NONCOMMUTATIVE ALGEBRA

1. Basics & Examples

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

here: always unital (with 1), associative
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 $\exists n\in\mathbb{N}_0$: $a^n=0$
invertible = unit if right and left invertible
($R^\times := \{a\in R:\ a \text{ invertible}\}$ group of invertible elts, unit group)
zerodivisor if right or left zerodivisor.

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

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

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

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

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

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

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

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

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

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

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

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

4) $R = \begin{bmatrix} \mathbb{Z} & \mathbb{Z}/2\mathbb{Z} \\ 0 & \mathbb{Z} \end{bmatrix}$ Here $\begin{bmatrix} 2 & \bar{0} \\ 0 & 1 \end{bmatrix}$ is a left zerodivisor, but not right zero divisor: $\begin{bmatrix} 2 & \bar{0} \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & \bar{1} \\ 0 & 0 \end{bmatrix} = 0$,

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

5) Free k-algebras: 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.

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

Coefficients commute with indeterminates, but indeterminates do not commute with each other, e.g. $xy - yx \neq 0$.

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

universal property

center   i.e. R' is a k-algebra

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

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

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

(as k-algebras)

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

$|X| \geq 2$: totally different from $k[x_1, \ldots, x_n]$!

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

monomorphism

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

e.g. $\varphi(z_2 z_3 z_1) = xy^2xy^3xy$

6) Algebras defined by generators & relations:

If R is a k-algebra (every ring is a $\mathbb{Z}$-algebra!), $(g_i)_{i\in I}$ is a system of generators $\rightarrow \exists$ hom. $\varphi: k\langle x_i : i \in I\rangle \twoheadrightarrow R$, $x_i \mapsto g_i$.

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

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

- $k\langle x, y \mid xy - yx\rangle = k\langle x,y\rangle/(xy-yx) \cong k[x,y]$
- $\mathbb{R}\langle x, y \mid x^2+1, y^2+1, xy+yx\rangle \cong \mathbb{H}$ $(x \mapsto i, y \mapsto j)$
- $k\langle x, y \mid xy - yx - 1\rangle =: A_1(k)$ is the 1^{st} Weyl algebra.

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

Interpretation as differential operators on $k[y]$:

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

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

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

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

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

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

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

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

Special cases: R commutative,

- G free monoid gen. by a set $X \Rightarrow R[G]$ is the free R-alg. gen. by X
- $G \cong (\mathbb{N}_0^{(I)}, +)$, so g generated by $\{x_i : i \in I\}$, so elts of G are of form $x_{i_1}^{n_1} x_{i_2}^{n_2} \dots x_{i_k}^{n_{i_k}}$, $i_1, \dots, i_k \in I$ pw. distinct

$\Rightarrow R[G] \cong R[x_i : i \in I]$ polynomial ring.

UP: If $\varphi: R \to R'$ is a ring hom, $\sigma: G \to (R', \cdot, 1)$ is a monoid hom s.t. $\varphi(r)\sigma(g) = \sigma(g)\varphi(r)$ for all $r \in R, g \in G$, then there exists a unique ring hom.

$$\bar{\varphi}: R[G] \longrightarrow R' \quad \text{s.t.} \quad \bar{\varphi}|_R = \varphi, \quad \bar{\varphi}|_G = \sigma.$$

9) Skew polynomial rings / Ore extensions R ring

a) $\sigma: R \to R$ endomorphism

$R[x;\sigma]$ elements: finite formal left R-linear combinations of x^i, $i \geq 0$:

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

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

Note: polynomials w. coeff on the right can be rewritten as

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

but the converse only works if σ is surjective.

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

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

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 δ be a derivation on R (i.e. $\delta(a+b) = \delta(a) + \delta(b)$

and $\delta(ab) = \delta(a)b + a\delta(b)$, i.e. Leibniz rule)

$R[x;\delta]$ again has elts $\sum_i a_i x^i$,

multiplication induced by $\boxed{\forall a \in R: \quad xa = ax + \delta(a)}$

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

$= ax^2 + 2\delta(a)x + \delta^2(a)$

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

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

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

In particular, elts of $A_1(k)$ have a (unique) representation

$\sum_{i,j}' a_{ij}\bar{y}^i\bar{x}^j$, i.e., $\{\bar{y}^i\bar{x}^j : i,j \geq 0\}$ is a k-basis of $A_1(k)$

(but also $\{\bar{x}^j\bar{y}^i : i,j \geq 0\}$ 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., $\delta(a+b) = \delta(a)+\delta(b)$, $\delta(ab) = \delta(a)b + \sigma(a)\delta(b)$)

$R[x;\sigma,\delta]$ ... same construction with $\boxed{\forall a \in R:\ xa = \sigma(a)x + \delta(a)}$

WHY? Suppose we want to define some multiplication

on formal sums $f = \sum' a_i x^i$, $g = \sum' b_j x^j$ s.t.

$\deg(fg) \leq \max\{\deg f, \deg g\}$.

In particular: $x \cdot a \overset{!}{=} \sigma(a)x + \delta(a)$ with maps $\sigma, \delta: R \to R$

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

$= (xa)b = (\sigma(a)\underline{x} + \delta(a))\underline{b} = \sigma(a)(\sigma(b)x + \delta(b)) + \delta(a)b$

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

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

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

$R[\![x]\!] = \{a_0 + a_1x + a_2x^2 + \ldots : a_i \in R\}$

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

Laurent series: $R(\!(x)\!) := \{\sum_{i=-n}^{\infty}{}' a_i x^i,\ a_i \in R\}$ invertible $\Leftrightarrow$ lowest coeff invertible

$\Rightarrow$ if R is a div. 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 $x^{-1}a = \sigma^{-1}(a)x^{-1}$)

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

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

Rem: 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

If M_R is a right R-module, it is a left R^{op}-module via
$$\underset{R^{op}}{a} \cdot m := m \cdot \underset{R}{a} \qquad [(a \cdot_{op} b)m = (ba)m = m(ba) = (mb)a = a(mb) = a(bm)]$$

$\Rightarrow$ Mod-$R \cong R^{op}$-Mod (as categories) ⚠ i.g. $R \not\cong R^{op}$

$R = R^{op} \Leftrightarrow R$ commutative. My default: right modules.

Rem: The right R-module structure σ can equivalently be described by a ring hom. $\tilde{\sigma} : R^{op} \to End_{\mathbb{Z}}(M)$

[Given σ, define $\tilde{\sigma}(a)(m) := ma$. E.g. $\tilde{\sigma}(ab)(m) = mab = (\tilde{\sigma}(a)(m))b =$
$$= \tilde{\sigma}(b)(\tilde{\sigma}(a)(m)) = (\tilde{\sigma}(b) \circ \tilde{\sigma}(a))(m) \Rightarrow \tilde{\sigma}(b \cdot_{op} a) = \tilde{\sigma}(b) \circ \tilde{\sigma}(a).$$

Conversely, given $\tilde{\sigma}$, define $m \cdot a := \tilde{\sigma}(a)m$.]
left R-module structure $\hat{=}$ ring hom. $R \to End_{\mathbb{Z}}(M)$.

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

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

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

<u>Exms</u> • $\mathbb{C}$, $\mathbb{H}$ are $\mathbb{R}$-algebras (of dimensions 2 resp. 4)
$\mathbb{C} \hookrightarrow \mathbb{H}$ as subring (e.g. $i \mapsto i$) but i is not central
$\mathbb{H}$ is not a $\mathbb{C}$-algebra!.

• R commutative → $R\langle X\rangle$, $R[G]$, $M_n(R)$ R-algebras,
$R[x; \sigma, \delta]$ i.g. is not!

• <u>Rings</u> = $\mathbb{Z}$-<u>Alg</u> as categories

<u>Exm</u> (Endomorphism rings) Let $M_R \in$ Mod-R,
$End(M_R) := \{ f: M_R \to M_R : f \text{ R-module hom} \}$ is a ring
with multiplication $\circ$ [<u>e.g.</u> $(f \circ (g+h))(m) = f((g+h)(m)) =$
$\overset{\nearrow \text{+ pointwise}}{=} f(g(m)+h(m)) \overset{⚠}{=} f(g(m)) + f(h(m)) = (f\circ g + f \circ h)(m)$.]
↑ f hom.

Special cases:

⚠ r on left

•) $M = R_R$: $L: R \to End(R_R)$, $r \mapsto L_r$, $L_r(x) = rx$
$\Rightarrow L$ is an isomorphism

[Consider $x = 1$: $0 = L_r \Rightarrow 0 = L_r(1) = r \cdot 1 = r \Rightarrow r = 0$, so L inj.

If $\varphi \in \mathrm{End}(R_R)$, then $\forall x \in R$: $\varphi(x) = \varphi(1 \cdot x) = \varphi(1) \cdot x$

$\Longrightarrow \varphi = L_r$, so L is surjective.]

- ⚠ $\mathrm{End}({}_R R) \cong R^{op}$

- $R = K$ a field, $V_K \cong K^n$ f.d. vector space (finite-dimensional)

  $\Longrightarrow \mathrm{End}(V_K) \cong M_n(K)$

- K field, R f.d. K-algebra

  $\Longrightarrow R \cong \mathrm{End}(R_R) \subseteq \mathrm{End}(R_K) \cong M_n(K)$ (as K-algebras)

So every f.d. K-algebra embeds into a matrix ring!

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

$(\mathbb{H} \hookrightarrow M_2(\mathbb{C}))$