Week 1 (MAT 512.UB)

This is a course on noncommutative algebra, building on the algebra courses of the bachelor curriculum (if you know commutative algebra that's even better!)

Aims: • Basics of ring and modules (for students of varying background)

→ following lecture notes of Alfred Geroldinger, books by Goodearl-Warfield, McConnell Robson

- Examples and construction of algebras (→ mostly exercise classes)
- Maybe: module categories and related properties of modules

0. Why study noncommutative algebra?

In "nature" things do not usually commute

⇝ first example: $M_n(\underset{\overset{\uparrow}{\text{field } k=\mathbb{R},\mathbb{C},\dots}}{k})$, known from linear alg., is $\underset{\text{ring}}{\text{noncomm.}}$

This should be close to being a field?!

But it's not, even for $n=2$, have zerodivisors $\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&0\\1&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$

→ Find structure of such noncomm. rings, classify them...

Where do noncomm. rings appear?

(1) Rep. theory: study groups, Lie algebras ⇝ understand their representations ⇝ understand group algebra, universal enveloping algebra

(2) Physics: many algebras arise e.g. for spin in quantum mechanics (Clifford algebras), dimer models (dimer algebras)

(3) Differential eqn's: linear diff. eqns correspond to modules over rings of diff. operators. Also: quantum groups (are algebras, not groups) arise in the study of integrable systems.

(4) Topology: cohomology of a top. space gives a ring. Jones polynomials for knots come from representation theory of Hecke algebras

(5) Number Theory: a basic object is the Brauer group, for classifying central simple algebras. Also: In proof of Wiles and Taylor of Fermat's last theorem (Hecke algebras)

(6) Functional analysis: C^*-algebras and von Neumann algebras

(7) Linear algebra: Jordan normal form is the classification of finite dim. modules over $K[x]$.

Contents of our course: Basics of noncomm. ring + module theory (Simple/semisimple modules structure thm [Artin-Wedderburn])

- uniform dimension
- quotient rings + Goldie's theorem
- Dedekind-like rings (?)
- Basics of path algebras (?)
- Diff. operator rings (?)

Follows A. Geroldinger's lecture notes, Book by Goodearl-Warfield

Notation:

In all of the course: all rings R (or Λ) have identity 1_R and homomorphisms $\varphi: R \to S$ send 1_R to 1_S.

Recall: A ring $(R,+,\cdot)$ is a set with two binary operations $+$ and $\cdot$, s.t. (1) $(R,+)$ is an abelian group and (2) $(R,\cdot)$ is assoc.

(G1): $a+(b+c)=(a+b)+c \quad \forall a,b,c\in R$
(G2): $\exists 0_R: a+0=0+a=a \quad \forall a\in R$
(G3): $\forall a: \exists b$ s.t. $a+b=b+a=0$
(G4): $a+b=b+a \quad \forall a,b\in R$

- $a\cdot(b\cdot c)=(a\cdot b)\cdot c$
- $\exists 1_R: a\cdot 1_R = 1_R\cdot a = a$.

and

(3) $+$ and $\cdot$ are distributive $\forall a,b,c\in R$: $a\cdot(b+c)=a\cdot b+a\cdot c$
$(a+b)\cdot c = a\cdot c + b\cdot c$

If $\cdot$ is commutative, i.e. $a\cdot b=b\cdot a$ $\forall a,b\in R$, then R is commutative. We will mostly be dealing with noncomm. rings.

Rmk: (1) assures that $R\neq\emptyset$. ($0_R\in R$)

Examples (0) $R=\{0\}$

(1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}_n, \underset{\substack{\uparrow\\ \text{field}}}{K}[x]$ are all commutative rings.

(2) Let R be any ring and $n\geq 1$. Then $M_n(R)$ is a ring with matrix mult. and addition.

(3) $R[X]$ is a ring with polyn. addition + mult, but we require commutativity between $r\in R$ and X: $r\cdot X = X\cdot r$ $\forall r\in R$. (Otherwise, the ring $R[X]$ would be much more complicated!)

(4) A domain D is a ring $\neq 0$, s.t. $\forall a,b\in D$: $a\cdot b=0 \Rightarrow a=0$ or $b=0$.

(5) A division ring (or skew field) is a ring $D\neq 0$ s.t. $\forall a\neq 0 \in D$, $\exists b \in D$ s.t. $a\cdot b = b\cdot a = 1$.

(e.g.: quaternions) A field is a commutative division ring.

A *ring homomorphism* $\varphi : R \to S$ is map s.t.

(RH1) $\varphi(a+b) = \varphi(a) + \varphi(b)$ $\forall a, b \in R$

(RH2) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

(RH3) $\varphi(1_R) = 1_S$.

- A *left (right) ideal* ^{I} of R is a subset $I \subseteq R$, s.t.

(I1) $I \neq \emptyset$

(I2) $\forall a, b \in I : a \pm b \in I$

(I3) $\forall r \in R, \forall a \in I : \quad r \cdot a \in I \quad (a \cdot r \in I)$

I is an *ideal* if it is both a left and right ideal.

Ex: In $M_n(K)$ ← field, the set $\left\{ \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{bmatrix}, a_{ij} \in K \right\}$ forms a right ideal (!).

and $\left\{ \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & 0 & \cdots & 0 \end{pmatrix}, a_{i1} \in K \right\}$ a left ideal.

- The isomorphism theorems:

(1) A homomorph. $\varphi : R \to S$ induces an isom.

$$R/\ker\varphi \cong \operatorname{Im}\varphi$$

(2) If I is an ideal of R and $S \subseteq R$ is a subring of R then $S/(S \cap I) \cong (S+I)/I$.

(3) If I is an ideal of R, then the ideals of R/I are of the form J/I with J an ideal containing I, and

$$(R/I)/(J/I) \cong R/J.$$

[The opposite ring R^{op} is obtained from $(R, +, \cdot)$ by using $r \circ s := sr$. Morphism $M_n(R)^{op} \xrightarrow{\text{transpose}} M_n(R^{op})$.

Further: • For a ring R, and if $a, b \in R$ with $a \cdot b = 1$, then a is a *left inverse of b*, and b is a *right inverse of a*.

- If a has a left + a right inverse, then these coincide and we say that a is *invertible*.
- We denote by $R^* := \{a \in R : a \text{ is invertible}\}$, the *unit group of R*.

sometimes $Z(R)$

- The *centre* of R is $C(R) := \{r \in R : r \cdot s = s \cdot r \ \forall s \in R\} \subseteq R$ and $C(R)$ is a commutative *subring* of R

  ↳ $S \subseteq R$ s.t. $S \neq \emptyset$
  $a \pm b \in S$
  $a \cdot b \in S$

- An element $a \in R$ is a left (right) *zero-divisor* if $\exists x \neq 0 \in R$ s.t. $ax = 0$ $(xa = 0)$. A zero-divisor is a left- and right zero-divisor; $zd(R) := \{r \in R : r \text{ zero-div}\}$, and $zd(R) \cap R^* = \emptyset$.
- $a \in R$ is *left (right) regular* if for any $x \in R$ and $xa = 0$ $(ax = 0)$ $\Rightarrow x = 0$. (Equiv: a is *not* a right (left) zero-div).

  $a \in R$ is *regular* if it is both left + right regular $\Leftrightarrow$ a is a NZD.

  $R^{\circ} := \{\text{regular } r \in R\}$ ← semigroup

Modules We will always consider *left* modules M if not further specified (i.e.

R ring, (M1) $(M,+)$ is abelian group, in part: $0 \in M$
(M2) Scalar mult: $R \times M \to M$
$(r,m) \mapsto r \cdot m$ s.t.
$(rr') \cdot m = r(r'm)$ $\forall r,r' \in R$ $\forall m \in M$.
(M3) distr: $r \cdot (m+n) = r \cdot m + r \cdot n$
(M4) unital: $1_R \cdot m = m$)

To make clear, write $M = {}_R M$.

Let now M be an R-module. Then M is

- cyclic if $M = {}_R\langle a \rangle$ for some $a \in M$

  ${}_R\langle a_1, \dots, a_n \rangle = \{ \sum_{i=1}^{m} r_i a_i , r_i \in R \}$ mod. generated by $\{a_1, \dots, a_n\}$

- torsion free if $\mathrm{ann}_R(x) = 0_R$ $\forall x \neq 0 \in M$

  $\{ r \in R : r \cdot x = 0_R \}$

- For a subset $E \subseteq M$, let
$$\ell\text{-}\mathrm{ann}_R(E) := \mathrm{ann}_R(E) = \{ \lambda \in R : \lambda x = 0 \ \forall x \in E \}$$
  be the left annihilator of E. Then $\ell\text{-}\mathrm{ann}_R(E)$ is a left ideal in R. (!)

  a subset $N \subseteq M$, s.t. N closed under addition from M, and scalar mult.

  If $N \subseteq M$ is a submodule, then $\mathrm{ann}_R(N)$ is a two sided ideal.

- The direct product of $\{M_i\}_{i \in I}$, denoted by $\prod_{i \in I} M_i$ consists of all sequences $(m_i)_{i \in I}$ with $m_i \in M_i$ and addition $(m_i)_{i \in I} + (n_i)_{i \in I} := (m_i + n_i)_{i \in I}$ and scalar mult: $r(m_i)_{i \in I} := (rm_i)_{i \in I}$ $\forall r \in R$ is a module (!).

Rmk The direct product of any family of domains is reduced. (e.g: $K[x] \times K[y]$ reduced, but $K[x]/(x^2) \times K[y]$ not: $(x,0) \neq (0,0)$, $(x,0)^2 = (0,0)$)

Finally: R is reduced if it has no nonzero nilpotent elements
i.e. $a^n = 0$ for some $n \geq 1 \Rightarrow a = 0$.

CHAPTER 1
MODULE THEORY

§1.1 Free, noetherian, and artinian modules

Def: Let M be an R-module. A family of elements $(u_i)_{i\in I}$ in M is called

- R-linearly independent if for any family $(\lambda_i)_{i\in I}$ we have: if $\lambda_i = 0$ for almost all $i \in I$ and $\sum_{i\in I} \lambda_i u_i = 0$, then $\lambda_i = 0 \ \forall i \in I$.
- R-basis of M if $(u_i)_{i\in I}$ is a linearly independent generating set of M. $\Longleftrightarrow$ the map $\begin{array}{l} R^{(I)} \longrightarrow M \\ (\lambda_i)_{i\in I} \longmapsto \sum_{i\in I} \lambda_i u_i \end{array}$ is an isomorphism.

The module M is called free if it has a basis. If $E \subset M$ is a generating set, then the map

$$f: R^{(E)} \longrightarrow M : (r_u)_{u\in E} \longmapsto \sum_{u\in E} r_u \cdot u$$

is an R-module epimorphism. So any such M is an epimorphic image of a free module.

Ex: (1) R^n is a free module for any ring R.

(2) Let $R = M_n(k)$ and $M = Re_1 = M_n(k)\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & & \\ \vdots & & & & \\ 0 & \cdots & & & \end{bmatrix} = \left\{ \left(\begin{array}{c|c} a_{11} & 0 - 0 \\ a_{21} & \\ \vdots & 0 \\ a_{n1} & \end{array} \right), a_{i1} \in k \right\}$

M is a left module but not free:

Clearly, M is generated by the element $1\!\!1_n \cdot e_1 = e_1 = \left(\begin{array}{c|c} 1 & \\ 0 & 0 \\ \vdots & \\ 0 & \end{array} \right)$

but $\begin{array}{l} f: R \to M \\ \quad A \mapsto Ae_1 \end{array}$ is not an isomorphism (e.g. $f\left(\left[\begin{array}{c|c} 1 & \\ 0 & A \\ \vdots & \\ 0 & \end{array}\right]\right) = f\left(\left[\begin{array}{c|c} 1 & \\ 0 & A' \\ \vdots & \\ 0 & \end{array}\right]\right)$ for any $A \neq A' \in M_{n\times n-1}(k)$)

(3) Vector spaces are modules over k. They are all free, since any $V \cong k^{(I)}$ for some I.

(4) Let $R = k[x,y]$, and $I = (x,y)$. Then I is <u>not</u> free, since x and y are not R-lin. independent. $\left(\underset{\substack{\cap \\ R}}{y} \cdot x + \underset{\substack{\cap \\ R}}{(-x)} \cdot y = 0\right)$

<u>Lemma 1.1.1</u>. Let $R \neq \{0\}$ be a ring. TFAE:

(a) R is a division ring. $(\forall a \neq 0 : \exists b : ab = ba = 1_R)$

(b)((c)) $\{0\}$ and R are the only right (left) ideals of R.

<u>Pf</u>: <u>(a) ⇒ (b)</u> [similar (a) ⇒ (c)] Note: $R = \overset{\text{generator!}}{1_R} \cdot R$. If $a \neq 0$, then $\exists b$ s.t. $a \cdot b = 1_R \Rightarrow \langle a \rangle_R = R$

<u>(b) ⇒ (a)</u> [similar (c) ⇒ (a)]: Let $a \neq 0 \in R$. Then by (b):

$$\langle a \rangle_R = aR = R \Longrightarrow \exists b \in R : \underline{ab = 1}.$$

Further, since $b \neq 0 \overset{(b)}{\Longrightarrow} \langle b \rangle = bR = R \Longrightarrow \exists \underset{\substack{\neq \\ 0}}{c} \in R : \underline{bc = 1}$

$$\Longrightarrow a = a \cdot 1 = a(bc) = (ab)c = c.$$

$$\Longrightarrow ba = 1, \text{ and so } b \text{ is an inverse of } a. \quad \square$$

<u>Lemma 1.1.2</u> Let R be a division ring. Then every R-module has a basis, and each two bases have the same cardinality.

Pf: (omitted) look at lin.alg pf of fact that every vector <u>space has a basis</u> + cardinality result) □

uses Zorn's lemma

from set theory!

The next notion should be familiar from commutative algebra: noetherian and artinian modules. First a lemma:

<u>Lemma 1.1.3</u> Let M be an (left - always assumed!) R-module. TFAE:

(a) Every non-empty set of submodules of M has a maximal (resp. minimal) element.

(b) Every ascending (resp. descending) chain of submodules of M becomes stationary. ACC (i.e. if $N_0 \subseteq N_1 \subseteq \dots$ are submods, then $\exists j \in \mathbb{N}$ s.t. $N_i = N_j$ $\forall i \geq j$)

(c) Every submodule of M is finitely generated. (resp. every factor module of M is f.g.) ($N \leq M \Rightarrow \exists u_1, \dots, u_n$ s.t. $N = {}_R\langle u_1, \dots, u_n \rangle$
($N \leq M$: $\exists \bar{u}_1, \dots, \bar{u}_n$ s.t. $M/N = {}_R\langle \bar{u}_1, \dots, \bar{u}_n \rangle$)

Rmk: (b) is called ACC (DCC)

Def: If M satisfies one of the conditions (a)-(c) of Lemma 1.1.3, then M is called noetherian (resp. artinian). The ring R itself is called left noetherian (resp. left-artinian) if ${}_RR$ is a noetherian (resp. artinian) R-module. Equivalently: every left ideal of R is finitely generated.

Same def for right noetherian (artinian).

If R is left and right-noetherian, then it is called noetherian.

(⤳ see examples in Ex. session!)

Rmk: Most examples will be at least one-sided noetherian.

Classical example of non-noetherian ring from commutative algebra: $R = k[x_1, x_2, x_3, \dots]$ polyn. ring in inf.-many vars, then $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \dots$ is a nonstationary ascending chain of ideals.

Pf (of Lemma 1.1.3): (b) ⇒ (a): Assume that R-module M has ACC. Assume that there is a nonempty set of R-submodules $\mathcal{N} \subseteq M$ without max. element. Choose $N_1 \in \mathcal{N}$, since there is no max. elt in $\mathcal{N}$, $\exists N_2 \subseteq \mathcal{N}$ such that $N_1 \subsetneq N_2$. Since N_2 is not maximal, $\exists N_3 \subseteq \mathcal{N}$ s.t. $N_1 \subsetneq N_2 \subsetneq N_3$. Continue this way to get contradiction to ACC.

(a) ⇒ (c): Let $N \leq M$ be a submodule, and let $\mathcal{N}$ be the family of f.g. submodules of M. Clearly, $\{0\} \in W$, and so $N \neq \emptyset$. Thus it has a max. element A. If $A \neq N$, then $\exists n \in N \setminus A$. The module $A' = A + Rn$ is then finitely generated, i.e. $A' \in W$, $+ A \subsetneq A'$. Contradiction to A max. $\Rightarrow A = N$ f.g.

<u>(c) ⟹ (b)</u>: Let $N_1 \leq N_2 \subseteq \ldots$ be an ascending chain of submod. Let $N := \bigcup_{i \in \mathbb{N}} N_i$. By (c) $\exists$ finite set of generators $\mathcal{U}$ of N. Since $\mathcal{U}$ is finite, it must be contained in some N_k, $k \geq 1$. But then $N_i = N_k$ $\forall i \geq k$. $\Rightarrow$ ACC. $\square$

<u>Rmk</u>: artinian works similar!

<u>Recall</u>: A <u>short exact sequence</u> (s.e.s.) of R-modules L, M, N is a diagram $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ s.t.
- $\operatorname{im}(f) = \ker(g)$.
- $\ker(f) = 0$ ← f inj.
- $\operatorname{im}(g) = N$ ← g surj.

<u>Lemma 1.1.4</u>: Let M be an R-module, L, N too.

(1) If $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ is s.e.s. of R-mods, then M is noeth. (artin.) $\Leftrightarrow$ L and N are noetherian (artinian).

(2) If $M = \bigoplus_{i=1}^{n} M_i$, then M is noetherian (artinian) $\Leftrightarrow M_1, \ldots, M_n$ are noetherian (artinian).

<u>Pf</u>: Exercise! (1): Note: $0 \to L \to M \to N \to 0 \Leftrightarrow 0 \to L \to M \to M/L \to 0$)

<u>⟹</u>: $L \hookrightarrow M$, so $\operatorname{im}(f) \cong L \leq M$ submod.

any asc. chain of submods in L is AC in M $\overset{\text{L-noeth}}{\Longrightarrow}$ statem. for L. If $N_1 \leq \ldots$ is AC in M/L then each $N_i \subseteq M_i \overset{\text{ACC in M}}{\Longrightarrow} M_i = M_{i'}$ $\forall i \geq i' \Rightarrow N_i = N_{i'}$

⟸: Prop 1.2 in [Goodearl - Warfield]

(2) Cor 1.3 in [Goodearl - Warfield].

In part: ideals and factor rings of a noeth. ring R are noetherian.

Cor 1.1.5: Let M be an R-module.

(1) TFAE: (a) R is left noetherian (left artinian).

(b) Every f.g. R-module is noetherian (artinian).

(2) If $f: R \to S$ is a ring epim. and R is left noetherian (left artinian), then the same is true for S.

(3) Let $R \subset S$ be a ring extension. If R is left noeth. and S is f.g. as R-module, then S is left noetherian.

Pf (1) (b) $\Rightarrow$ (a): obvious

(a) $\Rightarrow$ (b): Let M be f.g. R-module. Then $\exists n \in \mathbb{N}$ and epimorphism $f: R^n \to M$. Since R^n is noeth (artinian), M is noeth. (artinian) by Lemma 1.1.4.

(2) S is noeth. as R-module by 1.1.4. But any ideal in S is an R-module and R-submod of $S \overset{S \text{ noeth.}}{\Longrightarrow}$ any ideal f.g.

(3) Similar $\square$

Lemma 1.1.6 (Hilbert's basis theorem) If R is left noetherian, then $R[X]$ is left noetherian.

Pf: Adapt comm. Pf, see [G-W] Thm 1.9. .

Lemma 1.1.7. Let R be a division ring and M an R-module.

TFAE: (a) M is noetherian.

(b) M is artinian.

(c) $\dim_R(M) < \infty$.

Pf: Adapt comm. proof (uses f.c. modules and composition series $\rightsquigarrow$ see [Atiyah-MacDonald, Prop 6.10].

Remark 1.1.8 (1) Subrings of noetherian (artinian) rings need not be noetherian (artinian). Simple ex: $k[x,y]$ is noeth., but subring generated by by $\{xy^i, i \geq 0\}$ is not (!]

(2) Let $R \subset S$ be a ring extension. If S is comm. + noetherian and module finite (i.e. a f.g. R-module), then R is noetherian by the thm of Eakin-Nagata.