xrightarrow[\text{proj.}]{} f(M) \xrightarrow{f^{-1}} M$. Then $f \circ f^{-1} = \mathrm{id}_M$. ▨

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 $M_1, \ldots, M_k$.

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 $(D_1, n_1), \ldots, (D_k, n_k)$ are uniquely determined (up to order and isomorphism) and R has exactly k simple modules $S_1, \ldots, S_k$ up to isomorphism. Also $D_i \cong \text{End}(S_i)$.

October 23, 2025

C2.16

Proof: **Existance**: $R_R = S_1^{n_1} \oplus \cdots \oplus S_k^{n_k}$ 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
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 $f: S_1^{n_1} \oplus \cdots \oplus S_n^{n_k} \longrightarrow\!\!\!\!\rightarrow S$
$\Rightarrow S$ 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 $\text{Mod-}M_{m_i}(E_i)$.
$\Rightarrow V_1, \ldots, V_e$ are nonisomorphic simple R-modules
[with $V_i M_{m_j}(E_j) = 0$ $\forall i \neq j$]

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

Uniqueness of composition series (after renumbering):

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

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

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

Corrolary: 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: ·) $M_n(D)$, D div. ring (then $M_n(D)$ is also artinian).

·) $A_1(k)$, k field, $\mathrm{char}\, k = 0$, is simple (exercise)

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

⚠ R simple ring $\Rightarrow {}_RR$ simple module
(not even ${}_RR$ 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 $R_i R = R_i$, $R_j' R = R_j'$

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

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

2.5. Simple artinian rings

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

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

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

(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)
↳ 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), $I \trianglelefteq R$ 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 $\Omega = \{0 \neq I_R \leq R_R\} \leq \emptyset$
By right artinianity, Ω has a minimal element.

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

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

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

$\Rightarrow rI_R$ 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

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

Consider $\mathcal{F} = \{f : R_R \to M_R^n \mid n \geq 0, f \ R\text{-hom}\}$. 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 $0 \neq r \in \ker f$. $\operatorname{ann}(M) = 0 \Rightarrow \exists m \in R.\ mr \neq 0$.

Define $\hat{f} : R \to M^n \oplus M$, $x \mapsto (f(x), mx)$ $\Rightarrow \ker\hat{f} \subsetneq \ker f$ ↯ contradiction minimality]

So $F : R_R \hookrightarrow M_R^n$, M_R^n semisimple $\overset{T2.12}{\Rightarrow} M_R^n \cong R_R \oplus K_R$

$\overset{C2.13}{\Rightarrow} R_R$ semisimple, $R_R \cong M_R^m$ for some $m \leq n$.

(d)$\Rightarrow$(e): [T2.18]

(e)$\Rightarrow$(a): ✓ (exercises, fin.dim $\rightsquigarrow$ artinian) ▨

right art $\not\Rightarrow$ left art

right primitive $\not\Rightarrow$ left primitive

right artinian + right primitive $\Rightarrow$ left art, left prim

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

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

$\Updownarrow$ $\Updownarrow$

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. $T(\rho(g)v) = \sigma(g)Tv$.
= 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. $\rho: K[G] \to \mathrm{End}(M_{\mathbb{Z}})$.
"$\leftarrow$": A $K[G]$ module M is a k-vector space $(\rho|_K)$
"$\mapsto$": A repr. $\rho: G \to GL(V_K)$ gives rise to a monoid hom

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

($\mathrm{End}(V_K)$ is a ring)

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

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. $\pi \circ \varphi = id_V$.
$\operatorname{char} K \nmid |G| \Rightarrow |G| \in K^\times$
Define: $\tilde{\varphi}(v) := \frac{1}{|G|} \sum_{g \in G} \varphi(vg)g^{-1}$.

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

$$\tilde{\varphi}(\underbrace{v}_{V}\underbrace{g}_{G}) = \frac{1}{|G|}\sum_{g\in G}\varphi(vhg)^{-1}g = \frac{1}{|G|}\sum_{g\in G}\varphi(vg)g^{-1}k$$

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

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

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

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

▨

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

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

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

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: $\forall g \in G \; \exists \lambda_g \in K. \; 1_K \cdot g \mapsto \lambda_g$

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

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

3. Jacobson Radical

Definition: 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.

$\operatorname{ann}(m) := \operatorname{ann}(\{m\})$, $\operatorname{ann} X = \bigcap_{x \in X} \operatorname{ann}(x)$

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

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

Example: ·) $I \trianglelefteq R$ 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

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

Definition: The Jacobson radical of R is

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

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

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

[**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: $J(R) \overset{A}{=} \bigcap \{J \mid J_R \leq R_R \text{ maximal right ideal}\}$

$\overset{C}{=} \{r \in R \mid \forall x \in R.\ 1 - rx \text{ is right invertible}\}$

$\overset{D}{=} \{r \in R \mid \forall x, y \in R.\ 1 - xry \text{ is invertible}\}$

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 ⊆ 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 ⊆ 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 ⊆ A): Suppose $r \in C$. $Mr \neq 0$ for some simple module M.

$\Rightarrow \exists m \in M.\ mr \neq 0 \overset{M \text{ simple}}{\Rightarrow} M = mrR \Rightarrow \exists x \in R.\ m = mrx$

$\Rightarrow m(1-rx) = 0 \Rightarrow m = 0$ ↯

($\uparrow$ $1-rx$ right invertible)

(C = D): $D \subseteq C$ ✓

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

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

$xr \in J(R) \overset{C=A}{\Leftrightarrow} \exists z \in R : (1 - \underbrace{xry}_{\in J(R)})z = 1 \Rightarrow z$ 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 $\Rightarrow J(R) = 0$

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 $J(R) = 0$.

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 $J(R) = \bigcap \{\tilde{I} \mid \tilde{I} \subseteq R_R \text{ maximal}\}$ ▨

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

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

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

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

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

Respects submodules, morphisms, etc. (category isomorphism)

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

2) ($\Rightarrow$): ✓

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

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

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

($x \in J(R)$; $x \in J(R)$)

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.

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

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

Remark: Easy to prove: $I, J \trianglelefteq R_R$ nilpotent $\Rightarrow I+J$ nilpotent

Open Conjecture (Köthe Conjecture): $I, J \trianglelefteq R_R$ nil $\Rightarrow I+J$ nil.

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

Proof: Let $x \in I \Rightarrow \forall x \in R.\ xr$ nilpotent, say $(xr)^n = 0$
$\Rightarrow (1-xr)(1+xr+(xr)^2+\cdots+(xr)^{n-1}) = 1-(xr)^n = 1$
$\Rightarrow 1-xr$ 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: $J(R) \supseteq J(R)^2 \supseteq J(R)^3 \supseteq \cdots$ 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 $A \leq R_R$ be a right ideal minimal with the property $AI \neq 0$ (exists, because R is right artinian).
Let $x \in A$ s.t. $xI \neq 0$.
$\Rightarrow xI \cdot I = xI^2 = xI \neq 0 \underset{xI \leq A_R}{\Rightarrow} A = xI$
$\Rightarrow x = xy$ with $y \in I$ ($I \subseteq J(R)$) $\Rightarrow x(\underbrace{1-y}_{\in R^\times}) = 0 \Rightarrow x = 0$ ↯ ▨

3.2. Semisimple rings again

Lemma 3.7: A right ideal $I \leq R_R$ 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 $r \in R \cap (1-e)R$, then $r = ex = (1-e)y \quad (x, y \in R)$
$\Rightarrow er = e(ex) = ex = r$, so $r = er = e(1-e)y = (e-e^2)y = 0$

($\Rightarrow$): Suppose $R_R = I_R \oplus J_R \Rightarrow 1 = e + (1-e)$ with $e \in I$, $1-e \in J$
$\Rightarrow e(1-e) = (1-e)e \in I \cap J = 0 \Rightarrow e(1-e) = 0 = (e-1)e = 0$
$\Rightarrow e = e^2$
Finally: $\forall x \in I.\ x = ex + (1-e)x \overset{(1-e)x = 0}{\Rightarrow} x = ex$, 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.
$\exists I \leq R_R.\ R_R = J(R)_R \oplus I_R$ [T 2.12 (c)] If $J(R) \neq 0$, then $I \subsetneq R$
$\Rightarrow$ there exists a maximal right ideal $I \subseteq M \subsetneq R$
$\Rightarrow J(R) \subsetneq M$. ↯

(b) $\Rightarrow$ (c): ✓

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

(2) Every minimal $0 \neq I \leq R_R$ is a direct summand of R_R.
[$I \neq 0$, but $J(R) = 0 \Rightarrow \exists$ maximal right ideal $M \leq R_R$ s.t. $I \not\subseteq M \Rightarrow I + M = R$. Since I is simple, $I \cap M = 0$].

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

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

$$B_n = A_n \oplus \underbrace{(B_n \cap C_n)}_{=: B_{n+1} \subsetneq B_n} \quad \text{(because } A_n \leq B_n\text{)}$$

This gives us A_n. Note $B_1 \supsetneq B_2 \supsetneq \cdots$ 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 $J(R)^i / J(R)^{i+1}$ for $i = 0, 1, \ldots$

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 $M \supseteq MJ(R) \supseteq MJ(R)^2 \supseteq \cdots MJ(R)^n = 0$.
It suffices to show $MJ(R)^i/MJ(R)^{i+1}$ has a composition series $(i = 0, \ldots, n-1)$.

Now $MJ(R)^i/MJ(R)^{i+1}$ 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 $MJ(R)^i/MJ(R)^{i+1}$, 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.
($\Rightarrow$): R right artinian $\Rightarrow$ R semiprimary L3.10
$\overset{3.11}{\Rightarrow}$ R_R is noetherian
In particular: R right artinian $\Rightarrow$ R right noetherian

Corollary 3.13: If R_R is right artinian and M-Mod-R is Finitely generated, then $\ell(M) < \infty$.

3.3 Nakayama's Lemma

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

Proof: Let $M = \langle m_1, \ldots, m_k \rangle_R$ with k minimal. If $k \geq 1$, we can write $m_k = m_1 r_1 + \cdots + m_{k-1} r_{k-1}$ with $r_i \in J(R)$.

$\Rightarrow m_k(1-r_k) = m_1 r_1 + \cdots + m_{k-1} r_{k-1}$

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

Since $1-r_k \in R^\times$, also $m_k \in \langle m_1, \ldots, m_{k-1} \rangle_R$ ↯ k min. ▨

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 $\overline{M} = M/MJ(R)$ is annihilated by $J(R)$, so naturally an $\overline{R} := R/RJ(R)$-module.

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

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

If $f: M \longrightarrow M'$ is an R-hom, then $f(M(J(R))) \leq M'J(R)$, so it induces $\overline{f}$:

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

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

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

3.4. Group Algebras (w/o proof)

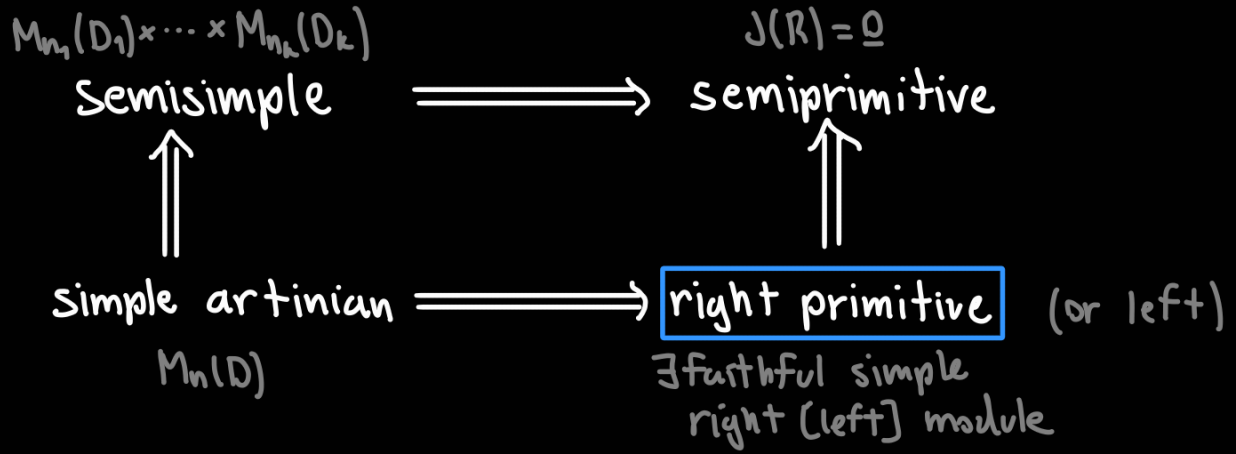
K Field. If G is infinite, then $K[G]$ is not semisimple [P2.24].

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 $\mathrm{char}\, K = 0$

4. Structure of Primitive rings & Jacobson Density Theorem



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

· left primitive $\not\Longleftrightarrow$ right primitive [Bergman 1964]

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

Proposition 4.1: Every semiprimitive 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 $R \to R_i$ surjective

Proof: $0 = J(R) = \bigcap_{\substack{M \in \text{Mod-}R \\ M \text{ simple}}} \text{ann}(M_R)$

$\Rightarrow R \hookrightarrow \prod_{M_R \text{ simple}} R/\text{ann}(M)$, and $R \to R/\text{ann}(R)$ is surjective ▨

($R/\text{ann}(M)$: right primitive)

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

M_R f.g., $MJ(R)=M \Rightarrow M=0$ November 6, 2025

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

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

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

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

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

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

Example [A non-simple left-primitive ring]:
D div. ring, V_D vector space, $R := \mathrm{End}(V_D)$ ($\cong$ column finite 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. $\forall r \in V$. $f(r) = 0 \Rightarrow f = 0$
So $\mathrm{ann}({}_RV) = \underline{0}$.
$\Rightarrow R$ is left primitive
If $\dim V_D = \infty$, then R is not simple.
$I := \{f \in R \mid \dim(\mathrm{im} f) < \infty\} \trianglelefteq R$ ($\cong$ 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 ($f \cdot m := f(m)$ for $f \in E, m \in M$), and $f(mr) = f(m)r$, so M is an (E,R)-module.

· If ${}_RM \in R\text{-mod}$, $E := \text{End}({}_RM)$, then ${}_RM_{E^{op}}$ is an (R, E^{op})-bimodule: $m \cdot (f \circ_{op} g) = (f \circ_{op} g)m = (g \circ f)(m) = g(f)(m)$
$g(m \cdot f) = (m \cdot f) \cdot g$

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

· ⚠ If $M_R \in \text{Mod-}R$, then ${}_{R^{op}}M \in R^{op}\text{-Mod}$ via $r \cdot m = mr$. In general this is not a bimodule structure!

[Suppose $(am)b = a(mb)$ differ i.g., e.g. if $\text{ann}(m) = 0$ and $ab \neq ba$
mab mba]

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 $\forall f \in E. \forall m_1, \dots, m_k \in M. \exists r \in R. \forall i: rm_i = f(m_i)$.
[Note: $R \to E$, $r \mapsto (m \mapsto rm)$ 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. $(v_1, \dots, v_k) \in V^k$. $\forall (v_1', \dots, v_k') \in V^k \exists r \in R. \forall i. rv_i = v_i'$.

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 $E := \mathrm{End}(V_D)$ acts densely.
Fix a D-basis $(e_1, \dots, e_n)$ of V.
Suppose $R \subseteq E$ acts densely on V, let $f \in E$.
$\Rightarrow \exists r \in R \; \forall 1 \le i \le n . \; r(e_i) = f(e_i) \Rightarrow r = f \in S$. ▨

Theorem 4.4 [Jacobson Density Theorem/Chevalley-Jacobson Theorem]:
Let R be a ring, ${}_R M$ a semisimple left R-module, $S = \mathrm{End}({}_R M)^{op}$. Then R acts densely on M_S.
A different proof from ours is presented in Brešar's book.

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

Proof: E-submodules are R-submodules, because $R \to E$, $r \mapsto (m \mapsto rm)$ is a ring hom.
Let ${}_R N \subseteq {}_R M$ be an R-submodule, and ${}_R N'$ s.t. ${}_R M = {}_R N \oplus {}_R N'$ [T2.11(c)]
Define: $\pi : {}_R M \to {}_R M$ s.t. $\pi|_N = id$, $\pi|_{N'} = 0$ (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
$\forall f \in E \; \forall n \in N . \; f(n) = f(\pi(n)) = f(n \cdot \pi) \overset{\text{bimodule structure}}{=} f(n) \cdot \pi = \pi(f(n))$

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

Proof of Theorem 4.4: $E := \mathrm{End}(M_S)$. Let $f \in E$, $m_1, \dots, m_k \in M$.
Show: $\exists r \in R . \forall i . \; f(m_i) = rm_i$

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

$$ \tilde{S} := \mathrm{End}({}_R\tilde{M}) = \mathrm{End}({}_R M^k) = M_k(\mathrm{End}({}_R M)^{op}) = M_k(S) $$
(matrix ring)
Define: $\tilde{f} : \tilde{M} \to \tilde{M}$, $(x_1, \dots, x_k) \mapsto (f(x_1), \dots, f(x_k))$

Claim: $\tilde{\varphi} \in \mathrm{End}(\tilde{M}_{\tilde{S}})$:

Proof of claim: $\tilde{\varphi}(\underline{x}+\underline{y}) = \tilde{\varphi}(\underline{x}) + \tilde{\varphi}(\underline{y})$ ✓ $(\underline{x},\underline{y} \in \tilde{M})$

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

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

$$\tilde{\varphi}(\underline{x}s) = \tilde{\varphi}\left(\sum_{i=1}^{k} x_i s_{i1}, \dots, \sum_{i=1}^{k} x_i s_{ik} \right)$$

$$= \left(\varphi\left(\sum_{i=1}^{k} x_i s_{i1}\right), \dots, \varphi\left(\sum_{i=1}^{k} x_i s_{ik}\right) \right)$$

$$= \left(\sum_{i=1}^{k} \varphi(x_i) s_{i1}, \dots, \sum_{i=1}^{k} \varphi(x_i) s_{ik} \right)$$

$$= (\varphi(x_1),\dots,\varphi(x_k))\, s = \tilde{\varphi}(\underline{x})s$$ □ (claim)

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

$\overset{L4.5}{\Rightarrow}$ ${}_R\tilde{C}$ is an $\mathrm{End}(\tilde{M}_{\tilde{S}})$-submodule of ${}_R\tilde{M}$.

$\Rightarrow \tilde{\varphi}(\tilde{C}) \le \tilde{C} \Rightarrow \varphi(m_1,\dots,m_k) = (\varphi(m_1),\dots,\varphi(m_k)) = r(m_1,\dots,m_k)$

for some $r \in R$. So $\varphi(m_i) = r m_i$ $\forall i$. ▨

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

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

Let $r \in R$ s.t. $\varphi(m_i) = r m_i$ $\forall i$ [T4.4].

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

$$\Rightarrow \varphi(m) = \varphi\left(\sum_{i=1}^{k} m_i s_i\right) = \sum_{i=1}^{k} \varphi(m_i) s_i = \sum_{i=1}^{k} (r m_i) s_i \overset{(R,S)\text{-bimodule}}{=} \sum_{i=1}^{k} r(m_i s_i) = rm$$ ▨

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

Theorem [Structure Theorem For Left Primitive Rings]:
Let R be left primitive with faithful simple left R-module V and $D := \mathrm{End}({}_R V)^{op}$. Then R embeds as a dense ring of linear operators, $R \hookrightarrow \mathrm{End}(V_D)$, 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. $R_n \to M_n(D)$.

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

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

Case 1: $n := \dim V_D < \infty$
Then $R \hookrightarrow \mathrm{End}(V_D)$ is surjective [C4.6], so $R \equiv \mathrm{End}(V_D) \cong M_n(D)$.
In particular, R is artinian.

Case 2: $\dim V_D = \infty$, choose D-lin. independent $v_1, v_2, v_3, \ldots$
Let $W_n := \langle v_1, \ldots, v_n \rangle$, $R_n := \{ r \in R \mid rW \subseteq W \}$
$I_n := \{ r \in R \mid rW = 0 \}$
$\Rightarrow R_n \subseteq R$ is a subring, $I_n \subseteq R_n$
$R_n W_n \subseteq W_n \Rightarrow W_n$ is an R_n-module and $I_n = \mathrm{ann}({}_{R_n} W)$
$\Rightarrow \varphi_n : R_n \to \mathrm{End}(W_{n D}) \cong M_n(D)$ is a ring hom. with $\ker \varphi_n = I_n$.
For any $w_1, \ldots, w_n \in W_n$. $\exists r \in R$. $r v_i = w_i$ [T4.4]
$\overset{\text{restrict}}{\Rightarrow} \varphi_n$ surjective
Claim: R is not left artinian
I_n is a left ideal of R
$\exists r \in R$: $r v_1 = \cdots = r v_n = 0$, $r v_{n+1} \neq 0 \Rightarrow r \in I_n \setminus I_{n+1}$
$\Rightarrow I_1 \supsetneq I_2 \supsetneq \cdots$

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", $\Rightarrow$ T4.7)

4.2. Application: Jacobson's Commutativity Theorem

(after Herstein, 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 $x^2 = x$.

$((\mathbb{Z}/2\mathbb{Z})^X \rightarrow X$ set, $\mathcal{P}(X)$ powerset $\quad X \cdot Y = X \cap Y$, $\quad X + Y = X \setminus Y \cup Y \setminus X$

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

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

$\Rightarrow xy + yx = 0 \overset{-1=1}{\Rightarrow} xy = yx$

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

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

[Since $0 = e(1-e) = (1-e)e$. $\forall r \in R$:

$er(1-e) = (er(1-e))^3 = 0 \Rightarrow er = ere$

$(1-e)re = ((1-e)re)^3 = 0 \Rightarrow re = ere$ $\quad = e \in Z(R)$]

- $(r^2)^2 = r^4 = r^2 \Rightarrow \forall r \in R.\ r^2$ idempotent $\Rightarrow r^2 \in Z(R)$
- $1 + r = (1+r)^3 = 1 + 3r + 3r^2 + r^3 \Rightarrow 3r = -3r^2 \in Z(R)$
- $(1+r)^2, r^2 \in Z(R) \Rightarrow (1+r)^2 - 1 - \underset{\| r}{r^2} = 2r \in Z(R)$
- $\Rightarrow r = 3r - 2r \in Z(R)$

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

Proof: Let $x \in J(R)$, $n>1$ s.t. $x^n=x$.
$\Rightarrow 0=x-x^n=(1-x^{n-1})x \Rightarrow x=0$ ▨
($1-x^{n-1} \in R^\times$ $(n\geq 2)$)

So $R \hookrightarrow \prod_{\substack{I \text{ left primitive} \\ \text{ideal of } R}} R/I$, each R/I retains the assumption 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], $R \hookrightarrow \mathrm{End}(V_D)$ densely with D a division ring. (V_D: faithful simple R-module) We show $\dim V_D=1$, then $R \cong \mathrm{End}(D_D) \cong D$.
Suppose $v,w \in V_D$ are D-linearly independent.
$\overset{T4.4}{\Rightarrow} \exists r \in R.\ rv=w,\ rw=0$
$\Rightarrow \forall n \geq 1.\ r^n v=0$ ↯ $r^{n(r)}=r$ ▨

Lemma 4.12 [Herstein]: Let D be a division ring with $\mathrm{char}D=p>0$. Suppose $a \in D \setminus Z(D)$ s.t. $a^{p^n}=a$ for some $n \geq 1$.
$\Rightarrow \exists x \in D, i>1.\ a^i \neq a$ 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 $\mathrm{char}D=p>0$, p prime.

wlog $\mathbb{F}_p \subseteq D$ ($\mathbb{F}_p \subseteq Z(D)$ because everything commutes with scalars)
Suppose there exists $a \in D \setminus \mathbb{F}_p$. Then $\mathbb{F}_p[a] \subseteq D$ is a finite field (since $a^{n(a)} - a = 0$) 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 $R := \mathbb{F}_p\langle a^k x^\ell \mid 0 \leq k \leq p^{n-1},\ 0 \leq \ell < m\rangle$ 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 $\overset{T4.13}{\Rightarrow}$ D field $\Rightarrow x, a$ commute ↯ ▨
↳exercise class

November 13, 2025

Proof of 4.12: Define $\delta : D \to D,\ x \mapsto [a, x] := ax - xa$. 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. $a^{p^m} = a \Rightarrow k \cong \mathbb{F}_{p^m}$ ($\mathbb{F}_{p^\ell} = \{c \in \mathbb{F}_p \mid c^{p^\ell} = c\}$)

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

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

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 $\mathrm{End}_k(D)$)

$f = \prod_{b \in k} (t - b)$. Let $g = t(t - b_1)(t - b_2) \cdots (t - b_\ell)$ with ℓ minimal s.t. $g(\delta) = 0$.
$\delta \neq 0 \Rightarrow \ell \geq 1 \Rightarrow \delta(\delta - b_1) \cdots (\delta - b_{\ell-1}) \neq 0$
($b_1, b_{\ell-1} \in k$)

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 δ 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 $b \neq 0$. ▨

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 $\mu_n^*(\bar{\mathbb{Q}}) := \{\zeta \in \mu_n(\bar{\mathbb{Q}}) \mid \zeta^m \neq 1 \text{ for } m \mid n, m \neq n\}$ 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 $m \mid n$, then $x^m - 1 \mid x^n - 1$ in $\mathbb{Z}[x]$.
(2) $\Phi_n(x) \in \mathbb{Z}[x]$ and $\Phi_n(x) \mid x^n - 1$ in $\mathbb{Z}[x]$.

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

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

$$\frac{x^n - 1}{F} = \prod_{\substack{\zeta \in \mu_n(\bar{\mathbb{Q}}) \\ \zeta \notin \mu_m^*(\bar{\mathbb{Q}}) \\ m \mid n,\, m \neq n}} (x - \zeta) = \prod_{\zeta \in \mu_n^*(\bar{\mathbb{Q}})} (x - \zeta) = \Phi_n(x) \quad \in \mathbb{Z}[x]$$

▨

Remark: Φ_n is irreducible.

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

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

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

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

where $a_1, \dots, a_l$ represent the nontrivial conjugacy classes in $D^\times$.
Here $|C(a_i)^\times| = q^{n_i} - 1$ for $1 < n_i < n$ since $C(a_i)$ is a division ring with some $n_i = \dim_F C(a_i) < n$.

Note $\frac{x^n - 1}{x^{n_i} - 1} = \Phi_n(x) H_i(x)$ 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 $H_i(q) \in \mathbb{Z}$)

$$\Rightarrow \Phi_n(q) \mid_{\mathbb{Z}} \frac{q^n - 1}{q^{n_i} - 1}.$$

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

But $\Phi_n(q) = \prod_{\zeta \in \mu_n^*(\mathbb{C})} (q - \zeta)$ 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 $G \leq K^\times$, G finite
Claim: G is cyclic ($G \cong \mathbb{Z}/n\mathbb{Z}$ for some n)

used in proof of 4.12.

$$(G, \cdot) \cong (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_d\mathbb{Z}) \qquad 1 \neq n_1 \mid n_2 \mid \cdots \mid n_d$$

$\Rightarrow \forall g \in G.\ g^{n_d} = 1 \Rightarrow \forall g \in G.$ g is a root of $x^{n_d} - 1$ in $K[x]$
$\Rightarrow |G| \leq n_d$
$\vdots$
$n_1 \cdots n_d$

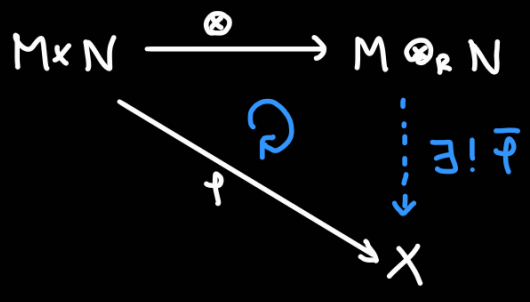
5. Tensor Products

R ring

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

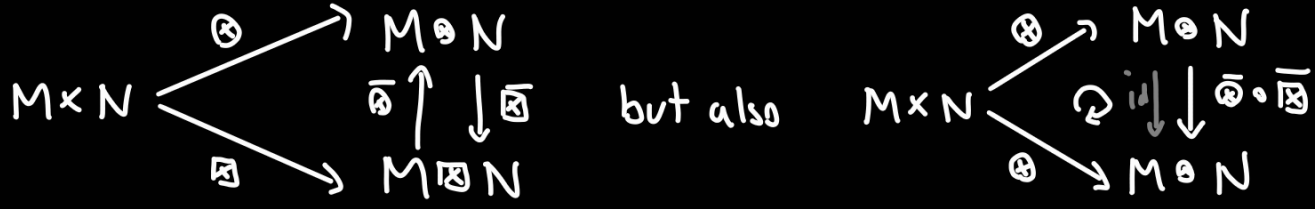
- $f(m+m', n) = f(m, n) + f(m', n)$
- $f(m, n+n') = f(m, n) + f(m, n')$
- $f(mr, n) = f(m, rn)$

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 $f: M \times N \longrightarrow X$ is R-balanced, there exists a unique group homomorphism ($= \mathbb{Z}$-hom) $\bar{f}: M \otimes_R N \longrightarrow X$ s.t. $f = \bar{f} \circ \otimes$



<u>$(M \otimes_R N, \otimes)$ is unique up to unique iso:</u>

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



uniqueness $\Rightarrow$ $\quad id_{M \otimes N} = \bar{\otimes} \circ \bar{\boxtimes}$

By simmetry: $\quad id_{M \otimes N} = \bar{\boxtimes} \circ \bar{\otimes}$.

<u>Existance:</u> 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 $\{\forall m, m' \in M, n, n' \in N, r \in R\}$:

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

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

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

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

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

If $f : M_R \longrightarrow M'_R$, $g : {}_R N \longrightarrow {}_R N'$ are module homomorphisms, then $(f,g) : M \times N \longrightarrow M' \otimes_R N'$, $(m,n) \mapsto f(m) \otimes g(n)$ is R-balanced. [$f(mr) \otimes g(n) = f(m)r \otimes g(n) = f(m) \otimes rg(n) = f(m) \otimes g(rn)$], and it induces a unique $f \otimes g : M \otimes N \longrightarrow M' \otimes N'$

$$m \otimes n \longmapsto f(m) \otimes g(n)$$

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

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

Bimodules: If ${}_S M_R$, ${}_R N_T$ are (S,R) resp. (R,T)-bimodules, then ${}_S M_R \otimes_R N_T = {}_S(M \otimes_R N)_T$ is a (S,T)-bimodule via $s(m \otimes n)t := (sm) \otimes (nt)$.

Remark: (1) If M_R, ${}_R N$ are just modules, they are ${}_{\mathbb{Z}} M_R$, ${}_R N_{\mathbb{Z}}$ 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: $M, N, X \in R\text{-Mod}$

$f: M \times N \to R$ is R-bilinear if it is R-balanced & $f(rm, n) = rf(m,n) = f(m, rn)$ $\forall m \in M. \forall n \in N. \forall r \in R.$

Then $M \otimes_R N$ satisfies the analogous UP wrt. R-bilinear maps:
$f: M \times N \longrightarrow X$ R-bilinear $\Rightarrow \exists! \bar{f} \in \mathrm{Hom}(M \otimes_R N, X_R)$. $\bar{f} \circ \otimes = f$.

$\otimes$ - Hom Adjunction:

Motivation/Comparison:

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

$f: A \times B \longrightarrow C \longmapsto (a \mapsto f_a : B \to C)$, $f_a(b) = f(a,b)$

$(a,b) \mapsto (f(a))(b) \longleftarrow f$

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

$f_* \qquad t \longmapsto f \circ t$

$f: B \to B'$ $\quad : \mathrm{Hom}(B', C) \to \mathrm{Hom}(B, C)$, $(g \circ \varphi)^* = f^* \circ \varphi^*$

f^* $\qquad \varphi \longmapsto \varphi \circ f$

Two (bi)functors: $- \times - : \underline{\mathrm{Set}} \times \underline{\mathrm{Set}} \longrightarrow \underline{\mathrm{Set}}$

$\mathrm{Hom}(-,-) : \underline{\mathrm{Set}}^{op} \times \underline{\mathrm{Set}} \longrightarrow \underline{\mathrm{Set}}$

$- \times B : \underline{\mathrm{Set}} \to \underline{\mathrm{Set}}$, $\mathrm{Hom}(B, -) : \underline{\mathrm{Set}} \longrightarrow \underline{\mathrm{Set}}$

$\circledast$: $- \times B$ is left adjoint to $\mathrm{Hom}(B, -)$

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

For (bi)modules: First note: if M_R, N_R are modules $\mathrm{Hom}(M_R, N_R)$ is in general only an Abelian group.
[$(fr)(m) = f(mr)$ does not work]. But:

- If ${}_S M_R$ is a bimodule, $\mathrm{Hom}({}_S M_R, N_R)_S$ is a right S-module via $(fs)(m) := f(sm)$.

contravariant

•) If ${}_T N_R$ is a (T,R)-bimodule, ${}_T\mathrm{Hom}({}_T M_R, {}_T N_R)$ is a left T-module via $(tf)(m) := tf(m)$. (covariant; t acts on the N)

⊗-Hom adjunction: ${}_R M_S$ bimodule

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

$\mathrm{Hom}_S({}_S M, -) : \underline{\mathrm{Mod}}\text{-}S \to \underline{\mathrm{Ab}}$

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

$$\mathrm{Hom}_S(X_R \otimes_R {}_R M_S, Y_S) \cong \mathrm{Hom}_R(X_R, \mathrm{Hom}({}_R M_S, Y_S)_R)$$

$$f \longmapsto (x \mapsto f_x),\ f_x(m) = f(x \otimes m)$$

$$x \otimes m \mapsto g(x)(m) \longleftarrow\!\shortmid\ g$$

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: ⊗ commutes with colimits (direct sum, cokernel)

If $A_R \xrightarrow{f} B_R \xrightarrow{g} C_R \to 0$ is exact, then so is

$A \otimes_R M \to B \otimes_R M \to C \otimes_R M \to 0$, i.e. $- \otimes_R M$ is right exact

$a \otimes m \mapsto f(a) \otimes m$

$b \otimes m \mapsto g(b) \otimes m$

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

Proof sketch: First verify:

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

$\Leftrightarrow \forall X \in \mathrm{Mod}\text{-}R : 0 \to \mathrm{Hom}(X_R, N_R) \xrightarrow{f_*} \mathrm{Hom}(X_R, M_R) \xrightarrow{g_*} \mathrm{Hom}(X_R, K_R)$ exact

$f_*(t) = f \circ t$, $g_*(\tau) = g \circ \tau$

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

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

$g^*(\rho) = \rho \circ g$, $f^*(\tau) = \tau \circ f$

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

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

Consider $A \otimes_R X \xrightarrow{f \otimes id_X} B \otimes_R X \xrightarrow{g \otimes id_X} C \otimes_R X \longrightarrow 0$ $(- \otimes_R X)$
Apply $\mathrm{Hom}_{\mathbb{Z}}(-, Y)$, $Y \in Ab$

$$\begin{array}{ccccccc}
0 \to \mathrm{Hom}_{\mathbb{Z}}(C \otimes_R X_{\mathbb{Z}}, Y_{\mathbb{Z}}) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(B \otimes_R X_{\mathbb{Z}}, Y_{\mathbb{Z}}) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(C \otimes_R X_{\mathbb{Z}}, Y_{\mathbb{Z}}) \\
\otimes\text{-Hom adj} \downarrow \wr & \circlearrowright & \downarrow \wr & \circlearrowright & \downarrow \wr \\
0 \to \mathrm{Hom}_R({}_R X, {}_R\mathrm{Hom}_{\mathbb{Z}}(C_R, Y)) & \longrightarrow & \mathrm{Hom}_R({}_R X, {}_R\mathrm{Hom}(B, Y)) & \longrightarrow & \mathrm{Hom}_R({}_R X, {}_R\mathrm{Hom}(A, Y))
\end{array}$$

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

Basic properties:

November 20, 2025

${}_U K_T, {}_T N_R, {}_R M_S$ bimodules

(1) $R \otimes_R M \cong M$, $r \otimes m \longmapsto rm$, $1 \otimes m \longleftarrow\!\shortmid\, m$ (canonical)
$M \otimes_S S \cong M$ canonically

(2) $\left(\bigoplus_{i \in I} N_i\right) \otimes_R M \cong \bigoplus_{i \in I} (N_i \otimes_R M)$ (canonicaly)
$N_i \in \mathrm{Mod}\text{-}R$

$$(n_i)_{i \in I} \otimes m \longmapsto (n_i \otimes m)_{i \in I}$$
$$\sum_{i \in I} (\widetilde{n_j})_{j \in I} \otimes m_i \longleftarrow\!\shortmid\, (n_i \otimes m_i)_{i \in I}$$
$\hookrightarrow \widetilde{n_j} = \begin{cases} n_i & \text{for } i = j \\ 0 & \text{for } i \neq j \end{cases}$

(3) $K \otimes_T (N \otimes_R M) \cong (K \otimes_T N) \otimes_R M$ (canonically)

(4) If R is commutative: $M \otimes_R N \cong N \otimes_R M$ (canonically)

As a consequence of (1), (2) if $F \cong \bigoplus_{i \in I} e_i R$ is free $\left(F \cong R_R^{(I)}\right)$:

$$F \otimes_R M = \left(\bigoplus_{i \in I} e_i R\right) \otimes_R M = \bigoplus_{i \in I} (e_i R \otimes_R M) \cong M^{(I)}$$

Lemma: If F_R is Free, $f: {}_R M \longrightarrow {}_R N$ injective, then $id_F \otimes f : F \otimes_R M \longrightarrow F \otimes_R N$ is injective.
So: $F \otimes_R -$ is exact; applies to all modules when R is a div. ring (in particular, a Field) R div ring $\Rightarrow$ F_R free

Proof: $F = \bigoplus_{i \in I} e_i R$; each element of $F \otimes_R M$ has a representative $\sum_{i \in I} e_i \otimes m_i$ with unique $m_i \in M$, and similarly for N.

$$0 = (id_F \otimes f)\left(\sum_{i \in I} e_i \otimes m_i\right) = \sum_{i \in I} e_i \otimes f(m_i) \Rightarrow f(m_i) = 0 \quad \forall i$$
($e_i \otimes f(m_i) \in F \otimes_R N$)
$$\Rightarrow m_i = 0 \quad \forall i$$
$$\Rightarrow id_F \otimes f \text{ is injective} \qquad \blacksquare$$

If $F = \bigoplus_{i \in I} e_i R$, $F' = \bigoplus_{j \in J} R e_j$ Free, then

$$F \otimes_R F \cong \bigoplus_{\substack{i \in I \\ j \in J}} \underbrace{(e_i R \otimes R e_j)}_{\cong R} \cong R^{(I \times J)} \quad \text{(as abelian groups)}$$

If R is commutative $\Rightarrow$ F is free with R-basis $\{e_i \otimes e_j \mid i \in I, j \in J\}$.
In particular: If $R = K$ is a Field, V, W vector spaces:

$$\dim(V \otimes_K W) = \dim(V) \cdot \dim(W).$$

6 Tensor Products of Algebras

k commutative ring, R, S k-algebras, $\otimes_k = \otimes$
[i.e. R ring & k-module s.t. $\lambda(rr') = (\lambda r)r' = r(\lambda r') \ \forall r,r' \in R, \lambda \in k$
$\Leftrightarrow$ there is a ring hom. $\varepsilon : k \to Z(R)$]

Proposition 6.1: There is a unique k-algebra structure on $R \otimes S$ that satisfies $(r \otimes s)(r' \otimes s') = (rr') \otimes (ss') \ \forall r,r' \in R. \forall s,s' \in S.$

Proof: Uniqueness: clear, since $R \otimes S = {}_k\langle r \otimes s \mid r \in R, s \in S \rangle$
Existence: Step 1: Fix r, s. Then $R \times S \to R \otimes S$, $(r', s') \mapsto rr' \otimes ss'$ is k-bilinear.
$\Rightarrow \exists \varphi_{r,s} : R \otimes S \to R \otimes S$, $r' \otimes s' \mapsto rr' \otimes ss'$ (k-hom).
Step 2: $R \times S \to \mathrm{Hom}_k(R \otimes S, R \otimes S)$, $(r,s) \mapsto \varphi_{r,s}$ is k-bilinear

$$\left[\begin{array}{l} \text{e.g. } \forall r, r'' \in R, \lambda \in k: \ \varphi_{r+\lambda r'', s}(r' \otimes s') = (r + \lambda r'')r' \otimes ss' \\ \qquad = rr' \otimes ss' + \lambda(r''r \otimes ss') \\ \qquad = \varphi_{r,s}(r' \otimes s') + \lambda \varphi_{r'',s}(r' \otimes s') \\ \Rightarrow \varphi_{r+\lambda r'', s} = \varphi_{r,s} + \lambda \varphi_{r'',s} \end{array}\right]$$

$\Rightarrow \exists \Phi : R \otimes S \to \mathrm{Hom}(R \otimes S, R \otimes S)$, $r \otimes s \mapsto \varphi_{r,s}$ (k-hom)
Now: $\mathrm{Hom}(R \otimes S, \mathrm{Hom}_R(R \otimes S, R \otimes S)) \cong \mathrm{Hom}((R \otimes S) \otimes (R \otimes S), R \otimes S)$
($\otimes$-Hom adjunction) gives $(r \otimes s) \otimes (r' \otimes s') \mapsto \varphi_{r,s}(r' \otimes s') = rr' \otimes ss'$. ✓ ▨

Remark: (1) For $R \in k\text{-Alg}$, $R \cong k \otimes_k R$, $r \mapsto 1 \otimes r$ and $R \cong R \otimes_k k$, $r \mapsto r \otimes 1$ are k-algebra isomorphisms.

(2) If R, S are k-algebras, $R \to R \otimes_k S$, $r \mapsto r \otimes 1_S$, $S \to R \otimes_k S$, $s \mapsto 1 \otimes s$ are k-algebra hom.

(3) If R, S, T are k-algebras, $R \otimes S \cong S \otimes R$, $r \otimes s \mapsto s \otimes r$
$(R \otimes S) \otimes T \cong R \otimes (S \otimes T)$ are k-algebra isomorphisms.

Observe: $(r\otimes 1)(1\otimes s) = r\otimes s = (1\otimes s)(r\otimes 1)$, so in $R\otimes_k S$, the images of R and S commute.

UP: If R, S are k-algebras, and $f: R\to T$, $g: S\to T$ are k-algebra hom. s.t. $\forall r\in R.\ \forall s\in S.\ f(r)g(s) = g(s)f(r)$, then there exists a unique k-algebra hom. $\gamma: R\otimes_k S \longrightarrow T$ s.t. $\forall r\in R.\ \forall s\in S.\ \gamma(r\otimes s) = f(r)g(s)$.

[By UP for tensor products of modules, there is a unique such k-hom γ, because $(r,s)\longmapsto f(r)g(s)$ is k-bilinear. Observe that this map respects multiplication.]

Example: R k-algebra

(1) $R\otimes_k M_n(k) \cong M_n(R)$

[E_{ij}, $1\le i,j\le n$ is a k-basis of $M_n(k)$, so

$$R\otimes M_n(k) = R\otimes \bigoplus_{i,j=1}^{n} k E_{ij} \cong \bigoplus_{i,j=1}^{n} (R\otimes_k k E_{ij})$$

$\Rightarrow$ elements of $R\otimes M_n(k)$ have a unique expression

$\bigoplus_{i,j=1}^{n} r_{ij}\otimes E_{ij}$, $r_{ij}\in R$

$R\otimes M_n(k)$ $\longrightarrow$ $M_n(R)$

Mapping $r_{ij}\otimes E_{ij}$ to $r_{ij}E_{ij}$ gives the isomorphism.

(2) $M_n(k)\otimes M_m(k) \cong M_n(M_m(k)) \cong M_{nm}(k)$

$E_{ij}\otimes E_{st} \longmapsto E_{i+n(s-1),\, j+n(t-1)}$

$1\le i,j\le m$, $1\le s,t\le n$

Extension of Scalars

k comm. ring, L comm. k-algebra

•) Using $k\to L$ every L-algebra is a k-algebra (restriction of scalars)

• If R is a k-algebra, then $R \otimes_k L$ is an L-algebra (extension of scalars), since $(r \otimes 1)(1 \otimes \lambda) = r \otimes \lambda = (1 \otimes \lambda)(r \otimes 1)$.

Example: $M_n(k) \otimes_k L \cong M_n(L)$ (as L-algebras)
$\mathbb{Z}[x] \otimes_{\mathbb{Z}} k \cong k[x]$
$\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \cong M_2(\mathbb{C})$ exercise

Proposition 6.2:
(1) If R is a k-algebra, S an L-algebra, then

$$\mathrm{Hom}_{L\text{-}\underline{\mathrm{Alg}}}(R \otimes_k L, S) \cong \mathrm{Hom}_{k\text{-}\underline{\mathrm{Alg}}}(R, S)$$

(2) If R_1, R_2 are k-algebras, $(R_1 \otimes_k L) \otimes_L (R_2 \otimes_k L) \cong (R_1 \otimes_k R_2) \otimes_k L$.

Proof: (1) By $\otimes$-Hom adjunction

$$\mathrm{Hom}_{L\text{-}\underline{\mathrm{Mod}}}(R \otimes_k L_L, S_L) \overset{(*)}{\cong} \mathrm{Hom}_{k\text{-}\underline{\mathrm{Mod}}}(R, \mathrm{Hom}_L(L_L, S_L)) \overset{(**)}{\cong} \mathrm{Hom}_{k\text{-}\underline{\mathrm{Mod}}}(R, S)$$

$\mathrm{Hom}_L(L_L, S_L) \cong S_L$ via $\varphi \mapsto \varphi(1)$

via: $\gamma \overset{(*)}{\longmapsto} (r \longmapsto \gamma_r)$, $\gamma_r(l) = \gamma(r \otimes l)$
$(r \longmapsto \varphi) \overset{(**)}{\longmapsto} (r \longmapsto \varphi(1))$

together: $\gamma \longmapsto (r \longmapsto \gamma(r \otimes 1))$

This restricts to $\mathrm{Hom}_{L\text{-}\underline{\mathrm{Alg}}}(R \otimes_k L, S_L) \cong \mathrm{Hom}_{k\text{-}\underline{\mathrm{Alg}}}(R, S)$

Converse direction: given $\gamma : R \longrightarrow S$, $\gamma \otimes \mathrm{id} : R \otimes_k L \cong S \otimes_k L \cong S$
$r \otimes l \longmapsto \gamma(r) \otimes l \mapsto \gamma(r) l$

$$\begin{aligned}(2)\ (R_1 \otimes_k L) \otimes_L (R_2 \otimes_k L) &\cong (R_1 \otimes_k L) \otimes_L (L \otimes_k R_2) \\ &\cong R_1 \otimes_k (L \otimes_L L) \otimes_k R_2 \\ &\cong R_1 \otimes_k L \otimes_k R_2 \\ &\cong (R_1 \otimes_k R_2) \otimes_k L\end{aligned}$$

Bimodules again: R, S rings ($= \mathbb{Z}$-algebras)

$$\{(R,S)\text{-bimodules}\} \cong \underline{\text{Mod}}\text{-}R^{op} \otimes_{\mathbb{Z}} S$$

- If ${}_R M_S$ is a bimodule, there are structure homs. $\varepsilon_R : R \to \text{End}(M_{\mathbb{Z}})$, $\varepsilon_S : S^{op} \to \text{End}(M_{\mathbb{Z}})$.

Bimodule property: $\varepsilon_R(r) \cdot \varepsilon_S(s) = \varepsilon_S(s) \cdot \varepsilon_R(r) \quad \forall r \in R \; \forall s \in S$

$(r(ms) = (rm)s)$

$\overset{\text{UP-}\otimes}{\Rightarrow}$ $\exists$ unique ring hom. $S^{op} \otimes_{\mathbb{Z}} R \to \text{End}(M_{\mathbb{Z}})$, giving a right $R^{op} \otimes_{\mathbb{Z}} S$ module structure: $S^{op} \otimes_{\mathbb{Z}} R = (S \otimes_{\mathbb{Z}} R^{op})^{op}$

$m(r \otimes s) = rms$

[More „pedestrian": $\mu_m : R^{op} \times S \to M$, $(r,s) \mapsto rms$ is $R^{op} \times S$-balanced. Induces: $(R^{op} \otimes S) \times M \to M$, $(r \otimes s, m) \mapsto rms$]

- Other direction: $j_R : R^{op} \to R^{op} \otimes_{\mathbb{Z}} S$, $r \mapsto r \otimes 1$,
  $j_S : S \to R^{op} \otimes_{\mathbb{Z}} S$, $s \mapsto 1 \otimes s$.

If $M \in \underline{\text{Mod}}\text{-}R^{op} \otimes_{\mathbb{Z}} S$, restriction of scalars gives a left R-module, right S-module structure. Images of j_R & j_S commute $\Rightarrow$ bimodule structure.

[$(rm)s = (m(r \otimes 1))(1 \otimes s) = m((r \otimes 1)(1 \otimes s)) = m(r \otimes s) = m(1 \otimes s)(r \otimes 1)$
$= \ldots = r(ms)$]

6.1. Central Algebras

Now: k field, $\otimes = \otimes_k$

If $Q \neq R$ is a k-algebra, the structure hom. $k \to Z(R)$ is injective.

WLOG: $k \subseteq Z(R)$

Definition: A central k-algebra is a k-algebra $R \neq Q$ s.t. $Z(R) = k$.

Example: $M_n(k)$,
$\mathbb{H}$ is a central $\mathbb{R}$-alg
$\mathbb{C}$ is not a central $\mathbb{R}$-algebra
$M_n(D)$, D division ring, is a $Z(D)$-central algebra

Definition: If R is a ring, $X \subseteq R$, the centralizer of X in R is
$Z_R(X) := C_R(X) := \{r \in R \mid \forall x \in X.\ rx = xr\}$.
$Z_R(R) = Z(R)$ (center of R)

-) $Z_R(X)$ is a subring of R (k-subalgebra if R is a k-algebra)
-) If R is a division ring, so is $Z_R(X)$ [$rx = xr, r \neq 0 \Rightarrow xr^{-1} = r^{-1}x$].

Theorem 6.3: Let R, S be k-algebras. If $R' \subseteq R$, $S' \subseteq S$ are k-subalgebras, then $Z_{R\otimes S}(R' \otimes S') = Z_R(R') \otimes Z_S(S')$.
In particular: -) $Z(R \otimes S) = Z(R) \otimes Z(S)$
-) If R, S central $\Rightarrow R \otimes S$ central.
-) If R central, $L \supseteq k$ a field extension, then $R \otimes_k L$ is a central L-algebra.

Proof: Since k is a field, if $R' \subseteq R$, $S' \subseteq S$ are k-subalgebras, they are sub-vs. $\Rightarrow R' \otimes S'$, $Z_R(R') \otimes Z_S(S')$ are vector spaces, and $Z_R(R') \otimes Z_S(S')$, $R' \otimes S' \subseteq R \otimes S$ are wlog. subspaces, so the statement makes sense.
($\supseteq$): If $r \in Z_R(R')$, $s \in Z_R(S')$, then, $\forall\, x \otimes y \in R' \otimes S'$
$(x \otimes y)(r \otimes s) = (xr) \otimes (ys) = (rx) \otimes (sy) = (r \otimes s)(x \otimes y)$
$\Rightarrow r \otimes s \in Z_{R\otimes S}(R' \otimes S')$.
($\subseteq$): Let $z \in Z_{R\otimes S}(R' \otimes S') \Rightarrow z = \sum_{i=1}^{n} r_i \otimes s_i$ with $n \geq 0$, $r_i \in R$, $s_i \in S$.
Take n minimal among all such repr. of z.
Then $(r_1, \dots, r_n)$ is k-linearly independent, and so is $(s_1, \dots, s_n)$.
[A linear dependence would give $r_i = \sum_{j \neq i} \lambda_j r_j$ for some i,

and give a shorter representation of z.]

Let $x \in S' \Rightarrow z(\underbrace{1 \otimes x}_{\in R \otimes S'}) - (1 \otimes x)z = 0$

$$\Rightarrow \sum_{i=1}^{n} (r_i \otimes s_i)(1 \otimes x) - (1 \otimes x)(r_i \otimes s_i) = \sum_{i=1}^{n} (r_i \otimes s_i x - r_i \otimes x s_i)$$

$$= \sum_{i=1}^{n} r_i \otimes \overbrace{(s_i x - x s_i)}^{\in S} = 0$$

$(r_i)_i$ are k-lin. indep. in $R \Rightarrow (r_i)_i$ S-lin. indep. in $R \otimes S$

$\Rightarrow \forall i.\ s_i x = x s_i \Rightarrow \forall i.\ s_i \in Z_S(S')$.

Symmetrically: $r_i \in Z_R(R') \Rightarrow z \in Z_R(R') \otimes Z_S(S')$ ▨

6.2. Simple Algebras

Again: k field, $\otimes = \otimes_k$

Definition: A k-algebra R is **simple** if it is simple as a ring.

Example: · $M_n(D)$, D div. ring, simple $Z(D)$ algebra
· $A_1(k)$, $\mathrm{char}\, k = 0$

Definition: R is **central simple**, if it central and simple as k-algebra.

Note: R simple ring $\Rightarrow Z(R)$ is a field (easy exercise), so every simple ring is central simple over $Z(R)$, but we are fixing k.

⚠ In many texts a central simple k-algebra (CSA) is central simple and fin. dim. over k.
(We are not making the last assumption.)

Theorem 6.4: Let R, S be k-algebras, S central simple. Then there is a bijection $\{\text{ideals of } R\} \longleftrightarrow \{\text{ideals of } R \otimes S\}$

$$I \longmapsto I \otimes S$$
$$J \cap R \longleftarrow\!\shortmid\ J.$$

Lemma 6.5: If $0 \neq J \trianglelefteq R \otimes S$, then $J \cap R \neq 0$.

Proof: $R \longrightarrow R \otimes S$, $r \longmapsto r \otimes 1$ is injective (we work over a field) so wlog. $R \subseteq R \otimes S$ and the claim makes sense.
Let $0 \neq x = \sum_{i=1}^{n} r_i \otimes s_i \in J$ with n minimal among all possible $x \in J \setminus \{0\}$. $\Rightarrow (r_i)_i$, $(s_j)_j$ are each k-lin. independent.
$s_1 \neq 0 \Rightarrow SsS = S \Rightarrow 1 = \sum_{i=1}^{m} x_i s y_i \quad (x_i, y_i \in S)$.

$$\text{Let } x' := \sum_{i=1}^{m} (1 \otimes x_i) x (1 \otimes y_i) = \sum_{i=1}^{m} \sum_{j=1}^{n} (1 \otimes x_i)(r_j \otimes s_j)(1 \otimes y_i)$$
$$= \sum_{i=1}^{m} \sum_{j=1}^{n} (r_j \otimes x_i s_j y_i)$$
$$= \sum_{j=1}^{n} r_j \otimes \underbrace{\left(\sum_{i=1}^{n} x_i s_j y_i \right)}_{=: s_j'}, \qquad s_1' = 1$$

Then $x' \in J$, and $x' \neq 0$ (the $(r_i)_i$ are k-lin. independent, and hence $(r_i \otimes 1)_i$ is lin. independent, and $s_1' \neq 0$).
$\forall s \in S.$ $\quad (1 \otimes s)x' - x'(1 \otimes s) = \sum_{j=1}^{n} (r_j \otimes s s_j' - r_j \otimes s_j' s)$

$$= \sum_{j=1}^{n} r_j \otimes (s s_j' - s_j' s)$$
$$\overset{s_1' = 1}{=} \sum_{j=2}^{n} r_j \otimes (s s_j' - s_j' s) \in J$$

minimal choice of x
$$\Rightarrow \quad 0 = \sum_{j=2}^{n} r_j \otimes (s s_j' - s_j' s) \Rightarrow \forall j.\ s_j' s = s s_j' \quad \left(\begin{smallmatrix} S\text{-lin. indep.} \\ \text{of } (r_j)_j \end{smallmatrix} \right)$$

$\Rightarrow s_j' \in Z(S) = k \Rightarrow r_j \otimes s_j' = r_j s_j' \otimes 1$

$\Rightarrow x' = \sum_{n=1}^{n} r_j \otimes s_j' = \sum_{n=1}^{n} (r_j s_j' \otimes 1) = \left(\sum_{j=1}^{n} r_j s_j'\right) \otimes 1 \in R \otimes 1 = R$

$\Rightarrow x' \in J \cap R,\ x' \neq 0$ ▨

November 27, 2025

Proof of Theorem 6.4: Since $R \longrightarrow R \otimes S$ is injective (again using that k is a field), injectivity is clear.

Show: If $J \trianglelefteq R \otimes S$, then $J = (J \cap R) \otimes S$.

Let $I := J \cap R$. Then $I \otimes S \subseteq J$.

Consider $0 \longrightarrow I \hookrightarrow R \longrightarrow R/I \longrightarrow 0$ (SES)

$\overset{k \text{ field}}{\underset{S \text{ free}}{\Longrightarrow}}$ $0 \longrightarrow I \otimes S \longrightarrow R \otimes S \xrightarrow{\pi} (R/I) \otimes S \longrightarrow 0$ is a SES

$\Rightarrow \ker(\pi) = I \otimes S$.

If $J \neq I \otimes S$, $0 \neq \pi(J) \trianglelefteq (R/I) \otimes S \overset{L6.5}{\Longrightarrow} \pi(J) \cap R/I \neq 0$,

i.e. $\exists r \in R \setminus I.\ (r+1) \otimes 1 \in \pi(J) \rightsquigarrow r \otimes 1 \in J \setminus I \otimes S$ ↯ $I = J \cap R$. ▨

Corollary 6.6: If R, S are central simple k-algebras, then $R \otimes_k S$ is a central simple k-algebra.

Proof: $Z(R \otimes S) = k$ by T6.3, $R \otimes S$ simple by T6.4. ▨

Corollary 6.7: If R is a fin. dim. c.s.a., $\dim_k R = n$, then $R \otimes R^{op} \cong \mathrm{End}(R_k) \cong M_n(k)$.

Proof: R, R^{op} c.s.a. $\Rightarrow R \otimes R^{op}$ is a csa of dimension n^2.

${}_R R_R$ bimodule $\Rightarrow \exists$ k-algebra hom. $f: \begin{cases} R \otimes R^{op} \longrightarrow \mathrm{End}(R_k) \cong M_n(k) \\ r \otimes s \longmapsto (x \mapsto rxs) \end{cases}$

$R \otimes R^{op}$ simple $\Rightarrow f$ injective

Comparing dimensions, f is bijective. ▨

Example: $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}^{op} \cong M_4(\mathbb{R})$

Since also $\mathbb{H} \cong \mathbb{H}^{op}$, via $z = a + bi + cj + dk \mapsto a - bi - cj - dk$ (since $\overline{zw} = \bar{w}\bar{z}$), in fact $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \cong M_4(\mathbb{R})$.

Theorem 6.7[1]: If R is a fin. dim. central simple k-algebra, then $[R:k]$ $(= \dim_k R)$ is a square.

Proof: $R = M_n(D)$ with D division ring [T 2.21].
$Z(D) \supseteq k \Rightarrow D$ is a finite dimensional division k-algebra, $m := [D:k]$.
Let $\bar{k}$ be the algebraic closure of k.
$\Rightarrow D \otimes_k \bar{k}$ has $\dim_{\bar{k}}(D \otimes_k \bar{k}) = m$ and is a central simple $\bar{k}$-algebra [T6.3, T6.4] $\overset{\bar{k} \text{ alg. closed}}{\underset{[1.23]}{\Longrightarrow}}$ $\underbrace{D \otimes_k \bar{k}}_{\dim. m} \cong \underbrace{M_r(\bar{k})}_{\dim r^2} \Rightarrow m = r^2$
$\Rightarrow \dim_k A = n^2 \dim_k D = m^2 r^2$ ∎

In particular: f. d. dim. algebras/k have square dimension.

Definition: R Fin. dim. central simple k-algebra ($R \cong M_n(D)$, D div. ring):
- $\deg_k R := \sqrt{[R:k]}$ is the degree of R
- $\operatorname{ind}_k R := \sqrt{[D:k]}$ is the index of R

Note: $[R:k] = n^2 [D:k]$, so $\operatorname{ind}_k(R) \mid \deg_k(R)$.

6.3. Extension of Scalars For Semisimple Algebras

K is a field

Example: $K = \mathbb{F}_p(t)$, $x^p - t$ is irreducible / K, but not seperable: in $K(a) \cong \mathbb{F}_p(t)[y]/(y^p - t)$ $x^p - t = x^p - a^p = (x-a)^p$ has a root with multiplicity p.
$\Rightarrow K(a)$ semisimple K-algebra, but

$$K(\alpha)\otimes_K K(\alpha) \cong K(\alpha)[y]/(y^p-\alpha^p) \cong \underbrace{K(\alpha)[y]/(y-\alpha)^p}$$

is not semisimple — Jacobson radical $(y-\alpha)+(y-\alpha)^p$

Recall: (1) An algebraic field extension L/K is seperable if the minimal polynomial $m_\alpha \in K[x]$ for each $\alpha \in L$ is seperable ($:\Leftrightarrow$ m_α has no repeated roots in $\bar{K} \Leftrightarrow m_\alpha' \neq 0$)
(2) If K has charasteristic 0 or is finite, L/K is always seperable.
(3) [Primitive Element Theorem]: If L/K is finite seperable, there exists $\alpha \in L/K$ s.t. $L = K(\alpha)$.

Theorem 6.8: Let L/K be a finite field extension. Then $(\forall K'/K.\ L_{K'} := L\otimes_K K'$ semisimple$) \Leftrightarrow L/K$ separable.

Proof: ($\Leftarrow$): Let $L = K(\alpha)$, so $L = K[x]/(m_\alpha) = \langle 1, \alpha, \alpha^2, \dots, \alpha^{n-1}\rangle_K$ with $n = [L:K]$, and $m_\alpha \in K[x]$ separable.
$\Rightarrow L_{K'}$ has K'-basis $(1\otimes 1, \alpha\otimes 1, \dots, \alpha^{n-1}\otimes 1)$, and $\alpha\otimes 1$ satisfies m_α, so $L_{K'} \cong K'[x]/(m_\alpha)$.
In $K'[x]$, $m_\alpha = p_1\cdots p_r$ with monic irreducible $p_i \in K'[x]$
m_α separable $\Rightarrow p_1,\dots,p_r$ are distinct prime elements of the PID $K'[x]$ (so comaximal, i.e., $(p_i)+(p_j) = K'[x]$ for $i\neq j$)
Chinese Remainder Theorem $\Rightarrow K'[x]/(m_\alpha) = K'[x]/(p_1)\times\cdots\times K'[x]/(p_r)$ with each $K'[x]/(p_i)$ a field.

($\Rightarrow$): Let $\alpha \in L$ be not separable, i.e. $m_\alpha \in K[x]$ not separable, say $m_\alpha = (x-\alpha_1)^{e_1}\cdots(x-\alpha_r)^{e_r} \in \bar{K}[x]$ with some $e_i \geq 2$, $\alpha_1,\dots,\alpha_r$ pairwise distinct.
$\Rightarrow \bar{K}\otimes_K K(\alpha) \cong \bar{K}[x]/(m_\alpha) \cong \bar{K}[x]/(x-\alpha_1)^{e_1}\times\cdots\times\bar{K}[x]/(x-\alpha_r)^{e_r}$ (CRT)
If $e_i \geq 2$ for some i, then $\bar{K}\otimes K(\alpha)$ has nonzero nilpotent elements, then so does $L\otimes_K \bar{K} \supseteq K(\alpha)\otimes_K \bar{K}$. Then $L_{\bar{K}}$ is

not semisimple (a commutative semisimple ring has no nonzero nilpotents, because it is a product of fields).

Definition: K Field, R f.d. semisimple K-algebra. Then $Z(R) \cong K_1 \times \cdots \times K_r$, K_i/K Finite field extensions (using T2.18). R is separable, if each K_i/K is separable.

Corollary 6.9: (1) IF R is a separable f.d. semisimple k-algebra, then $R \otimes_K K'$ is semisimple for all fields $K' \supseteq K$.
(2) IF R, S are f.d. semisimple k-algebras, and at least one is separable, then $R \otimes_K S$ is semisimple.

Proof: $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$ with D_t/K f.d. division algebras, $Z(D_i) = K_i$ separable $/K$.

$$\begin{aligned} K' \otimes R &\cong K' \otimes (M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)) \\ &\cong (K' \otimes M_{n_1}(D_1)) \times \cdots \times (K' \otimes M_{n_r}(D_r)) \end{aligned}$$

Now
$$\begin{aligned} K' \otimes_K M_{n_i}(D_i) &\cong K' \otimes_K (K_i \otimes_{K_i} M_{n_i}(D_i)) \\ &\cong_{[T6.8]} (K' \otimes_K K_i) \otimes_{K_i} K' \otimes_K M_{n_i}(D_i) \\ &\cong (L_1 \times \cdots \times L_{s_i}) \otimes_{K_i} M_{n_i}(D_i) \qquad (L_i \text{ fields}) \\ &\cong (L_1 \otimes_{K_i} M_{n_i}(D_i)) \times \cdots \times (L_{s_i} \otimes_{K_i} M_{n_i}(D_i)) \end{aligned}$$

and $L_j \otimes_{K_i} M_{n_i}(D_i)$ is simple by T 6.4 since $M_{n_i}(D_i)$ is central simple, L_j is simple.

(2) Reducing over finite products (as in (1)), w.l.o.g. R, S are simple and $Z(S)/K$ is separable.

$$R \otimes_K S \cong R \otimes_K (Z(S) \otimes_{Z(S)} S) \cong (R \otimes_K Z(S)) \otimes_{Z(S)} S$$
$$\overset{(1)}{\cong} (R_1 \times \cdots \times R_t) \otimes_{Z(S)} S = \prod_{i=1}^{t} (\underbrace{R_i \otimes_{Z(S)} S}_{\text{simple by T6.4}})$$

Conclusion of (1) also holds if R not separable, but K'/K separable.

Example: $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is semisimple, so $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \times \mathbb{C}$ as $\mathbb{R}$-algebras.
Exercise: Show $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \times \mathbb{C}$ via $z \otimes w \longmapsto (zw, z\bar{w})$.

6.4. The Skolem-Noether Theorem

If R is a K-algebra, $u \in R^\times$, then $d: R \to R$, $x \mapsto uxu^{-1}$ is a K-automorphism. Such automorphisms are called inner automorphisms.

Theorem 6.10 [Skolem-Noether]: Let R be a fin. dim. central simple K-algebra and S a simple K-algebra. If $f, g: S \to R$ are K-algebra hom. (necessarily injective) then there is an inner endomorphism $d: R \to R$ s.t. $d \circ f = g$.
Equivalently: If $R_1, R_2 \subseteq R$ are isomorphic simple subalgebras of R, and $h: R_1 \to R_2$ is a K-algebra homomorphism, there exists $u \in R^\times$ s.t. $\forall x \in R_1 . \, h(x) = uxu^{-1}$.

[Equivalence: $\Rightarrow$: Take $f: R_1 \hookrightarrow R$, $g: R_1 \xrightarrow{h} R_2 \hookrightarrow R$
$\Rightarrow \exists u \in R^\times . \, uxu^{-1} = uf(x)u^{-1} = g(x) = h(x) \quad \forall x \in R_1$.
$\Leftarrow$: $R_1 := f(S) \xrightarrow{g \circ f^{-1}} R_2 := g(S) \Rightarrow g \circ f^{-1} = d$, d inner $\Rightarrow g = d \circ f$.]

Corollary 6.11: If R is a F.d. simple K-algebra and $f \in \mathrm{Aut}_K(A)$, then $f(x) = uxu^{-1}$ for some $u \in R^\times$.

Lemma 6.12: R F.d. simple algebra, $M, N \in \mathrm{Mod}\text{-}R$, F.d./$k$. Then $M \cong N \Leftrightarrow \dim_K M = \dim_K N$.

Proof: $\Rightarrow$: ✓ $\Leftarrow$: as a simple artinian ring, R has a unique simple module $U_R \Rightarrow M \cong U_R^r$, $N \cong U_R^t \Rightarrow$
$r \cdot \dim_K U = \dim_K M = \dim_K N = t \dim_K U \to r = t \Rightarrow M \cong M \cong N$. ▨

Proof of T6.10: ${}_RR_R$ is an (R,R)-bimodule $(r(xr') = (rx)r')$.
Now $f,g: S \longrightarrow R$ define two (S,R)-bimodule structures on R:
$s \cdot r = f(s)r$, $s \circ r := g(s)r$ $(\forall r \in R.\ s \in S)$
Egivalently, these are $S^{op} \otimes_K R$ right module structures with the same K-dimension. $S^{op} \otimes_K R$ is a f.d. simple K-algebra [T6.4] so the bimodule structures are isomorphic.
Meaning: $\exists$ K-linear bijective $h: R \to R$ s.t.
(i) $\forall s \in S. \forall x \in R.\ h(f(s)x) = g(s)h(x)$
(ii) $\forall x, r \in R.\ h(xr) = h(x)r$ $\overset{x=1}{\Rightarrow}$ $h(r) = h(1)r$ $\forall r \in R$
$\overset{h \text{ bijective}}{\Rightarrow}$ $h(1) \in R^\times$, $u := h(1)$ $\overset{(i),r=1}{\Rightarrow}$ $\underset{u}{h(1)}f(s) = g(s)\underset{u}{h(1)} \Rightarrow g(s) = uf(s)u^{-1}$ ▨

Applications: Shorter proofs of Wedderburn's Little Theorem, ...

6.5. The Centralizer Theorem

If R is a K-algebra, $X \subseteq R$, then $Z_R(X) = \{r \in R \mid \forall x \in X.\ rx = xr\}$ is a subalgebra.
Note: $X \subseteq Z_R(Z_R(X))$ (double centralizer)

Theorem 6.13 [Centralizer Theorem]: Let R be a finite dimensional central simple K-algebra (K a field), $S \subseteq R$ a simple subalgebra.
(1) $Z_R(S)$ is simple.
(2) $[Z_R(S) : K][S : K] = [R : K]$
(3) $Z_R(Z_R(S)) = S$ [Double Centralizer Theorem]

Proof: (1) $R \cong M_n(D) \cong \mathrm{End}(V_D)$ with ${}_RV$ the unique simple R-module, $D = \mathrm{End}({}_RV)^{op}$ [left version of T2.11 or T4.7]
${}_RV_D$ is an (R,D)-bimodule, hence (S,D)-bimodule, i.e. left $S \otimes_K D^{op}$-module. ↙ bimodule end.
Claim: $Z_R(S) \cong \mathrm{End}({}_SV_D) = \mathrm{End}({}_{S\otimes D^{op}}V)$

$$[Z_R(S) \hookrightarrow R \xrightarrow{\cong} \mathrm{End}(V_D)$$
$$r \longmapsto \mu_r, \quad \mu_r(v) = rv$$

Show: $\{\mu_r \mid r \in Z_R(S)\} = \mathrm{End}(_S V_D)$.

($\subseteq$): Let $r \in Z_R(S)$. $\mu_r(sv) = rsv = srv = s\mu_r(v)$ $(s \in S, v \in V)$

($\supseteq$): Let $r \in R$ s.t. $\mu_r(sv) = s\mu_r(v)$ $\forall s \in S. r \in V$

$\Rightarrow (rs - sr)v = 0 \ \forall r \in R \overset{{}_R V \text{ Faithful}}{\Longrightarrow} rs - sr = 0.$]

$S \otimes_K D^{op}$ is simple [T6.4]

$\Rightarrow S \otimes_K D^{op} \cong M_m(E) \cong \mathrm{End}(W_E)$ with $E = \mathrm{End}(_{S \otimes_K D^{op}} W)^{op}$ (div. ring) (*)

W_E unique simple $S \otimes_K D^{op}$-module $\Rightarrow V \cong W^t$ as $S \otimes_K D^{op}$-modules, $t \geq 1$

$\Rightarrow \mathrm{End}_{S \otimes D^{op}}(V) \cong \mathrm{End}_{S \otimes D^{op}}(W^t) = M_t(\underbrace{\mathrm{End}_{S \otimes D^{op}}(W)}_{E^{op}})$

$\Rightarrow Z_R(S) \cong M_t(E^{op})$ simple

(2) $[R:K] = n^2 [D:K]$

$[S:K][D:K] = m^2 [E:K]$ by (*)

$[Z_R(S):K] = t^2 [E:K]$

$n[D:K] = \dim_K V = \dim_K W^t = t \dim_K W = tm [E:K]$ $(V \cong W^t)$

$\Rightarrow [S:K][Z_R(S):K] = m^2 t^2 \frac{[E:K]^2}{[D:K]} = m^2 t^2 \frac{[D:K]^2 n^2}{t^2 m^2 [D:K]} = [R:K].$

(3) $S \subseteq Z_R(Z_R(S))$ and by (2): $[R:K] = [Z_R(S):K][S:K]$ (simple by T6.13 (1))

$= [Z_R(Z_R(S)):K][Z_R(S):K]$

So $[S:K] = [Z_R(Z_R(S)):K] \Rightarrow S = Z_R(Z_R(S))$ ▨

Corollary 6.14: If $S \subseteq R$ are finite dimensional central simple algebras, then $R \cong S \otimes Z_R(S)$ (as algebras).

Proof: $S, Z_R(S)$ commute in R

$\Rightarrow \exists$ K-algebra homomorphism $f: S \otimes Z_R(S) \longrightarrow R$, $s \otimes s' \mapsto ss'$ (UP)

$S \otimes Z_R(S)$ simple [T6.4] $\Rightarrow f$ injective

$\overset{\text{dimensions}}{\Rightarrow}$ 6.13(2) f surjective. ▨

December 4, 2025