MA 312 Commutative Algebra / Jan–April 2020
(BS, Int PhD, and PhD Programmes)

Download from : http://www.math.iisc.ac.in/patil/courses/Current Courses/...

Tel : +91-(0)80-2293 3212 / 09449076304 **E-mails :** patil@math.ac.in

Lectures : Tuesday and Thursday ; 15:30–17:00 **Venue:** MA LH-5 / LH-1

2. Modules* [1]

Submit a solutions of *Exercises ONLY. **Due Date : Thursday, 06-02-2020**

Recommended to solve the violet colored R Exercises

* The concept of a module seems to have made its first appearance in Algebra in *Algebraic Number Theory* – in studying subsets of *rings of algebraic integers*. Modules first became an important tool in Algebra in late 1920's largely due to the insight of Emmy Noether (1882-1935), who was the first to realize the potential of the module concept. In particular, she observed that this concept could be used to bridge the gap between two important developments in Algebra that had been going on side by side and independently:the theory of representations (=homomorphisms) of finite groups by matrices due to Frobenius, Burnside, Schur et al and the structure theory of algebras due to Molien, Cartan, Wedderburn et al.

2.1 Let A be a commutative ring and V be an A-module with the action (ring) homomorphism $\vartheta : A \longrightarrow \operatorname{End}(V,+)$.

(a) If $a \in A$ is a unit in A, then the homothecy $\vartheta_a : V \to V\ x \mapsto ax$ is bijective. Give an example of a non-zero A-module V and a non-unit $a \in A$ such that the homothecy ϑ_a is bijective. (**Hint :** Consider $\mathbb{Z}$-modules, i. e. Finite abelian groups.)

(b) If $\varphi : A' \longrightarrow A$ is a ring homomorphism, then the composition ring homomorphism $\vartheta' = \vartheta \circ \varphi : A' \longrightarrow \operatorname{End}(V,+)$ defines the A'-module structure on V with the operation $(a',x) \mapsto a'x = \varphi(a')x$. It is called the induced A'-module structure on V by φ. Particularly important is the case when A' is a subring of A and $\varphi = \iota : A' \hookrightarrow A$ is the canonical inclusion. In this case the A'-operation on V is simply the restriction of the A-operation on V. For example, the restriction of the tautological

[1] **Module–structures.** Let A be a ring and $(V,+)$ an additive abelian group. If
$$A \times V \longrightarrow V\,, \quad (a,x) \longmapsto ax\,,$$
is an operation of the multiplicative monoid $(A,\cdot)$ of A on V as monoid of group homomorphism, i. e. the action homomorphism
$$\vartheta : A \longrightarrow \operatorname{End} V\,, \quad a \longmapsto (\vartheta_a : x \mapsto ax)\,,$$
is a homomorphism of $(A,\cdot)$ in the multiplicative monoid $(\operatorname{End} V, \circ)$ of the endomorphism ring $\operatorname{End} V = (\operatorname{End} V, +, \circ)$ of $(V,+)$. Since $\operatorname{End} V$ is a ring, it is natural to consider such an operation of A which is even a ring homomorphism. In other words, an additive abelain group $(V,+)$ together with an operation $A \times V \to V$ is called an (left) A-module or also a (left) module over A, if the action homomorphism of this operation is defined by a ring homomorphism $\vartheta = \vartheta_V : A \to \operatorname{End} V$, i. e. for all $a,b \in A$ and all $x,y \in V$, we have :
$$(1)\ \ (ab)x = a(bx)\,, \quad (2)\ \ a(x+y) = ax+by\,, \quad (3)\ \ (a+b)x = ax+bx\,, \quad (4)\ \ 1\cdot x = x\,.$$

On the ring A itself has two module structures which are compatible in the following sense : The homothecies of one structure commute with the homothecies of the other structure : $\lambda_a \circ \rho_a = \rho_a \circ \lambda_a$ for all $a,b \in A$, where $\lambda_a : A \to A$, $c \mapsto ac$ (resp. $\rho_a : A \to A$, $c \mapsto ca$) denoted the left (resp. right) multiplication on A by a.

More generally, two (left) module structures on the same abelian group $(V,+)$ with action (ring) homomorphisms $\vartheta : A \longrightarrow \operatorname{End}(V,+)$ and $\eta : B \longrightarrow \operatorname{End}(V,+)$ are compatible if the homothecies ϑ_a, $a \in A$ and η_b, $b \in B$, commute, i. e. $a(bx) = b(ax)$ for all $a \in A$, $b \in B$, $x \in V$. This means that the homothecies of one structure are linear with respect to the other structure. In such case one says that V is an A-B-bimodule. Every ring A is an A-$A^{\rm op}$-bimodule and every module over a *commutative* ring A with one and the same A-module structure is a A-A-bimodule.

Tautological module structure on an abelian group. Let $(W,+)$ be an abelian group. then the identity (ring) homomorphism $\operatorname{End}(W,+) \longrightarrow \operatorname{End}(W,+)$ defines the so-called tautolgical $\operatorname{End}(W,+)$-module structure on $(W,+)$ with the scalar multiplication $f\,x := f(x)$, $f \in \operatorname{End}(W,+)$ $x \in W$.

End $(V,+)$-module structure (see Footnote No. 1) on $(V,+)$ defines $\mathrm{End}_A V$-module structure on V. Every complex (i. e. $\mathbb{C}$-)vector space is also a real (i. e. $\mathbb{R}$-)vector space and every $\mathbb{R}$-vector space is also a $\mathbb{Q}$-vector space.

(c) (Torsion elements, Torsion and Torsion-free modules) An element $x \in V$ is called a torsion element of V if there exists a non-zerodivisor $a \in A^*$ with $ax = 0$ or equivalently if the annihilator $\mathrm{Ann}_A\, x$ contains a non-zerodivisor. The set of all torsion elements of V is denoted by $\mathrm{T}_A V$ which is obviously an A-submodule of V. For a non-zerodivisor $a \in A^*$, $\mathrm{T}_a V := \mathrm{Ker}\,\vartheta_a = \{x \in V \mid ax = 0\}$ is called the a-torsion of V. Then $Aa \subseteq \mathrm{Ann}_A \mathrm{T}_a V$ and hence $\mathrm{T}_a V$ is an (A/Aa)-module (see part (c) below), and $\mathrm{T}_A V = \bigcup_{a\in A} \mathrm{T}_a V$. Further, V is called a torsion module if $\mathrm{T}_A V = V$ and is called torsion-free if $\mathrm{T}_A V = 0$.

(d) (Annihilator of an A-module) The ideal

$$\mathrm{Ann}_A V := \mathrm{Ker}\,\vartheta = \{a \in A \mid ax = 0 \text{ for all } x \in V\} = \{a \in A \mid aV = 0\}$$

is called the Annihilator of the A-module V. Clearly, $\mathrm{Ann}_A V = \bigcap_{x\in V} \mathrm{Ann}_A\, x$, where $\mathrm{Ann}_A\, x := \{a \in A \mid ax = 0\}$ is the annihilator of the element $x \in V$ which is the kernel of the A-module homomorphism $A \to V$, $a \mapsto ax$. The A-module V is called a faithful A-module if $\mathrm{Ann}_A V = 0$, i. e. the action (ring) homomorphism $\vartheta : A \to \mathrm{End}_A(V,+)$ is injective.

(e) Let $\mathfrak{a}$ be an ideal in A with $\mathfrak{a} \subseteq \mathrm{Ann}_A V$. Then the action ring homomorphism $\vartheta : A \to \mathrm{End}\,(V,+)$ induces a homomorphism $\overline{\vartheta} : A/\mathfrak{a} \longrightarrow \mathrm{End}\,(V,+)$ of rings and hence induces an $(A/\mathfrak{a})$-module structure on V with scalar multiplication $\overline{a}x = ax$ and $\mathrm{Ann}_{(A/\mathfrak{a})} V = (\mathrm{Ann}_A V)/\mathfrak{a}$. Conversely, $(A/\mathfrak{a})$-module structure on $(V,+)$ defines an A-module structure using the canonical residue-class ring homomorphism $\pi_{\mathfrak{a}} : A \to A/\mathfrak{a}$ with $\mathfrak{a} \subseteq \mathrm{Ann}_A V$. Therefore the $(A/\mathfrak{a})$-modules and the A-modules whose annihilator contain $\mathfrak{a}$ are one and the same. The annihilator of an abelian group $(W,+)$ (as $\mathbb{Z}$-module) is the ideal $\mathbb{Z}\,\mathrm{Exp}\,W \subseteq \mathbb{Z}$. For $m \in \mathbb{N}$, the abelian groups with $\mathrm{Exp}\,W \mid m$ and the $\mathbf{A}_m$-modules are one and the same. In particular, for a prime number $p \in \mathbb{P}$, elementary abelian p-groups and $\mathbf{F}_p$-vector spaces are identical objects.

2.2 Let U, W, U', W' be submodules of an R-module V. Then :

(a) (Modular Law) If $U \subseteq W$, then $W \cap (U + U') = U + (W \cap U')$.

(b) If $U \cap W = U' \cap W'$, then U is the intersection of $U + (W \cap U')$ and $U + (W \cap W')$.

2.3 Let U and W be A-submodules of the A-module V.

(a) Obtain the following canonical isomorphisms: $U/(U \cap W) \xrightarrow{\sim} (U + W)/W$, and if $U \subseteq W$, then $V/W \xrightarrow{\sim} (V/U)/(W/U)$.

(b) The following so-called Mayer-Vietoris Sequences:

$$0 \longrightarrow U \cap W \longrightarrow U \oplus W \longrightarrow U + W \longrightarrow 0$$

$$0 \longrightarrow V/(U \cap W) \longrightarrow (V/U) \oplus (V/W) \longrightarrow V/(U + W) \longrightarrow 0$$

are exact, where the non-trivial homomorphisms in the first sequence are defined by $x \longmapsto (x, -x)$ and $(x, y) \longmapsto x + y$, respectively and in the second sequence are defined (analogously) by $\overline{x} \longmapsto (\overline{x}, -\overline{x})$ and $(\overline{x}, \overline{y}) \longmapsto \overline{x + y}$, respectively.

In particular, if $A = K$ is a field, then from the first exact sequences we get the so-called dimension formula:

$$\mathrm{Dim}_K U + \mathrm{Dim}_K W = \mathrm{Dim}_K (U \cap W) + \mathrm{Dim}_K (U + W)$$

and from the second we get the so-called codimension formula:

$$\mathrm{Codim}_K U + \mathrm{Codim}_K W = \mathrm{Codim}_K (U \cap W) + \mathrm{Codim}_K (U + W)$$

2.4 Let U, V and W be modules over a commutative ring A. Then :

(a) If $\mu_A(V) \in \mathbb{N}$, then every generating system of V contains a finite generating subsystem. (Recall that The infimum of the cardinal numbers of the generating systems of V (which exists by the well ordering of cardinal numbers!) is called the m i n i m a l n u m b e r o f g e n e r a t o r s f o r V and is denoted by $\mu_A(V)$. If $\mu_A(V) \in \mathbb{N}$, then V is called a f i n i t e A-module. If $\mu_A(V) \leq 1$, i.e. V is generated by (at most) one element, then V is called c y c l i c. Note that $\mu_A(0) = 0$.

— **Remarks:** Note that a minimal generating system of a finite A-module can contain more than $\mu_A(V)$ elements. For example, $\{2,3\}$ is a minimal generating system for the cyclic $\mathbb{Z}$-module $\mathbb{Z}$. Further, an A-module V may not have any minimal generating system. Then naturally, $\mu_A(V)$ is infinite. For example, the $\mathbb{Z}$-module $\mathbb{Q}$ has no minimal generating system, see the Exercise below.)

(b) For every $m \in \mathbb{N}^*$, there is a minimal generating system for the abelian group $\mathbb{Z}$ with exactly m elements.

(c) Suppose that $\mu_A(V)$ is not finite. Then every generating system of V has a generating subsystem with $\mu_A(V)$ elements. In particular, every minimal generating system of V has $\mu_A(V)$ elements.

(d) If $0 \to U \xrightarrow{f} V \xrightarrow{g} W \to$ is an exact sequence of A-modules and A-module homomorphisms, then $\mu_A(V) \leq \mu_A(U) + \mu_A(W)$. — In particular, if both U and W are finitely generated, then V is finitely generated.

2.5 The $\mathbb{Z}$–module $\mathbb{Q}$ does not have minimal generating system. (**Hint:** In fact the additive group $(\mathbb{Q},+)$ does not have a subgroup of finite index $\neq 1$. This follows from the fact that the group $(\mathbb{Q},+)$ is divisible[2] and hence every quotient group of $(\mathbb{Q},+)$ is also divisible. Further, *If H finitely generated divisible abelian group, then $H = 0$.* — More generally, the quotient field $\mathrm{Q}(A)$ of an integral domain A which is not a field, has no minimal generating system as an A-module. In particular, $\mathrm{Q}(A)$ is not finitely generated A-module.)

2.6 Let V be an A-module over a ring A.

(a) If $Y \subseteq V$ is an infinite generating system for V. then every generating system x_i, $i \in I$, of V contains a generating system x_j, $j \in J \subseteq I$ with $\#J \leq \#Y$. In particular, if V has a countable generating system then every generating system of V contains a countable generating system.

(b) If every ideal in A is generated by r elements and if V is generated by n elements, then every A-submodule of V is generated by nr elements. In particular, over principal ideal ring every submodule of a module generated by n elements is also generated by n elements. (**Hint:** By induction on n. Suppose $V = Ax_1 + \cdots + Ax_n$ and $f : V \to V/Ax_1$ is the residue-class map, then consider the restriction map $f|U : U \to V/Ax_1$ and note that if V_1, V_2 and U are submodules of V with $V_1 \subseteq V_2$. Then $(V_2 \cap U)/(V_1 \cap U)$ is isomorphic to a submodule of V_2/V_1, and $(V_2 + U)/(V_1 + U)$ is isomorphic to a residue-class module of V_2/V_1.)

2.7 Let V be an A-module over the local ring A with the unique maximal ideal (= the Jacobson-Radical $\mathfrak{m}_A$ and v_i, $i \in I$, be a family of elements of V.

(a) If v_i, $i \in I$, is a generating system of V, then v_i, $i \in I$, is minimal if and only if $\mathrm{Syz}_A(v_i, i \in I) \subseteq \mathfrak{m}_A A^{(I)}$. (**Hint:** Use $A^\times = A \smallsetminus \mathfrak{m}_A$.) Moreover, in this case, the residue classes $[v_i] \in V/\mathfrak{m}_A V$, $i \in I$, form a $(A/\mathfrak{m}_A)$-basis of $V/\mathfrak{m}_A V$, and

$$\mu_A(V) = |I| = \mathrm{Dim}_{A/\mathfrak{m}_A}(V/\mathfrak{m}_A V).$$

In particular, for every finite A-module V : $\mu_A(V) = \mathrm{Dim}_{A/\mathfrak{m}_A}(V/\mathfrak{m}_A V)$ and $V = 0$ if and only if $V = \mathfrak{m}_A V$.

---

[2] **Divisible abelian groups.** An abelian (additively written) group H is d i v i s i b l e if for every $n \in \mathbb{Z}$, the group homomorphism $\lambda_n : H \to H$, defined by $a \mapsto na$ is surjective. For example, the group $(\mathbb{Q},+)$ is divisible, the group $(\mathbb{Z},+)$ and finite groups are not divisible. Further, *quotient of a divisible group is also divisible. Free abelian groups of finite rank are not divisible.*

(b) (Lemma von Nakayama) If $U \subseteq V$ is an A-submodule of V such that the residue class module V/U is finite and if $V = U + \mathfrak{m}_A V$, then $V = U$. (**Hint:** Note that $V/U = \mathfrak{m}_A(V/U)$ and hence $V/U = 0$.) If V is finite, then the elements v_i, $i \in I$, generates V if and only if their residue classes generate the vector space $V/\mathfrak{m}_A V$ over the field $A/\mathfrak{m}_A$.

2.8 Let K be a field.
(a) Let A be a subring of K such that K is the quotient field of A. If K is a finite A-module, then $A = K$. In particular, $\mathbb{Q}$ is not a finite $\mathbb{Z}$–module. (**Hint:** Suppose $K = Ax_1 + \cdots + Ax_n$ and $b \in A$, $b \neq 0$, with $bx_i \in A$ for $i = 1, \ldots, n$. Now, try to express $1/b^2$ as a linear combination of $x_i, i = 1, \ldots, n$.)
(b) More generally, if A is a subring of K and if the A-module K is finite, then A itself is a field. (**Hint:** Let $x_1, \ldots, x_m \in K$ be a A-generating system of K , $\mathrm{Q}(A)$ be the quotient field of A contained in K and let $y_1, \ldots, y_n$ be a $\mathrm{Q}(A)$-basis of K with $y_1 = 1$. Then $y_1^*(x_1), \ldots, y_1^*(x_m)$ is an A-generating system of $\mathrm{Q}(A)$, where y_1^* is the first coordinate function with respect to the basis $y_1, \ldots, y_n$. Now use the part (a).)

***2.9** Let A be an integral domain with quotient field K. Then :

(a) If V is a torsion module (See Exercise 2.1) over A, then $\mathrm{Hom}_A(V, A) = 0$.

(b) $\mathrm{Hom}_A(K, A) \neq 0$ if and only if $A = K$. In particular, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = 0$. (**Hint:** Every element $f \in \mathrm{Hom}_A(K, A)$ is a homothecy of K by the element $f(1)$.)

(c) If K is an A-submodule of an arbitrary direct sum of finite A-modules, then $A = K$.

(**Solution:** Suppose V_i, $i \in I$, is a family of finite A-modules with $K \subseteq \bigoplus_{i\in I} V_i$ and $\iota : K \to \bigoplus_{i\in I} V_i$ is the natural injective A-module homomorphism. We shall apply the part (b) to conclude that $A = K$. For this we need to prove that $\mathrm{Hom}_A(K, A) \neq 0$. Note that $\iota(1)$ is not a torsion element in V (if $a \in A$ and if $\iota(a) = a \cdot \iota(1) = 0$, then $a = 0$, since $\iota : K \to \bigoplus_{i\in I} V_i$ injective A-module homomorphism) and there exists a finite subset $J \subseteq I$ such that $(x_i)_{i\in I} = \iota(1) \in \bigoplus_{i\in I} V_i$ with $0 \neq x_j \in V_j$ for all $j \in J$ and $x_i = 0$ for all $I \smallsetminus J$. Now, consider the composite A-module homomorphsim :

$$f : K \xrightarrow{\iota} \textstyle\bigoplus_{i\in I} V_i \xrightarrow{\pi_J} \bigoplus_{j\in J} V_j \xrightarrow{\pi} \bigoplus_{j\in J} (V_j/\mathrm{t}_A V_j),$$

where π_J is the projection of $\bigoplus_{i\in I} V_i$ onto $\bigoplus_{j\in J} V_j$ and π is the product of the canonical residue-class homomorphism $V_j \to V_j/\mathrm{t}_A V_j$, $y \mapsto \bar{y}$, $j \in J$, modulo the torsion-submodules. Note that, since $\iota(1)$ is not a torsion element, it follows that $\overline{x_j} \neq 0$ for some $j \in J$ and hence $y := f(1) = \left(\overline{x_j}\right)_{j\in J} \neq 0$. Altogether, we have a finite torsion-free A-module $W := \bigoplus_{j\in J} (V_j/\mathrm{t}_A V_j)$ and a *non-zero* A-module homomorphism $f : K \to W$. Now, we use the following Exercise to conclude that $\mathrm{Hom}_A(K, A) \neq 0$ and hence can apply (b) to get the required equality $A = K$.

Exercise *For every finite torsion-free module W over an integral domain A is torsion-less* [3], i. e. for every $y \in W$, $y \neq 0$, there exists a linear form $\varphi : W \to A$ with $\varphi(y) \neq 0$.

Solution: It is enough to prove that there exists an injective A-module homomorphism $W \to F$ where F is a finite free A-module. Let $w_1, \ldots, w_m \in W$ be a maximal linearly independent over A subset of W and put $F := Ax_1 + \cdots + Ax_m \subseteq W$. Then F is a free A-submodule of W with A-basis $x_1, \ldots, x_m$. Note that every $w \in W$, there exists $a \in A$, $a \neq 0$ with $aw \in F$ by the maximal linear independence property of the subset $\{x_1, \ldots, x_n\}$. Since W is finite, it follows that there exists $0 \neq a \in A$ with $aW \subseteq F$. With this the composite map $W \xrightarrow{\lambda_a} aW \xrightarrow{\iota} F$ is an injective A-module homomorphism.)

[3] **Torsionless modules** An A-module V over a commutative ring A is called torsionless if for every two elements $x, y \in V$, there exists a linear form $\varphi : V \to A$ on V with $\varphi(x) \neq \varphi(y)$. An A-module V is torsionless if and only if for every $z \in V$, $z \neq 0$, there exists a linear form $\varphi : V \to A$ with $\varphi(z) \neq 0$.
Submodules of torsionless module are torsionless. The arbitrary I-fold direct product A^I are torsionless, since two distinct I-tuples $(b_i), (c_i)$ have distinct values under at least one A-linear projection $(a_i) \mapsto a_j$. Free A-modules are torsionless : If x_i, $i \in I$, is an A-basis of V, then the coordinate functions x_i^*, $i \in I$, are A-linear and for two distinct elements $x, y \in V$, $x_i^*(x) \neq x_i^*(y)$ for some $i \in I$. *Every torsionless A-module V is torsion-free.* Converse is not true in general, for example, the $\mathbb{Z}$-module $\mathbb{Q}$ is torsion-free, but not torsionless, see Exercise 2.7 (b). However, Finite torsion-free modules over an integral domain are torsionless, see the above proof.

2.10 Let A be a commutative ring and let V_i, $i \in I$, be an infinite family of non-zero A-modules. Prove that $W := \bigoplus_{i \in I} V_i$ is not a finite A-module.

2.11 Let A be a non-zero ring and let I be an *infinite* indexed set. For every $i \in I$, let e_i be the I-tuple $(\delta_{ij})_{j \in I} \in A^I$ with $\delta_{ij} = 1$ for $j = i$ and $\delta_{ij} = 0$ for $j \neq i$.

(a) The family e_i, $i \in I$, is a minimal generating system for the ideal $A^{(I)}$ in the ring A^I. In particular, $A^{(I)}$ is not finitely generated ideal. (**Remark:** Submodules of finitely generated modules need not be finitely generated!)

(b) There exists a generating system for the A^I-module $A^{(I)}$ that does not contain any minimal generating system. (**Hint:** First consider the case $I = \mathbb{N}$ and the tuples $e_0 + \cdots + e_n$, $n \in \mathbb{N}$.)

2.12 Let A be a non-zero commutative ring.

(a) The ring A is a field if and only if every A-module is free.

(b) Let $V = Ax$ be a cyclic free A-module with basis x. Then $y = ax \in V$, $a \in A$ is a basis of V if and only if $a \in A^\times$.

2.13 Let A be a commutative ring, $A \neq 0$ and let V be an A-module. with generating system x_i, $i \in I$. If $W \subseteq V$ is a free A-submodule of V then $\mathrm{Rank}_A W \leq \# I$.

2.14 (Simple modules) Let A a non-zero (not necessarily commutative) ring. An A-module V is called a simple A-module if $V \neq 0$ and the only submodules of V are the trivial submodules 0 and V.

(a) For an A-module V, the following statements are equivalent:
(i) V is simple.
(ii) Every homomorphism $V \to W$ of A-modules is either the zero-homomorphism or is injective.
(iii) $V = Ax$ for every $x \in V \smallsetminus \{0\}$.
(iv) V is isomorphic to a residue-class module $A/\mathfrak{m}$, where $\mathfrak{m}$ is a maximal left-ideal in A.

(b) Let V be simple A-module. Then the *annihilator* (See Exercise 2.1) ideal $\mathrm{Ann}_A V$ of V is the intersection of the maximal left-ideals $\mathrm{Ann}_A x$, $x \in V \smallsetminus \{0\}$.

2.15 Let A be a (not necessarily commutative) ring and let $f : V \to W$ be a homomorphism of A-modules.

(a) For a submodule $U \subseteq V$, we have $f^{-1}(f(U)) = U + \mathrm{Ker} f$ and
$$U/(U \cap \mathrm{Ker} f) \xrightarrow{\sim} (U + \mathrm{Ker} f)/\mathrm{Ker} f \xrightarrow{\sim} f(U).$$

(b) If f surjective, then the maps $U \mapsto f(U)$ and $X \mapsto f^{-1}(X)$ are inverse maps of each other between the set of submodules U of V containing $\mathrm{Ker} f$ and the set of all submodules X of W.

(c) Let V and W be simple A-modules (see the above Exercise). Then every A-homomorphism $V \longrightarrow W$ is either the zero-homomorphism or is an isomorphism. In particular, (Lemma of (Issai) Schur): $\mathrm{End}_A V$ is a division ring[4].

(d) If A is commutative, then the modules $A/\mathfrak{m}$, $\mathfrak{m} \in \mathrm{Spm} A$, up to isomorphism, are the only simple A-modules and distinct maximal ideals of A define non-isomorphic simple

[4] A ring is called a division ring if $(A \smallsetminus \{0\} \cdot)$ is a (not necessarily commutative) group with neutral element $1 \neq 0$.

A-modules. (**Remark :** Note that $\operatorname{Ann}_A(A/\mathfrak{m}) = \mathfrak{m}$. — The classification of the simple modules over non-commutative rings is complicated. Over a local ring A with Jacobson-radical $\mathfrak{m}_A$, up to isomorphism of A-modules, the residue-class division ring $A/\mathfrak{m}_A$ is the only simple A-module.)

R **2.16** Let V be a vector space over a field K.

(a) If $V \neq 0$, then V is a simple $\operatorname{End}_K V$-module (See Exercise 2.1) The endomorphisms of V as $\operatorname{End}_K V$-module are the homothecies ϑ_a, $a \in K$, of V. In particular, $\operatorname{End}_{\operatorname{End}_K V} V \xrightarrow{\sim} K$ is the image of the action homomorphism $\vartheta : K \longrightarrow \operatorname{End} V$. The Jacobson-Radical of $\operatorname{End}_K V$ is 0. (**Hint :** Note that $\operatorname{Ann}_{\operatorname{End}_K V} V = \bigcap_{x \in V} \operatorname{Ann}_{\operatorname{End}_K V} x = 0$.)

(b) Let V be a finite dimensional vector space over the field K of dimension $n > 0$. Then $\operatorname{End}_K V$ is a simple ring[5]. (**Hint :** If $f \in \operatorname{End}_K V$ and if $v_1, \ldots, v_n \in V$ is a K-basis of V with $f(v_1) \neq 0$, then the two-sided ideal generated by f in $\operatorname{End}_K V$ contains an element f_1 with $f_1(v_j) = \delta_{1j}(v_j)$, $j = 1, \ldots, n$ and hence also contains id_V.)

(c) For every K-basis $v_1, \ldots, v_n$ of V, the map $\operatorname{End}_K V \longrightarrow V^n$, $f \longmapsto (f(v_1), \ldots, f(v_n))$, is an isomorphism of $\operatorname{End}_K V$-modules, and V is the *only* simple left $(\operatorname{End}_K V)$-module, up to isomorphism.

(d) Suppose that $\alpha = \operatorname{Dim}_K V \geq \aleph_0 := \#\mathbb{N}$, i. e. V is *not* finite dimensional. Then the maps $\beta \longmapsto \{f \in \operatorname{End}_K V \mid \operatorname{Rank} f < \beta\}$ and $\mathfrak{b} \longmapsto \operatorname{Min}\{\gamma \mid \operatorname{Rank} f < \gamma \text{ for all } f \in \mathfrak{b}\}$ are inverse isomorphisms to each other from the (well ordered) set of infinite cardinal numbers $\beta \leq \alpha$ and the set (ordered by the inclusion) of two-sided ideals $\mathfrak{b} \subseteq \operatorname{End}_K V$ with $0 \neq \mathfrak{b} \neq \operatorname{End}_K V$. In particular, $\mathfrak{m}_\alpha := \{f \in \operatorname{End}_K V \mid \operatorname{Dim}_K \operatorname{Img} f < \alpha\}$ is the *only* maximal two-sided ideal in $\operatorname{End}_K V$. The ring $(\operatorname{End}_K V)/\mathfrak{m}_\alpha$ is simple, but not a division ring. — How many two-sided ideals are there in the ring $\operatorname{End}(\mathbb{R}, +) = \operatorname{End}_{\mathbb{Q}} \mathbb{R}$?

(**Hints and Remarks :** Recall that for $f \in \operatorname{End}_K V$, $\operatorname{Rank}_K f := \operatorname{Dim}_K \operatorname{Img} f$. Put $B := \operatorname{End}_K V$. The map $Bf \longmapsto \operatorname{Ker} f$ is an anti-isomorphism of lattices from the lattice $\{Bf \mid f \in B\}$ of left-ideals in B onto the lattice of all K-subspaces of V. Moreover, if V is finite dimensional then the ring B is left-principal ideal ring as well as right-principal ideal ring.)

* **2.17** Let V be an A-module over the ring A and $U \subseteq V$ be an A-submodule of V. Recall that, by definition, U is a direct summand of V if U has an A-module complement $W \subseteq V$, i. e. $V = U \oplus W$.

(a) The A-submodule U is a direct summand of V if and only if there exists a *projection* $p \in \operatorname{End}_A V$, i. e. $p^2 = p$ with $\operatorname{Img} p = U$. In this case $V = U \oplus W$ with $W := \operatorname{Ker} p$, and $p = p_{U,W}$ is the projection onto U along W, and the complementary projection $q = q_{U,W} = \operatorname{id}_V - p_{U,W} = p_{W,U}$ is the projection along U onto W.

(b) If $A = K$ is a field, then every subspace $U \subseteq V$ has a complement.

(c) Let W be a complement of U. Then the map $f \longmapsto \Gamma_f = \{f(y) + y \mid y \in W\} \subseteq V$ is a bijection from $\operatorname{Hom}_A(W, U)$ onto the set of all complements of U in V.

2.18 Let V be an A-module over the ring $A \neq 0$. We say that V is indecomposable if $V \neq 0$ and it has *no* direct sum decomposition $V = U \oplus W$ with submodules $U \neq 0 \neq W$ of V.

(a) The A-module V is irreducible if and only if $V \neq 0$ and the endomorphism ring $\operatorname{End}_A V$ has no non-trivial idempotent elements. Every simple A-module is indecomposable. Give

[5] **Simple ring.** A ring A is called simple if $A \neq 0$ and if 0 and A are the only two-sided ideals in A. Note that A ring, $A \neq 0$, is simple if and only if every ring homomorphism $A \to B$ from A into a ring B with $B \neq 0$, is injective. Division rings are obviously simple, but not every simple ring is a division ring! *Commutative* simple rings are fields.

an example of an indecomposable module which is not simple. The ring A as A-(left- or right-) module is indecomposable if and only if the ring A has no non-trivial idempotent elements.
(**Remark :** Note the difference between the irreducibility of the ring A as A-(left- or right-) module and that of A as the ring. The later is equivalent with the condition that A has no non-trivial *central* idempotent elements.)

(b) The only indecomposable vector spaces over a field K are one dimensional vector spaces. (**Remarks :** In general it difficult — if not impossible to classify the indecomposable modules over a given ring A. The finitely generated indecomposable abelian groups (= $\mathbb{Z}$-modules) are precisely the cyclic groups $\mathbb{Z} = \mathbf{Z}_0$ and $\mathbf{Z}_{p^\alpha}$, $p \in \mathbb{P}$, $\alpha \in \mathbb{N}^*$. This is essentially the *Structure Theorem for finitely generated abelian groups.* But there are many more indecomposable abelian groups, for example, all subgroups $\neq 0$ of $\mathbb{Q} = (\mathbb{Q}, +)$ are indecomposable and similarly all Prüfer's p-groups[6] $\mathrm{I}(p)$, $p \in \mathbb{P}$, are also indecomposable. Every abelian p-group with 1-dimensional (i. e. non-zero cyclic) p-socal[7] is indecomposable. Up to isomorphism these are precisely the groups $\mathbf{Z}_{p^\alpha}$, $\alpha \in \mathbb{N}^*$, and $\mathrm{I}(p)$. Why?)

2.19 Let A be a non-zero ring. Then

(a) If $A^m \xrightarrow{\sim} A^{m+1}$ (as A-modules) for $m \in \mathbb{N}$, then $A^m \xrightarrow{\sim} A^n$ for all $n \geq m$.

(b) Let $x, y \in A$. then x, y is a basis of the A-module A if and only if there exists elements $a, b \in A$ with (i) $ax + by = 1$, (ii) $xa = 1$, (iii) $xb = 0$, (iv) $ya = 0$, and (v) $yb = 1$. (Equivalently,

$$\begin{pmatrix} x, & y \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = (1) , \quad \begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} x, & y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} ,$$

where all matrices are considered over the opposite ring A^{op}, see Footnote No. 10 also.)

(c) Let B be a ring $\neq 0$ and V be a B-module $\neq 0$ with $V \cong V \oplus V$ (for example, a free B-module with infinite basis). Then in the endomorphism ring $A := \mathrm{End}_B V$, there exists elements a, b, x, y, which satisfy the equations (i) to (v) in (b) above. In particular, the finite free A-modules do not have rank. (**Hint :** Describe inverse isomorphisms of each other $V \xrightarrow{\sim} V \oplus V$ and $V \oplus V \xrightarrow{\sim} V$ with matrices over the ring $\mathrm{End}_A V$.)

2.20 *Let $\varphi : A \longrightarrow B$ be a homomorphism of rings. If every free B-module has a rank, then every free A-module also has a rank.*

(**Proof :** We need to show that : If $m, n \in \mathbb{N}$ and $A^m \cong A^n$ (as A-modules), then $m = n$. Let $f : A^n \to A^m$ and $g : A^m \to A^n$ be inverse A-isomorphisms to each other which are described[8] by the matrices

---

[6] **Prüfer's p-group.** For a prime number $p \in \mathbb{P}$, the p-primary component of the torsion group $\mathbb{Q}/\mathbb{Z}$ and every other group which isomorphic to it, is called the Prüfer's p-group (named in the honour of Prüfer, E. P. H (1896-1934) and is denoted by $\mathrm{I}(p)$. For an arbitrary group G and a prime number $p \in \mathbb{P}$, the subset $G(p) := \cup_{n \in \mathbb{N}} \mathrm{T}_{p^n} G := \{x \in G \mid \mathrm{Ord}\, x \text{ is a power of } p\} \, (\subseteq \mathrm{T}(G) := \{x \in G \mid \mathrm{Ord}\, x > 0\})$ is called the p-primary component of G.

[7] p-**Socal of a group.** For a prime number $p \in \mathbb{P}$, the p-torsion ${}_pG := \{x \in G \mid x^p = e_G\}$ of an arbitrary group G is called the p-socal of G. If G is abelian, then the p-socal ${}_pG = \mathrm{Ker}\,(G \to G, x \mapsto x^p)$ is an elementary abelian p-group, see the Remark in the Exercise 1.3 (b).

[8] *Every A-module homomorphism $f : A^n \longrightarrow A^m$ can be described by a $m \times n$-matrix $\mathfrak{A} = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in$* $\mathrm{M}_{m,n}(A^{\mathrm{op}})$. We write elements $x \in A^n$ (resp. $y \in A^m$) as 1-column matrices with n (resp. m) rows, then

$$f(x) = \mathfrak{A}x = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix} = y \text{ with } y_i = \sum_{j=1}^{n} x_j a_{ij} \, , \; 1 \leq i \leq m \, .$$

Note that the entries in the matrices are considered in the opposite ring A^{op} and are multiplied there! This provides the summands $x_j a_{ij}$ instead of $a_{ij} x_j$ and this is also followed in the multiplication of matrices as well. Therefore : *The endomorphism ring* $\mathrm{End}_A A^n$ *of the free A-module A^n is the ring* $\mathrm{M}_n(A^{\mathrm{op}})$ *of the square $n \times n$-matrices with entries in the opposite ring* A^{op}. The identity of $\mathrm{End}_A A^n$ is represented by the unit matrix $\mathfrak{E}_n = (\delta_{ij})) \in \mathrm{M}_n(A)$. In the important case when A is commutative, naturally one need not distinguish the rings A and A^{op}.

$\mathfrak{A}=(a_{ij})\in \mathrm{M}_{m,n}(A^{\mathrm{op}})$ and $\mathfrak{B}=(b_{jk})\in \mathrm{M}_{n,m}(A^{\mathrm{op}})$. Then the product matrices $\mathfrak{B}\mathfrak{A}\in \mathrm{M}_n(A)$ and $\mathfrak{A}\mathfrak{B}\in \mathrm{M}_m(A)$ describe the compositions $g\circ f=\mathrm{id}_{A^n}$ and $f\circ g=\mathrm{id}_{A^m}$, respectively, where $\mathfrak{E}_n$ and $\mathfrak{E}_m$ denote the unit matrices. Then the φ-images $\varphi(\mathfrak{A})=(\varphi(a_{ij}))\in \mathrm{M}_{m,n}(B^{\mathrm{op}})$ and $\varphi(\mathfrak{B})=(\varphi(b_{jk}))\in \mathrm{M}_{n,m}(B^{\mathrm{op}})$ describe the inverse B-isomorphisms of each other $B^n\to B^m$ and $B^m\to B^n$, respectively. Therefore $m=n$ by hypothesis on B. •

— **Remark :** The *Theory of Rings* is the theory of modules over rings where as in the *Commutative Algebra* all modules over noetherian commutative rings are studied. The large part of *Linear Algebra* is concentrated to study linear maps between free modules and in particular, determining the structure of the linear maps between the vector spaces (by the Theorem on the *Existence of bases* (for vector space) which are readily free). Moreover, in the case of a field K, the homomorphism groups $\mathrm{Hom}_K(V,W)$ are even K-vector spaces and hence free.)