# MA 312 Commutative Algebra / Aug–Dec 2017

(Int PhD. and Ph. D. Programmes)

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

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

**Lectures :** Wednesday and Friday ; 14:00–15:30 **Venue:** MA LH-2 ( **if LH-1 is not free** ) / LH-1

**Seminars :** Sat, Nov 18 (10:30–12:45) ; Sat, Nov 25 (10:30-12:45)

**Final Examination :** Tuesday, December 05, 2017, 09:00–12:00

## Supplement 1A

## Modules*

* 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, 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.

**S1A.1** (Module–structures) Let $R$ be a ring and $V$ an additive abelain group. If

$$R\times V\to V\,,\quad (a,x)\mapsto ax\,,$$

is an operation of the multiplicative monoid $(R,\cdot)$ of $R$ on $V$ as monoid of group homomorphism, i.e. the action homomorphism

$$\vartheta : A\to \operatorname{End} V\,,\quad a\mapsto (\vartheta_a : x\mapsto ax)\,,$$

is a homomorphism of $(R,\cdot)$ 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 $R$ which is even a ring homomorphism.

Let $R$ be a ring. An additive abelain group $(V,+)$ together with an operation $R\times V\to V$ is called an $R$-module or also a module over $R$, if this operation is defined (the action homomorphism) 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 :

$$(1)\ \ (ab)x=a(bx)\,,\quad (2)\ \ a(x+y)=ax+by\,,\quad (3)\ \ (a+b)x=ax+bx\,,\quad (4)\ \ 1\cdot x=x\,.$$

A map $f : V\to W$ of the $R$-module $V$ in the $R$-module $W$ is an $R$-homomorphism or a homomorphism of $R$-modules or a $R$-linear map, if $f$ is a homomorphism of the additive groups of $V$ and $W$, which is compatible with the operations $\vartheta_V$ and $\vartheta_W$ of $R$ on $V$ resp. $W$, i.e. if $f\circ\vartheta_{V,a}=\vartheta_{W,a}\circ f$ for all $a\in R$, i.e. if for all $a\in R$ and all $x,y\in V$, we have:

$$f(x+y)=f(x)+f(y)\,,\quad f(ax)=af(x)\,.$$

The modules over a division domain $K$ are called $K$-vector spaces or vector spaces over $K$.

The operation $R\times V\to V$ of an $R$-module $V$ is called the scalar multiplication of $V$. It is biadditive. In particular, $0\cdot x=0=a\cdot 0$ for all $x\in V$ and all so-called scalars $a\in R$. The operation $\vartheta_a : V\to V$, $x\mapsto ax$, of $a\in R$ on $V$ is called the homothecy or stretching by $a$. If this is injective, then $a\in A$ called regular for the $R$-module $V$. The additive translation $\tau_{x_0} : x\mapsto x_0+x$ of $V$ by an element $x_0\in V$ is called called the shifting by $x_0$. The composition of $R$-homomorphisms is again an $R$-homomorphism. The set of all $R$-homomorphisms $f : V\to W$ of an $R$-module $V$ in an $R$-module $W$ is denoted by

$$\operatorname{Hom}_R(V,W)\,.$$

*Obviously, this is a subgroup of the group* $\operatorname{Hom}(V,W)$ of the homomorphisms of the additive groups of $V$ and $W$. Accordingly, denote by $\operatorname{Iso}_R(V,W)\subseteq\operatorname{Hom}_R(V,W)$ the set of all $R$-isomorphisms of $V$ onto $W$, i.e. the set of all bijective $R$-homomorphisms $V\to W$. *The set* $\operatorname{End}_R V:=\operatorname{Hom}_R(V,V)$ *of all the* $R$*-endomorphisms of* $V$ *is a subring of* $\operatorname{End} V$*, its whose unit group* $(\operatorname{End}_R V)^\times$ *is the group*

$$\operatorname{GL}_R V=\operatorname{Aut}_A V=\operatorname{Iso}_R(V,V)$$

*of the* $R$*-automorphisms of* $V$.[1] *If* $R$ is commutative*, then the homothecies* $\vartheta_{V,a}$*,* $a\in R$*, of an* $R$*-module* $V$ *are* $R$*-linear.* In this case, it follows that the $a$-fold $af=\vartheta_{W,a}\circ f=f\circ\vartheta_{V,a}$ of an $R$-homomorphism $V\to W$ is again an $R$-homomorphism, and one can easily check that with this scalar multiplication $\operatorname{Hom}_R(V,W)$ is an $R$-module. We summarise once again:

*If* $V$ *and* $W$ *are modules over the ring* $R$*, then* $\operatorname{Hom}_R(V,W)$ *is a subgroup of* $\operatorname{Hom}(V,W)$*. Moverover, if* $R$ *is commutative, then* $\operatorname{Hom}_R(V,W)$ *is an* $R$*-module with the scalarmultiplication* $af : x\mapsto af(x)=f(ax)$*,* $a\in R$*,* $f\in\operatorname{Hom}_R(V,W)$.

An $R$-submodule $U$ of $V$ is a subgroup of $(V,+)$, which is invariant under the scalar multiplication, i.e. $ax\in U$ for all $a\in R$ and $x\in U$. If $U_i\subseteq V$, $i\in I$, are submodules of $V$, then their sum $\sum_{i\in I}U_i\subseteq V$ is not only a subgroup, but even an $R$-submodule of $V$ and it is the smallest submodule of $V$ which contains all the $U_i$, $i\in I$. Images and inverse images of submodules under the $R$-linear map $f : V\to W$ of $R$-modules are obviously again submodules. In particular, $\operatorname{Img} f$ is a submodule of $W$ and $\operatorname{Ker} f=f^{-1}(0)$ is a submodule of $V$.

**S1A.2** (Examples of modules) (1) Let $W$ be an abelain group. The characteristic homomorphism $\chi : \mathbb{Z}\to \operatorname{End} W$, $a\mapsto\chi_a=a\,\mathrm{id}_W$, is the only ring homomorphism of $\mathbb{Z}$ into $\operatorname{End} W$. It follows that $W$ has a unique $\mathbb{Z}$-module

[1] Often, the suffix $R$ in the notation for sets of $R$-homomorphisms is suppressed if there is no doubt about the scalar ring $R$. Generally, the scalar ring $R$ is also often known as the base ring, if it is always (chosen) fixed.

structure, and it is given by the multiple-map $(a,x)\mapsto ax$, $a\in\mathbb{Z}$, $x\in W$. *Abelian groups and $\mathbb{Z}$-modules are one and the same, and* $\operatorname{Hom}(V,W)=\operatorname{Hom}_{\mathbb{Z}}(V,W)$ *for abelian groups $V,W$.*

(2) Let $R$ be a ring. The Cayley-homomorphism $R\to\operatorname{End}(R,+)$, $a\mapsto L_a$, defines an $R$-module structure on $R$, whose homothecies are the left translations $L_a$, $a\in R$. The corresponding operation $R\times R\to R$ is the (ring) multiplication of $R$. Unless otherwise specified, $R$ is considered with this $R$-module structure. *The $R$-submodules of $R$ are then precisely the left-ideals of $R$.*

If $f\colon R\to V$ is an $R$-homomorphism, then $f(a)=f(a\cdot 1)=af(1)$ for all $a\in R$. Therefore $f$ is uniquely determined by the value $f(1)$. Conversely, for arbitrary $v\in V$, the map $R\to V$, $a\mapsto av$ is an $R$-homomorphism. Therefore : *The map*

$$\operatorname{Hom}_R(R,V)\xrightarrow{\sim}V\,,\quad f\mapsto f(1)\,,$$

*is bijective and obviously, even a group isomorphism resp. an $R$-module homomorphism, if $R$ is commutative.* If $V=R$, then $(f\circ g)(1)=f(g(1))=g(1)f(1)$ for the composition of two $R$-endomorphisms $f,g\colon R\to R$. *The map $f\mapsto f(1)$ is a ring isomorphism* $\operatorname{End}_A A\xrightarrow{\sim}A^{\rm op}$.

The right translations $R_a\colon x\mapsto xa$, $a\in R$, defines a ring homomorphism $R\colon R^{\rm op}\to\operatorname{End}(R,+)$ and hence an $R^{\rm op}$-module structure on $R$ whose homothecies are the right stranslations $R_a$, $a\in R$, and the $R^{\rm op}$-submodules are the right-ideals in $R$.

Generally, an $R^{\rm op}$-module is called a $R$-right modulel and all the time $R$-modules considered are $R$-left modules, unless explicitly mentioned otherwise. An $R$-right module structure on $V$ is written as a right operation $V\times A\to V$, $(x,a)\mapsto xa$, such that the following well arranged computational rules hold :

$$(1)\ x(ab)=(xa)b\,,\quad (2)\ (x+y)a=xa+yb\,,\quad (3)\ x(a+b)=xa+xb\,,\quad (4)\ x\cdot 1=x$$

for all $a,b\in R$, $x,y\in V$. The ring $R$ itself have two module structures, moreover, they are compatible in the folowing sense : The homothecies of one structure commute with the homothecies of the other structure, i.e. $L_a\circ R_b=R_b\circ L_a$ for all $a,b\in A$.

(3) (Bimodules) More generally, two (left-)module structures on the same abelain group $(V,+)$ with the action homomorphisms $\vartheta\colon R\to\operatorname{End}V$ resp. $\eta\colon S\to\operatorname{End}V$ are compatible, if the homothecies $\vartheta_a$, $a\in R$, and $\eta_b$, $b\in S$, commute, i.e. if $a(bx)=b(ax)$ for all $a\in R$, $b\in S$, $x\in V$, equivalently, if the homothecies of one structure are linear with respect to the other structure. In such a case we say that $V$ is a $R$-$S$-bimodule. Therefore, every ring $R$ is a $R$-$R^{\rm op}$-bimodule, and every module over a *commutative* ring $R$ with a and the same $R$-module structure a $R$-$R$-bimodule. If $V$ is a $R$-$S$-bimodule and $W$ is an $R$-module, then $\operatorname{Hom}_R(V,W)$ with the right operation $\operatorname{Hom}_R(V,W)\times S\to\operatorname{Hom}_R(V,W)$, $(f,b)\mapsto fb:=f\circ\eta_b$, is a $S$-right module, i.e. a $S^{\rm op}$-(left-)module. In analogous way, $\operatorname{Hom}_R(V,W)$ with the left operation $bf:=\eta_b\circ f$ is a $S$-left module if $W$ has a $R$-$S$-bimodule structure.

As above if $R$ is commutative, using the canonical $R$-$R$-bimodule structure of $V$ (or of $W$), we get the $R$-module structure on $\operatorname{Hom}_A(V,W)$. For every ring $R$ and every $R$-module $V$, the above isomorphism $\operatorname{Hom}_R(R,V)\xrightarrow{\sim}V$ is an $R$-module isomorphism if $\operatorname{Hom}_R(R,V)$ has the $R$-module structure induced from the $R$-$R^{\rm op}$-bimodule structure on $R$. – In contrast, to the elements of $\operatorname{Hom}_R(R,V)$, the so-called $R$-linear forms $f\in V^*:=\operatorname{Hom}_R(V,R)$ on $V$ are difficult to characterize. However, by the last remark, the $R$-$R^{\rm op}$-bimodule structure on $R$ induces an *$R$-right*module structure on

$$V^*=\operatorname{Hom}_R(V,R)$$

with the scalar multiplication $fa\colon x\mapsto f(x)a$, $a\in A$, $f\in V^*$. With this module structure $V^*$ is called the dual module of $V$.

(4) (Restriction of scalars) Let $V$ be an $R$-module with action homomorphism $\vartheta\colon R\to\operatorname{End}V$. If $\varphi\colon R'\to R$ is a homomorphism of rings, then the composition $(\vartheta':=\vartheta\circ\varphi)\colon R'\to\operatorname{End}V$ defines a $R'$-module structure on $V$ with the operation $(a',x)\mapsto a'x=\varphi(a')x$. It is called the induced $R'$-module structure on $V$ by $\varphi$. It is particularly important in the case when $R'$ is a subring of $R$ and $\varphi$ is the canonical inclusion $R'\hookrightarrow R$. Then the $R'$-operation on $V$ is simply the restriction of the $R$-operation. Without mentioning explicitly, we will consider every $R$-module also as $R'$-module. For example, every complex (i.e. $\mathbb{C}$-)vector space also a real (i.e. $\mathbb{R}$-)vector space and every $\mathbb{R}$-vector space also a $\mathbb{Q}$-vector space.

(4) (Annihilator) Let $V$ be an $R$-module with action homomorphism $\vartheta\colon A\to\operatorname{End}V$. Then the two-sided ideal

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

is called the Annihilator *the module* $V$. It is $\operatorname{Ann}_R V=\bigcap_{x\in V}\operatorname{Ann}_A x$, where

$$\operatorname{Ann}_R x:=\{a\in A\mid ax=0\}$$

the annihilator *of the element* $x\in V$. Since $\operatorname{Ann}_R x$ is the kernel of the $R$-homomorphism $R\to V$, $a\mapsto ax$, and so it is (only) a left-ideal. The $R$-module $V$ is called a faithful $R$-module if $\operatorname{Ann}_R V=0$. If $\mathfrak{a}\subseteq\operatorname{Ann}_R V$ is a two-sided ideal in annihilator of $V$, then the action homomorphism $\vartheta\colon A\to\operatorname{End}V$ induces a homomorphism $\overline{\vartheta}\colon A/\mathfrak{a}\to\operatorname{End}_R V$ of rings and hence a $(R/\mathfrak{a})$-module structure on $V$ with scalar multiplication $[a]_{\mathfrak{a}}x=ax$ and $\operatorname{Ann}_{R/\mathfrak{a}}V=(\operatorname{Ann}_R V)/\mathfrak{a}$. Conversely, an $(R/\mathfrak{a})$-module structure on $V$, using the canonical projection $R\to R/\mathfrak{a}$, defines an $R$-module structure on $V$ with $\mathfrak{a}\subseteq\operatorname{Ann}_R V$. Therefore : *$(R/\mathfrak{a})$-modules and $R$-modules whose annihilator contain $\mathfrak{a}$ are one and the same.* For example, the annihilator of an abelian group $W$ (considered as $\mathbb{Z}$-module) is the ideal $\mathbb{Z}\operatorname{Exp}W\subseteq\mathbb{Z}$. For $m\in\mathbb{N}$, the abelian groups with $(\operatorname{Exp}W)\mid m$ and $\mathbf{A}_m$-modules are 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.

(5) (Torsion module–Torsion-free Modules) Let $V$ be a module over the *commutative* ring $R$. an element $x\in V$ is called a torsion element of $V$ if there exists a nonzero-divisor $a\in A^*$ such that $ax=0$, or equivalently, $\operatorname{Ann}_R x$ contains a nonzero-divisor. The set of all torsion elements of $V$ is denoted by

$$\mathrm{T}_R V\,.$$

Obviously, $\mathrm{T}_R V$ is a $R$-submodule of $V$. For a nonzero-divisor $a \in A^*$, $\mathrm{T}_a V := \mathrm{Ker}\,\vartheta_a = \{x \in V \mid ax = 0\}$ is called the $a$-torsion of $V$. Then $Ra \subseteq \mathrm{Ann}_R \mathrm{T}_a V$, and hence $\mathrm{T}_a V$ is an $(R/Ra)$-module (see (4)), and $\mathrm{T}_R V = \bigcup_{a \in R} \mathrm{T}_a V$. The $R$-module $V$ is called a torsion module if $\mathrm{T}_R V = V$, and is called torsion free if $\mathrm{T}_R V = 0$.

(6) Let $W$ be an additive abelian group. The identity map $\mathrm{End}\,W \to \mathrm{End}\,W$ defines the so-called tautological $(\mathrm{End}\,W)$-module structure on $W$ with scalar multplication

$$fx := f(x)\,, \quad f \in \mathrm{End}\,W,\ x \in W.$$

In particular, $W$ is a module over every subring of $\mathrm{End}\,W$. An arbitrary $R$-module structure on $W$ is induced by the action homomorphism $\vartheta \colon R \to \mathrm{End}\,W$.

**S1A.3** Let $R$ be a commutative ring and $V$ be an $R$-module. Let $a \in R$ be a unit. Then the homothecy $\vartheta_a : V \to V\ \ x \mapsto ax$ is bijective. Give an example of a non-zero $R$-module and a non-unit $a \in R$ such that the homothecy $\vartheta_a$ is bijective. **Hint:** Consider $\mathbb{Z}$-modules, i.e. Finite abelian groups.

**S1A.4** 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 $U + (W \cap W')$.

**S1A.5** In this supplement, we recall the concepts of direct products and direct sums of arbitrary family of modules.

**a)** (Direct products) Let $W_i$, $i \in I$, be a family of $R$-modules. Then the direct product $\prod_{i \in I} W_i$ with componentwise addition and componentwise scalar multiplication is also an $R$-module. Analogous to abelian groups, with the canonical $R$-linear projections $p_i \colon \prod_{i \in I} W_i \to W_i$, it has the following universal property : *For every $R$-module $V$, the canonical map*

$$\mathrm{Hom}_R\bigl(V, \prod_{i \in I} W_i\bigr) \xrightarrow{\sim} \prod_{i \in I} \mathrm{Hom}_R(V, W_i)\,, \quad f \mapsto (p_i f)_{i \in I}\,,$$

*is a group isomorphism and if $R$ is commutative, then an $R$-module isomorphism.* The $I$-tuple $(f_i)_{i \in I} \in \prod_{i \in I} \mathrm{Hom}_R(V, W_i)$ is the image of the $R$-homomorphism $V \to \prod_{i \in I} W_i$, $x \mapsto (f_i(x))_{i \in I}$, which is denoted by $(f_i)_{i \in I}$.

**b)** (Direct sums) Let $V_j$, $j \in J$, be a family of $R$-modules. The restricted direct product or the direct sum $\bigoplus_{j \in J} V_j := \{(x_j)_{j \in J} \in \prod_{j \in J} V_j \mid x_j = 0$ for almost all $j \in J\}$ of $V_j$, $j \in J$, is a submodule. Besides the canonical projections $(v_j)_{j \in J} \mapsto v_j$, now the canonical injections $\iota_j \colon V_j \to \bigoplus_{j \in J} V_j$, $j \in J$, an important rolle. For $x_j \in V_j$, the $J$-tuple $\iota_j(x_j) = (\delta_{ij} x_j)_{i \in J}$ with $j$-th component $x_j$ and all other components 0. Analogous to the abelian groups the direct sums with the canonical $R$-linear injections $\iota_j \colon V_j \to \bigoplus_{j \in J} V_j$ has the following universal property : *For every $R$-module $W$, the canonical map*

$$\mathrm{Hom}_R\bigl(\bigoplus_{j \in J} V_j, W\bigr) \xrightarrow{\sim} \prod_{j \in J} \mathrm{Hom}_R(V_j, W)\,, \quad g \mapsto (g \iota_j)_{j \in J}\,,$$

*is a group isomorphism und if $R$ is commutative, then an $R$-module isomorphism.* The $J$-tuple $(f_j)_{j \in J} \in \prod_{j \in J} \mathrm{Hom}_R(V_j, W)$ is the image of the $R$-homomorphism

$$\sum_{j \in J} f_j \colon \bigoplus_{j \in J} V_j \to W\,, \quad (x_j)_{j \in J} \mapsto \sum_{j \in J} f_j(x_j)\,.$$

**c)** The combination of the universal properties of direct product and direct sum provide the following important theorem :

*Let $V_j$, $j \in J$, and $W_i$, $i \in I$, be families of $R$-modules. Then the canonical map*

$$\mathrm{Hom}_R\bigl(\bigoplus_{j \in J} V_j, \prod_{i \in I} W_i\bigr) \xrightarrow{\sim} \prod_{(i,j) \in I \times J} \mathrm{Hom}_R(V_j, W_i)\,,\ f \mapsto (f_{ij})_{(i,j) \in I \times J}\,,\ f_{ij} := p_i f \iota_j\,,\ i \in I, j \in J,$$

*is a group isomorphism and if $R$ is commutative, then an $R$-module isomorphism.* The matrix $(f_{ij})_{(i,j) \in I \times J} \in \prod_{(i,j) \in I \times J} \mathrm{Hom}_R(V_j, W_i)$ is the image of the homomorphism

$$f \colon \bigoplus_{j \in J} V_j \to \prod_{i \in I} W_i\,, \quad (x_j)_{j \in J} \mapsto (y_i)_{i \in I} \ \text{ mit } \ y_i := \sum_{j \in J} f_{ij}(x_j)\,,\ i \in I.$$

( For finite index sets, direct sums and direct product coincides. Let $I, J, K$ be finite sets and $U_k$, $k \in K$, an another family of $R$-modules. Then, if the matrices $\mathfrak{B} = (g_{jk}) \in \prod_{j,k} \mathrm{Hom}_R(U_k, V_j)$ and $\mathfrak{A} = (f_{ij}) \in \prod_{1,j} \mathrm{Hom}_R(V_j, W_i)$ describe the homomorphisms $g \colon \bigoplus_{k \in K} U_k \to \bigoplus_{j \in J} V_j$ resp. $f \colon \bigoplus_{j \in J} V_j \to \bigoplus_{i \in I} W_i$, then the composition $f \circ g \colon \bigoplus_{k \in K} U_k \to \bigoplus_{i \in I} W_i$ is defined by the product matrix

$$\mathfrak{A}\mathfrak{B} := (f_{ij})_{i,j} (g_{jk})_{j,k} = (h_{ik})_{i,k} \in \prod_{(i,k) \in I \times K} \mathrm{Hom}_R(U_k, W_i) \ \text{ with } \ h_{ik} := \sum_{j \in J} f_{ij} \circ g_{jk}\,,\ (i,k) \in I \times K.$$

If the index sets $I$, $J$, $K$ are not finite, then formulate the restrictions of the matrices $\mathfrak{A}$ and $\mathfrak{B}$.

More often used are the cases $R^n$ and $R^m$ in the theorem in part c) (under the identification $\mathrm{End}_R R = R^{\mathrm{op}}$). Then : Every $R$-module homomorphism $f \colon R^n \to R^m$ is given by an $m \times n$-matrix $\mathfrak{A} = (a_{ij}) \in \mathrm{M}_{m,n}(R^{\mathrm{op}}) = \bigl(R^{\mathrm{op}}\bigr)^{\{1,\ldots,m\} \times \{1,\ldots,n\}}$. It is – as usual common to denote – the elements $\mathfrak{x} \in R^n$ resp. $\mathfrak{y} \in R^m$ as one column matrices with $n$ resp. $m$ rows, then

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

Note that the matrix coefficients are considered and multiplied in the opposite ring $R^{\rm op}$! This provides the summands $x_j a_{ij}$ instead of $a_{ij}x_j$ and so also note the multiplication of matrices. *The endomorphism ring of the R-module $R^n$ is the ring $\mathrm{M}_n(R^{\rm op})$ of the square $n\times n$-matrices with coefficients in $R^{\rm op}$.* The identity of $R^n$ is then represented by the unit matrix $\mathfrak{E}_n = (\delta_{ij})) \in \mathrm{M}_n(R)$. In the important case when $R$ is commutative, naturally one nedd not distinguish between $R$ and $R^{\rm op}$. )

**d)** In general, it is simpler to produce a direct sum representation of an module than the direct product representation. For example, the following lemma:

(Direct sums of submodules) *Let $U_i$, $i\in I$, be a family of submodules of the R-module V and $h\colon \bigoplus_{i\in I} U_i \to V$, $(u_i)_{i\in I} \mapsto \sum_{i\in I} u_i$, be the canonical R-homomorphism with the image $\sum_{i\in I} U_i$. Then h injective* i.e. the sum of $U_i$ is direct *if and only if the following condition is satisfied*: *For every $i\in I$, one has*

$$U_i \cap \sum_{j\neq i} U_j = \{0\}\,.$$

*If I is totally ordered, then this condition is also equivalent with the following: $U_i \cap \sum_{j<i} U_j = \{0\}$ for all $i\in I$.*

If the sum $\sum_{i\in I} U_i \subseteq V$ is direct, then this sum is also denoted by $\sum_{I\in I}^{\oplus} U_i$.

**S1A.6** (Residue-class modules) Let $V$ be an $R$-module and $U\subseteq V$ be an $R$-submodule. The residue-class group

$$V/U$$

is always an $R$-module. Its scalar multiplication is defined by $a\,[x]_U = [ax]_U$, $a\in R, x\in V$. The operation $\overline{\vartheta}_a$ of $a\in R$ on $V/U$ is induced by the operation $\vartheta_a$ of $a$ on $V$ (since $\vartheta_a(U)\subseteq U$, $\overline{\vartheta}$ is well-defined). The canonical projection $\pi_U : V \to V/U$ is $R$-linear and has the following universal property:

**a)** (Universal property of the residue-class module) *Let U be a submodule of the R-module V and $f\colon V\to W$ be a R-linear map in an R-module W with $U\subseteq \mathrm{Ker} f$. Then there exists a unique R-linear map $\overline{f}\colon V/U \to W$ with $f = \overline{f}\circ\pi_U$. There by $\overline{f}\big([x]_U\big) = f(x)$, $x\in V$, $\mathrm{Img}\,\overline{f} = \mathrm{Img}\,f$ and $\mathrm{Ker}\,\overline{f} = (\mathrm{Ker}\,f)/U$ $(\subseteq V/U)$. – The map $\overline{f}$ is an isomorphism if and only if f surjective and $U = \mathrm{Ker}\,f$. In particular, $V/\mathrm{Ker}\,f \xrightarrow{\sim} \mathrm{Img}\,f$* (Isomorphism theorem for modules).

The cosets $x+U$, $x\in V$, of a $K$-subspace $U$ of a $K$-vector space $V$ ($K$ skew-field) are also called affine subspaces (parrallel to $U$) of $V$.[2]

The above theorem is a special case of the following:

**b)** (Theorem on induced homomorphisms for modules) *Let $g\colon V\to W$ and $f\colon V\to X$ be homomorphisms of R-modules. Suppose that g is surjective, and* $\mathrm{Ker}\,g \subseteq \mathrm{Ker}\,f$. *Then there exists a unique homomorphism $\overline{f}\colon W\to X$ such that $f = \overline{f}\circ g$. – Further, $\overline{f}$ surjective if and only if f surjective. – $\overline{f}$ is injective if and only if* $\mathrm{Ker}\,g = \mathrm{Ker}\,f$. *– $\overline{f}$ is an isomorphism if and only if f surjective and* $\mathrm{Ker}\,g = \mathrm{Ker}\,f$ (Isomorphism Theorem for modules).

**S1A.7** For submodules $U,W$ of a $R$-module $V$ obtain the following canonical isomorphism: (1) $U/(U\cap W) \xrightarrow{\sim} (U+W)/W$. (2) If $U\subseteq W$, then $V/W \xrightarrow{\sim} (V/U)/(W/U)$.

**S1A.8** (Generating systems, Minimal number of generators and Minimal generating systems) Let $R$ be a commutative ring and $V$ be an $R$-module.

**a)** For an arbitrary family $v_i$, $i\in I$, of elements of $V$, the elements

$$\sum_{i\in I} a_i v_i\,,\quad (a_i)_{i\in I}\in R^{(I)}\,,$$

are called the linear combinations of the $v_i$, $i\in I$, (with coefficients in $R$). They form the submodule of $V$ generated by $v_i$, $i\in I$, i.e. the smallest $R$-submodule of $V$ which contains all the $v_i$, $i\in I$. If this submodule is equal to $V$, then $v_i$, $i\in I$, is called a generating system for $V$. The linear combinations of the family $v_1,\ldots,v_n$ in $V$ are the elements

$$a_1v_1+\cdots+a_nv_n\,,\quad (a_1,\ldots,a_n)\in R^n.$$

For $v\in V$, $Rv = \{av \mid a\in A\}$ is the submodule generated by $v$ and consequently, $\sum_{i\in I} Rv_i$ is the submodule generated by the $v_i$, $i\in I$. If $M\subseteq V$ is a subset of $V$, then $RM$ is the submodule of $V$ generated by $M$. Thereby for rings we use the following already introduced convention: For a subset $S$ of $R$ and a subset $M$ of $V$, $RM$ denote the sub*group* of $(V,+)$ generated by the complex-product $\{ax \mid a\in S,\ x\in M\}$ of $S$ and $M$.

**b)** The infimum of the cardinal numbers of the generating systems of $V$ (which exists by the well ordering of cardinal numbers) is called the minimal number of generators for $V$ and is denoted by $\mu_R(V)$. If $\mu_R(V)\in\mathbb{N}$,

[2] Occasionally similar such term is also used for modules.

then $V$ is called a finite $R$-module. If $\mu_R(V)\leq 1$, i.e. $V$ is generated by (at most) one element, then $V$ is called cyclic. Note that $\mu_R(0)=0$. Prove that:

**1)** If $\mu_R(V)\in\mathbb{N}$, then every generating system of $V$ contains a finite generating subsystem.

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

**3)** If $0\to U\xrightarrow{f} V\xrightarrow{g} W\to$ is an exact sequence of $R$-modules and $R$-module homomorphisms, then $\mu_R(V)\leq\mu_R(U)+\mu_R(W)$. – In particular, if $V$ is finitely generated if and only if both $U$ and $W$ are finitely generated.

(**Remarks:** Note that a minimal generating system of a finite $R$-module can contain more than $\mu_R(V)$ elements. For example, $\{2,3\}$ is a minimal generating system for the cyclic $\mathbb{Z}$-module $\mathbb{Z}$. More generally, for a given $m\in\mathbb{N}^*$, there are minimal generating systems for the $\mathbb{Z}$-module $\mathbb{Z}$ which have exactly $m$ elements.
Further, an $R$-module $V$ may not have any minimal generating system. (Then naturally, $\mu_R(V)$ is infinite.) For example, the $\mathbb{Z}$-module $\mathbb{Q}$ has no minimal generating system, see the Exercise below.)

**S1A.9** 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[3] 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 $\mathrm{Q}(R)$ of an integral domain $R$ which is not a field, has no minimal generating system as an $R$-module. In particular, $\mathrm{Q}(R)$ is not finitely generated $R$-module.

**S1A.10** Let $R$ be a commutative ring and let $V_i$, $i\in I$, be an infinite family of non-zero $R$-modules. Prove that $W:=\bigoplus_{i\in I}V_i$ is not a finite $R$-module.

**S1A.11** Let $K$ be a field and let $R$ be a subring of $K$ such that every element of $K$ can be expressed as a quotient $a/b$ with $a,b\in R, b\neq 0$. (i. e. $K$ is the quotient field of $R$). If $K$ is a finite $R$-module, then prove that $R=K$. In particular, $\mathbb{Q}$ is not a finite $\mathbb{Z}$–module. (**Hint:** Suppose $K=Rx_1+\cdots+Rx_n$ and $b\in R, b\neq 0$, with $bx_i\in R$ for $i=1,\ldots,n$. Now, try to express $1/b^2$ as a linear combination of $x_i$, $i=1,\ldots,n$.)

**S1A.12** Let $R$ be an integral domain. If the set of all non-zero ideals in $R$ have a minimal element (with respect to the inclusion). Show that $R$ is a field. In particular, an integral domain such that the set of all ideals is an artinian ordered set (with respect to inclusion), is a field. (Recall that an ordered set $(X,\leq)$ is called artinian if every non-empty subset of $X$ has a minimal element. For example finite ordered sets are artinian. An ordered set is well ordered if it is totally ordered and artinian. The prototype of the well ordered set is the set $\mathbb{N}$ of natural numbers with its natural order.)

**S1A.13** (Free modules) Let $R$ be an arbitrary ring and $I$ be an index-set. In the $|I|$-fold direct sum $R^{(I)}=\sum_{i\in I}^{\oplus}R\subseteq R^I$, for every $i\in I$, let $e_i:=(\delta_{ij})_{j\in I}$ be the $I$-tuple with $i$-th component 1 and all other components. Then every element $(a_i)_{i\in I}\in R^{(I)}$ has the (unique) representation $(a_i)_{i\in I}=\sum_{i\in I}a_ie_i$. Therefore the family $e_i$ is a generated system for the $R$-module $R^{(I)}$. The $R$-module $R^{(I)}$ is called the free $R$-module corresponding to the (index-)set $I$. It is a prototype of a free $R$-module, see ???. Since $\mathrm{Hom}_R(R,V)\xrightarrow{\sim}V$ $(f\mapsto f(1))$, the $R$-module $R^{(I)}$ together with the map $\iota_I: I\to R^{(I)}$, $i\mapsto e_i$ has the following universal property:

*Let $R$ be ring and $I$ be a set. Then for every $R$-module $V$, the map*

$$\mathrm{Hom}(R^{(I)},V)\xrightarrow{\sim}V^I\,,\quad f\mapsto f\circ\iota_I=(f(e_i))_{i\in I}\,,$$

*is an isomorphism of groups and if $R$ is commutative, it is even an isomorphism of $R$-mdules. The inverse image of the $I$-tuple $\mathfrak{v}=(v_i)_{i\in I}\in V^I$, is the homomorphism*

$$f_{\mathfrak{v}}: R^{(I)}\to V\,,\quad (a_i)_{i\in I}\mapsto\sum_{i\in I}a_iv_i\,,$$

*whose image is the submodule $\sum_{i\in I}Rv_i$ of $V$ generated by $v_i$, $i\in I$. In particular, $f_{\mathfrak{v}}$ is surjective if and only if $\sum_{i\in I}Rv_i=V$, i.e. $v_i$, $i\in I$, is a generating system for $V$.*

The kernel of the homomorphism $f_{\mathfrak{v}}: R^{(I)}\to V$, $(a_i)_{i\in I}\mapsto\sum_{i\in I}a_iv_i$, is the submodule

$$\mathrm{Rel}_R(v_i,i\in I)=\mathrm{Syz}_R(v_i,i\in I):=\big\{(a_i)\in A^{(I)}\;\big|\;\sum_{i\in I}a_iv_i=0\big\}$$

and is called the relation module or the syzygy module of the family $(v_i)_{i\in I}\in V^I$. Its elements are so-called the relations or Syzygies of the $v_i$, $i\in I$.[4] Therefore

$$A^{(I)}/\,\mathrm{Syz}_R(v_i,i\in I)\xrightarrow{\sim}\mathrm{Img}\,f=\sum_{i\in I}Av_i\,.$$

[3] **Divisible abelian groups.** An abelian (additively written) group $H$ is divisible 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.*

[4] The use of the word "‘Syzygy"’ goes back to D. Hilbert (1862-1943).

In particular, $R^{(I)}/\operatorname{Syz}_R(v_i, i \in I) \xrightarrow{\sim} V$, if $v_i$, $i \in I$, is a generated system for $V$. *Every $R$-module with generating system consisting of $|I|$ elements is isomorphic to a residue-class module of $R^{(I)}$.* In particular, residue-class modules of $R^n$ are, up to isomorphisms, all finite modules with $n$ generators, $n \in \mathbb{N}$. A cyclic $R$-module $V = Rx$ is isomorphic to a residue-class module of $R$, more precisely, $Rx \cong R/\operatorname{Syz}_R x = R/\operatorname{Ann}_R x$. To provide an $R$-module, often one can give only a submodule $U \subseteq A^{(I)}$ which is the syzygy module of a generating system of $V$ and there by restrict ro supply a generating system of $U$. If $I$ is finite and $R$ is noetherian, then $U$ is always generating by finitely many elements, see ???. The module $V$ is then itself finitely generated.

Let $v_i$, $i \in I$, be a family of elements of an $R$-module $V$.

**a)** The family $v_i$, $i \in I$, is linearly independent over $R$ if $\operatorname{Syz}_R(v_i, i \in I) = 0$, and hence if a linear combination $\sum_{i\in I} a_i v_i$ of $v_i$, $i \in I$, over $R$ is 0 if and only if *all* (and not only almost all) coefficients $a_i$ $i \in I$, are 0.

Obviously, the family $v_i$, $i \in I$, is linearly independent over $R$ if and only if its every *finite* subfamily is linearly independent.

The family $v_i$, $i \in I$, is linearly independent over $R$ if and only if the $R$-module homomorphism $f_{\mathfrak{v}} : R^{(I)} \to V$, $(a_i)_{i\in I} \mapsto \sum_{i\in I} a_i v_i$, is injective. Equivalently, the sum $\sum_{i\in I} Rx_i$ of cyclic submodules $Rv_i$ is direct and more over, $\operatorname{Ann}_R Rv_i = 0$ for every $i \in I$.

If $f : V \to W$ is a $R$-linear map and if the image family $f(v_i)$, $i \in I$, is linearly independent over $R$, then the family $v_i$, $i \in I$, is also linearly independent over $R$.

**b)** The family $v_i$, $i \in I$, is an $R$-basis of $V$, if it a linearly independent generating system of $V$. The $R$-module $V$ is a free $R$-module, if $V$ has a basis over $R$.

The family $v_i$, $i \in I$, is a basis of $V$ over $R$ if and only if the $R$-module homomorphism $f_{\mathfrak{v}} : R^{(I)} \to V$, $(a_i)_{i\in I} \mapsto \sum_{i\in I} a_i v_i$, is bijective. *If $R \neq 0$, then every basis $v_i$, $i \in I$, of $V$ is a minimal generating system for $V$* (Note that $v_i \notin \sum_{j\neq i} Rv_j$ for every $i \in I$).

**c)** The knowledge of a basis of $V$ provides a complete description of the elements of $V$. Often, such a basis a given by the construction. For example, for $V = R^{(I)}$ the so-called the standard basis $e_i$, $i \in I$, given above. Analogous to the free $R$-module $R^{(I)}$, a free $R$-module $V$ with basis $v_i$, $i \in I$, has the following universal property, due to which it is known as the free object. It allows to assign the images of the $v_i$ freely:

*For every $R$-module $W$, the map*

$$\operatorname{Hom}_R(V, W) \xrightarrow{\sim} W^I, \quad f \mapsto \big(f(v_i)\big)_{i\in I},$$

*is a group isomorphism and if $R$ is commutative, then an $R$-module isomorphism.*

The inverse image $f\colon V \to W$ of the $I$-tuple $(w_i)_{i\in I} \in W^I$, maps the linear combination $\sum_i a_i v_i \in V$ onto the linear combination $\sum_i a_i w_i \in W$. Further, $f$ is surjective if and only if the $w_i$, $i \in I$, generates the module $W$, and is injective if and only if the $w_i$, $i \in I$, are linearly independent.

**d)** The following simple lemma is very useful:

*Let $v_i$, $i \in I$, be a family in the $R$-module $V$ and $I = I' \uplus I''$ be a partition of $I$. Then $v_i$, $i \in I$, is linearly independent if and only if (resp. a basis) the subfamily $v_i$, $i \in I'$, is linearly independent and the family of residue-classes $[v_i]$, $i \in I''$, is linearly independent in (resp. a basis of) $V/U$, where $U := \sum_{i\in I'} Rv_i$.*

**e)** Vector spaces are free. The basic principle of the proof is the following trivial lemma:

*Let $V$ be a vector space over the division domain $K$ and $v_i$, $i \in I$, be a linearly independent family in $V$. For every vector $v \in V$ with $v \notin U := \sum_{i\in I} Kv_i$, then the extended family $v$, $v_i$, $i \in I$, is also linearly independent and hence a basis of $U' := Kv + U$. Moreover, if $w \in U' \smallsetminus U$ is arbitrary, then $w$, $v_i$, $i \in I$, is also a basis of $U'$.* (**Proof:** Suppose that $0 = av + \sum_{i\in I} a_i v_i$ with $a \in R$, $(a_i) \in R^{(I)}$. If $a \neq 0$, then $v = -\sum_{i\in I} a^{-1} a_i v_i \in \sum_{i\in I} Kv_i$, a contradiction. Therefore $a = 0$ and then also $(a_i) = 0$, for all $i \in I$, since $v_i$, $i \in I$, are linearly independent. The proof of the supplement is left to the reader. •)

**f)** Prove the following fundamental theorem on the existence of basis:

*Let $V$ be a vector space over the division domain $K$, and $v_i$, $i \in I$, be a generating system for $V$. Further, assume that $v_i$, $i \in I' \subseteq I$, be a linearly independent subsystem. Then there exists a subset $I'' \subseteq I$ with $I' \subseteq I''$ such that $v_i$, $i \in I''$, is a basis of $V$. In particular, $V$ has a basis.* (**Proof:** The supplement follows by taking $I' = \emptyset$. – For a proof of existence of $I''$ consider the set $\mathcal{M}$ of those subsets $J$ of $I$ with $I' \subseteq J \subseteq I$, such that the $v_i$, $i \in J$, is linearly independent. The set $\mathcal{M}$ is inductively (even strictly inductively) ordered with respect to the natural inclusion: Since $I' \in \mathcal{M}$, $\mathcal{M} \neq \emptyset$, and for a non-empty chain $\mathcal{K} \subseteq \mathcal{M}$, $\bigcup_{J\in\mathcal{K}} J \in \mathcal{M}$ is an upper bound of $\mathcal{K}$ in $\mathcal{M}$. Therefore, by Zorn's Lemma $\mathcal{M}$ has a maximal element, and every such maximal element $I'' \in \mathcal{M}$ provide a basis $v_i$, $i \in I''$, of $V$. Namely, if $U := \sum_{i\in I''} Kv_i \subsetneq V$, then there exists a $i_0 \in I$ with $v_{i_0} \notin U$ (since the $v_i$, $i \in I$, generate the $K$-vector space $V$), and then by Lemma in f), $I'' \uplus \{i_0\}$ is a strictly bigger element than $I''$ of $\mathcal{M}$, a contradiction. •

– **Remarks:** Note that in the above proof of the existence of a maximal $I'' \in \mathcal{M}$ is trivial if the index set $I$ is finite, i.e. if $V$ is a finite $K$-vector space. Hamel's basis: The existence of bases for an arbitrary vector space was first proved in 1905 by G. Hamel (1877-1954) for the special case of $\mathbb{R}$ as $\mathbb{Q}$-vector space. Till today the $\mathbb{Q}$-bases of $\mathbb{R}$ are called Hamel bases. Hamel's proof make use of a well-order on $I$ with $i' < i$ for all $i' \in I'$, $i \in I \smallsetminus I'$ – the Well-ordering Theorem of Zermelo has only just been proved in 1904 by E. Zermelo (1871-1953) – and define $I''$ in the following way: $i \in I''$ if and only if $x_i \notin \sum_{j<i} Kx_j$. Then $I' \subseteq I''$ and $v_i$, $i \in I''$, is a basis of $V$. Proof! – Hamel used a $\mathbb{Q}$-Basis $v_i$, $i \in I$, of $\mathbb{R}$ (whose cardinality must be $\aleph$), to solve the following Problem of Cauchy: Does there exit additive maps $\mathbb{R} \to \mathbb{R}$, which are not any stretchings $L_a\colon x \mapsto ax$ with an $a \in \mathbb{R}$? Since by the universal property of a basis, we have the canonical isomorphism $\operatorname{End}\mathbb{R} = \operatorname{End}_{\mathbb{Q}}\mathbb{R} \xrightarrow{\sim} \mathbb{R}^I$, and the homothecies $L_a$, $a \in \mathbb{R}$, correspond to the $I$-tuple $(av_i)_{i\in I}$, the most additive endomorphisms of $\mathbb{R}$ are not stretchings $L_a$, $a \in \mathbb{R}$. The cardinality of $\operatorname{End}\mathbb{R}$ is equal to $\aleph^{\aleph} = 2^{\aleph} > \aleph$, since every $\mathbb{Q}$-basis of $\mathbb{R}$ has the cardinality $\aleph$.

It is by no means self-evident that two bases of a free modules over a ring $\neq 0$ have the same cardinal numbers. Indeed it is also false. There exist rings $R \neq 0$, such that for the $R$-module $R$ there is a basis consisting of two (and hence also $n \in \mathbb{N}^*$) elements, therefore $R \cong R^n$ for all $n \in \mathbb{N}^*$, see Supplement S1A.37.)

**S1A.14** Let $K$ be a field and let $b_0, \ldots, b_m$ be elements of $K$, all of which are not equal to 0. Then there exist at most $m$ distinct elements $x \in K$, which satisfy the equation

$$0 = b_0 \cdot 1 + b_1 x + \cdots + b_m x^m \,.$$

(**Hint :** If $x_1, \ldots, x_{m+1}$ are distinct elements in $K$, then the elements $h_j := (x_1^j, \ldots, x_{m+1}^j) \in K^{m+1}$, $0 \leq j \leq m$, are linearly independent over $K$. — **Remark :** The same result is also true for integral domains, since every integral domain is contained in a field, for example, in its quotient field. With the help of concept of polynomials the above assertion can be formulated as : *A non-zero polynomial of degree $\leq m$ over a field (or an integral domain) $K$ has at most $m$ zeros in $K$.*)

**S1A.15** Let $A$ be an integral domain (which is contained in a field $Q$). Further, let $U$ be a subgroup of the unit group $A^\times$ of $A$ with an exponent [5] $m \neq 0$. Then $U$ is cyclic (and finite). In particular, every finite subgroup of $A^\times$ is cyclic; further, the unit group of every finite field (for example, the unit group of a prime ring of characteristic $p$, $p$ prime, is cyclic.) (**Hint :** The equation $x^m = 1$ has at most $m$ solutions in $A$ by Supplement S1A.14. Now use the following Exercise on groups : *Let $G$ be a finite group with neutral elements $e$. Suppose that for every divisor $d \in \mathbb{N}^*$ of the order* $\operatorname{Ord} G$ *there are at most $d$ elements $x \in G$ such that $x^d = e$. Then $G$ is a cyclic group.*)

**S1A.16** Let $U, W$ be submodules of the $R$-module $V$. Then both the so-called Meyer-Vietoris-Sequences

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

are exact, where the non-trivial homomorphisms in the first sequence are defined by $x \mapsto (x, -x)$ resp. $(x,y) \mapsto x+y$ and in the second sequence analogously are defined by $[x] \mapsto ([x], -[x])$ resp. $([x],[y]) \mapsto [x+y]$.

**S1A.17** For a family $v_i$, $i \in I$, of vectors in a $K$-vector space, the following are equivalent : (i) $v_i$, $i \in I$, is a basis of $V$. (ii) $v_i$, $i \in I$, is a minimal generating system for $V$. (iii) $v_i$, $i \in I$, is a maximal linearly independent family in $V$.

**S1A.18** Let $R \neq 0$ and let $x$ be a basis of the cyclic $R$-module $V := Rx$. Then $y = ax \in V$, $a \in R$, is a basis of $V$ if and only if $a$ is a unit in $R$. (Note that $Rx \neq 0$ may be a free $R$-module without $x$ being a basis of $Rx$, See Supplement S1A.37 c).)

**S1A.19** (Modules with rank) A free module $V$ over the ring $R$ has by definition a rank if all bases of $V$ have the same cardinality. This common cardinal number is then called the rank of $V$ (over $R$) and is denoted by

$$\operatorname{Rank} V = \operatorname{Rank}_R V \,.$$

In case of vector spaces over a division domain $K$, in general, instead of rank, we use the dimension of $V$ and write

$$\operatorname{Dim} V = \operatorname{Dim}_K V \,.$$

**a)** Without any problem free modules with infinite basis have rank :

*Every finite free module $V$ with an infinite basis $v_i$, $i \in I$, over a ring $R \neq 0$ has the rank* $\operatorname{Rank}_R V = |I|$. (**Proof :** Since $v_i$, $i \in I$, is a minimal generating system for $V$, by Lemma Supplement S1A.8 b) 1) there is no finite generating system for $V$ and hence has no finite basis. Suppose that $w_j$, $j \in J$, is an arbitrary basis of $V$. Then by Supplement S1A.8 b) 2) $|J| = |I| = \mu_R(V)$. •)

**b)** For vector spaces in general we have :

*Every vector space $V$ over a division domain $K$ has a dimension,* i.e. *all bases of $V$ have the same cardinality.* (**Proof :** By the Theorem in a), we may assume that $V$ is a $K$-vector space with finite basis. In this case the assertion follows from the following Lemma in c). •)

**c)** *Let $V$ be a $K$-vector space with basis $v_1, \ldots, v_n$. Then every $n+1$ vectors $w_1, \ldots, , w_{n+1} \in V$ are linearly dependent.* (**Proof :** We apply induction on $n$. The assertion is trivial for $n = 0$ (and $n = 1$). For the inductive step from $n$ to $n+1$, we may assume that $v_1, \ldots, v_{n+1}$ is a basis of $V$ and that $w_1, \ldots, , w_{n+2} \in V$ are linearly independent. Then by induction hypothesis, not all $w_i$ belong to the subspace $U := Kv_1 + \cdots + Kv_n \subseteq V$. If, say, $w_{n+2} \notin U$, then by Lemma in Supplement S1A.13 e), $v_1, \ldots, v_n, w_{n+2}$ is a basis of $V$ and the residue-classes $[v_1], \ldots, [v_n] \in V/Kw_{n+2}$ is a basis of $V/Kw_{n+2}$ by Lemma in Supplement S1A.13 d). In any case, by Lemma in Supplement S1A.13 d), $[w_1], \ldots, [w_{n+1}]$ are linearly independent in $V/Kw_{n+2}$, which is not possible by induction hypothesis. •)

**d)** *The vector spaces $K^n$, $n \in \mathbb{N}$, represent, up to isomorphism, all finite dimensional vector spaces over a division domain $K$.* However, it should not be mistakes that only these spaces as finite dimensional vector spaces are considered.

[5] **Exponent of a group.** Let $G$ be a group with neutral element $e$. Then the set of integers $n$ with $a^n = e$ for all $a \in G$ forms a subgroup $U_G$ of the additive group of $\mathbb{Z}$, i.e. $U_G := \{n \in \mathbb{Z} \mid a^n = e \text{ for all } a \in G\}$ and hence there is a unique $m \in \mathbb{N}$ such that $U_G = \mathbb{Z}m$. This natural number $m$ is called the exponent of $G$ and usually denoted by $\operatorname{Exp} G$. For example, if $G$ is a finite cyclic group, then $\operatorname{Exp} G = \operatorname{Ord} G$ ; $\operatorname{Exp} \mathfrak{S}_3 = \operatorname{Ord} \mathfrak{S}_3$ ; In general : $\operatorname{Exp} G$ *and* $\operatorname{Ord} G$ *have the same prime divisors.* (proof!).

The identification of an $n$-dimensional $K$-vector space $V$ with $K^n$, i.e. an calibration of $V$, mean the choice of a $K$-basis $v_1,\ldots,v_n$ of $V$, which was a non-trivial process (already for $n=1$ and $|K|>2$). – From the Lemma in Supplement S1A.13 d), it follows directly :

**e)** (Rank Theorem) *Let* $0\to U\xrightarrow{f} V\xrightarrow{g} W\to 0$ *be an exact sequence of K-vector spaces and K-homomorphisms. Then*

$$\mathrm{Dim}_K V=\mathrm{Dim}_K U+\mathrm{Dim}_K W\,.$$

*In particular,* $\mathrm{Dim}_K V=\mathrm{Dim}_K U+\mathrm{Dim}_K(V/U)$ *for a K-vector space V and a K-subspace* $U\subseteq V$.

For a $K$-linear map $f:V\to W$ from a finite dimensional $K$-vector space into arbitrary $K$-vector space, it follows

$$\mathrm{Rank}\,f:=\mathrm{Dim}_K\mathrm{Im}\,f=\mathrm{Dim}_K V-\mathrm{Dim}_K\mathrm{Ker}\,f$$

This equality which is also known as Rank-Nullity Theorem, also explain the use of the term Rank Theorem.

From the first exact sequence in Supplement S1A.16 deduce in the case that $A=K$ is a division domain, 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 exact sequence in Supplement S1A.16 deduce the so-called codimension formula

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

Thereby, for an arbitrary subspace $U$ of a $K$-vector space $V$, $\mathrm{Codim}_K(U,V):=\mathrm{Dim}_K(V/U)$ is called the ($K$-)codimension of $U$ in $V$. In particular, in the case of a finite dimensional $K$-vector space $V$, we have two inequalities :

$\mathrm{Dim}_K(U\cap W)\geq\mathrm{Dim}_K U+\mathrm{Dim}_K W-\mathrm{Dim}_K V$ and $\mathrm{Codim}_K(U\cap W,V)\leq\mathrm{Codim}_K(U,V)+\mathrm{Codim}_K(W,V)$. Further, if $\mathrm{Dim}_K U+\mathrm{Dim}_K W>\mathrm{Dim}_K V$, then $U\cap W\neq 0$.

**S1A.20** (Free modules over commutative rings) *Free modules over a commutative ring* $R\neq 0$ *also has a rank.* (**Proof :** This can be proved by the following construction on reducing to the case of the field : First, let $V$ be an arbitrary module over the arbitrary ring $R$ and $\mathfrak{a}\subseteq R$ be a two-sided ideal in $R$. Then $\mathfrak{a}V$ is a submodule of $V$ with $\mathfrak{a}V=\sum_{i\in I}\mathfrak{a}v_i$ for every generating system $v_i$, $i\in I$, of $V$. Moreover, $\mathfrak{a}\subseteq\mathrm{Ann}_R(V/\mathfrak{a}V)$ and hence $V/\mathfrak{a}V$ is an $A/\mathfrak{a}$-module, see Supplement S1.2 (4). Now, if $v_i$, $i\in I$, is a basis of $V$, then $\mathfrak{a}V=\sum_{i\in I}^{\oplus}\mathfrak{a}v_i\subseteq V=\sum_{i\in I}^{\oplus}Rv_i$ and $(R/\mathfrak{a})^{(I)}\cong\bigoplus_{i\in I}(Rv_i/\mathfrak{a}v_i)\xrightarrow{\sim}V/\mathfrak{a}V$. Then it follows that the residue-classes $[v_i]$, $i\in I$, form a $(R/\mathfrak{a})$-basis of $V/\mathfrak{a}V$. Therefore, it follows that : if all free $(R/\mathfrak{a})$-modules have a rank, then all free $R$-modules also have a rank. Since every commutative ring $R\neq 0$ has maximal ideal $\mathfrak{m}$ by the Theorem of Krull, and $R/\mathfrak{m}$ is a field, the assertion is a special case of the Theorem in Supplement S1.18 b) •)

**S1A.21** Using an analog (see part c) below) of the Lemma in Supplement S1A.19 c) for commutative rings $\neq 0$, once again we prove free modules over commutative ring $\neq 0$ have rank.

Let $R$ be a ring $\neq 0$.

**a)** Let $w_1,\ldots,w_{n+1}$ be linearly independent elements in free $R$-module $V$ with the basis $v_1,\ldots,v_n$. Then $V$ has a free submodule with a countably infinite basis (**Hint :** For $k\in\mathbb{N}$, recursively construct linearly independent elements $u_0,\ldots,u_k\in V$ and free submodules $U_k\subseteq V$ with a basis consisting of $n$ elements such that the direct sum decomposition $Ru_1\oplus\cdots\oplus Ru_k\oplus U_k$ holds. Then $u_0,u_1,u_2,\ldots$ generate the required submodule. One can begin with $u_0:=w_1$, $U_0:=Rw_2\oplus\cdots\oplus Rw_{n+1}$.)

**b)** If $R$ is left-noetherian and $n\in\mathbb{N}$, then every $n+1$ elements in a $R$-module $V$ with $\mu_R(V)\leq n$ are linearly dependent. (We may assume that $V\cong R^n$, and note that $R^n$ is a noetherian $R$-module. – From a) it also follows that the analogous assertion for left-artinian rings. But, this already follows from the well cited Theorem of Hopkins.)

**c)** With a trick the result in b) can be deduced for an arbitrary *commutative* rings $R\neq 0$ : If $R$ is commutative and $n\in\mathbb{N}$, then every $n+1$ elements in a $R$-module $V$ with $\mu_R(V)\leq n$ are linearly dependent. (We may assume that $R^n$ contain $n+1$ linearly independent elements $w_j=\sum_{i=1}^{n}a_{ij}e_i$, $j=1,\ldots,n+1$. By the Hilbert's Basis Theorem the smallest subring $S:=\mathbb{Z}[a_{ij},1\leq i\leq n,1\leq j\leq n+1]\subseteq R$ of $R$ which contain all the coefficients $a_{ij}$, is noetherian and the elements $w_1,\ldots,w_{n+1}\in S^n$ are also linearly independent over $S$ in $S^n$, a contradiction to b). – The method applied here is to reduce the problem to the noetherian case is also known as noetherization of a problem.)

**S1A.22** We record the following important corollary of the Theorem in Supp S1A.21 b) :

*Let R be a commutative ring* $\neq 0$ *and V an R-module with a generating system* $x_i$, $i\in I$, *and W be a free submodule of V. Then* $\mathrm{Rank}_R W\leq|I|$. (**Proof :** If $I$ is finite, then the assertion follows from directly from the Supplement S1A.21 b). Now, assume that $I$ is infinite and $y_j$, $j\in J$, be a $R$-basis of $W$. Then for every $j\in J$, there exists a finite subset $I(j)$ of $I$ such that $y_j\in\sum_{i\in I(j)}Rx_i$. The map $j\mapsto I(j)$, from $J$ into the set $\mathfrak{P}_{\mathrm{f}}(I)$ of finite subsets $I$ has finite fibres by Supplement S1A.21 b) and hence it follows that $\mathrm{Rank}_R W=|J|\leq|\mathfrak{P}_{\mathrm{f}}(I)|=|I|$. •)

**S1A.23** We prove the following general theorem on the invariance of ranks :

*Let* $\varphi\colon R\to S$ *be a homomorphism of rings. If every free S-module has a rank, then every free R-module also has a rank.* (**Proof :** In view of the Theorem in Supplement S1A.19 a), we have to show that : If $m,n\in\mathbb{N}$ are such that $R^m\cong R^n$, then $m=n$. Suppose that $f\colon R^n\to R^m$ and $g\colon R^m\to R^n$ are $R$-isomorphism which are inverses of each other, which are described by the matrices $\mathfrak{A}=(a_{ij})\in\mathrm{M}_{m,n}(R^{\mathrm{op}})$ and $\mathfrak{B}=(b_{jk})\in\mathrm{M}_{n,m}(R^{\mathrm{op}})$, see Supplement S1A.5 c). Then the product matrices beschreiben die Produktmatrizen $\mathfrak{B}\mathfrak{A}\in\mathrm{M}_n(A)$ and $\mathfrak{A}\mathfrak{B}\in\mathrm{M}_m(A)$ describe the compositions $g\circ f=\mathrm{id}_{R^n}$ resp. $f\circ g=\mathrm{id}_{R^m}$, and hence are the unit matrices $\mathfrak{E}_n$ resp. $\mathfrak{E}_m$. Then the $\varphi$-images $\varphi(\mathfrak{A})=(\varphi(a_{ij}))\in\mathrm{M}_{m,n}(S^{\mathrm{op}})$ and $\varphi(\mathfrak{B})=(\varphi(b_{jk}))\in\mathrm{M}_{n,m}(S^{\mathrm{op}})$ describe $S$-isomorphisms which are inverses of each other $S^n\to S^m$ resp. $S^m\to S^n$. Therefore, by hypothesis on $S$, it follows that $m=n$. •)

– **Remark :** The theory of rings is essentially the theory of modules over rings, where as in the commutative algebra all modules over noetherian commutative rings are considered. On the other hand, in the linear algebra most part is occupied with linear maps between free modules and thereby in particular, with the structure of linear maps between vector spaces (which are free by the Theorem on the existence of bases, see Supplement S1A.13 f)). In the case of fields, it comes along with the groups of homomorphisms $\operatorname{Hom}_K(V,W)$ which are even $K$-vector spaces.

**S1A.24** (Rank of arbitrary modules over integral domains) Let $R$ be an integral domain, $V$ an arbitrary $R$-module and $x_i$, $i \in I$, be a linearly independent system of elements of $V$. Then, obviously, $a_i x_i$, $i \in I$, is also a linearly independent system in $V$ for every $(a_i) \in R^I$ with $a_i \neq 0$, $i \in I$.

The set of linearly independent subsets of $V$ is inductively ordered by the natural inclusion and hence by Zorn's Lemma every linearly independent subset of $V$ is contained in a maximal linearly independent subset of $V$. Therefore, if $y_j$, $j \in J$, is an arbitrary linearly independent system in $V$ for every $y_j$ there exists a non-trivial relation in the $x_i$, $i \in I$, and $y_j$, i.e. there exist $a_j \in R$, $a_j \neq 0$, with $a_j y_j \in F := \sum_{i \in I} Rx_i$. Now, $a_j y_j$, $j \in J$, are linearly independent and hence generate a free submodule of $F$ of the rank $|J|$. Therefore by Supplement S1A.22 $|J| \leq \operatorname{Rank}_R F = |I|$. It follows trivially that any two maximal linearly independent system of elements in $V$ have the same cardinality. This common cardinality is called the rank of $V$ over $R$ and also denote it by $\operatorname{Rank}_R V$. If $V$ is a free $R$-module, then this is same as already defined rank of $V$ as a free $R$-module. If $W$ is a submodule of $V$, then $\operatorname{Rank}_R W \leq \operatorname{Rank}_R V$. If $W$ is a submodule of $V$ and if for every $y \in V$, there exists an $a \in R$, $a \neq 0$, with $ay \in W$, then even $\operatorname{Rank}_R W = \operatorname{Rank}_R V$, since every maximal linearly independent system in $W$ also such a system in $V$. The $R$-modules of rank 0 are precisely the torsion modules over $R$.
Es sei bemerkt, daÃą man den hier eingefÂĄhrten allgemeinen Rangbegriff durch Åąbergang zum QuotientenkâĂİrper von $A$ leicht auf den Dimensionsbegriff bei VektorrâĂđumen zurÂĄckfÂĄhren kann, vgl. Teil 2, §51, Beispiel 11.

**S1A.25** *Let R be a ring and V be a free R-module of infinite rank. Then*

$$|V| = |R| \cdot \operatorname{Rank}_R V = \operatorname{Sup}\{|R|, \operatorname{Rank}_R V\}\,.$$

(**Proof :** Let $x_i$, $i \in I$, be a $R$-basis of $V$. Then $|I| = \operatorname{Rank}_R V$. We have to show that $V$ and $R \times I$ have the same cardinality. By we have the equality $|R| \cdot |I| = \operatorname{Sup}\{|A|, |I|\}$. Let $R_1 := R \setminus \{0\}$. If $R$ is finite, then $|R \times I| = |I|$ and $|R_1 \times I| = |I|$ by If $R$ is infinite, then $|R| = |R_1|$. In any case, $|R \times I| = |R_1 \times I|$. The map $(a,i) \mapsto ax_i$ from $R_1 \times I$ into $V$ is injective. It follows that $|R \times I| = |R_1 \times I| \leq |V|$.
Nach 7.6 besitzt die unendliche Menge $A \times I$ dieselbe MâĂđchtigkeit wie die Menge $\mathfrak{E}(A \times I)$ der endlichen Teilmengen von $A \times I$. Die Abbildung $E \mapsto \sum_{(a,i) \in E} ax_i$ von $\mathfrak{E}(A \times I)$ in $V$ ist aber surjektiv, woraus $|A \times I| = |\mathfrak{E}(A \times I)| \geq |V|$ folgt. Beide Ungleichungen zusammen ergeben mit dem Bernsteinschen Å¡quivalenzsatz die Gleichheit $|A \times I| = |V|$. •

— Note that $\operatorname{Dim}_{\mathbb{Q}}\mathbb{R} = \operatorname{Dim}_{\mathbb{Q}}\mathbb{C} = \aleph$; in words : The cardinality of the Hamel's basis of $\mathbb{R}$ and $\mathbb{C}$ over $\mathbb{Q}$ are equal to the cardinality of the continuums. Since $|\mathbb{Q}| \leq |\mathbb{R}| = |\mathbb{C}| = \aleph$, the assertion follows directly from Supplement S1A.25.)

**S1A.26** Let $R$ 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 $(\delta_{ij})_{j \in I} \in R^I$ 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 left-ideal $R^{(I)}$ in the ring $R^I$. In particular, $R^{(I)}$ is not finitely generated ideal.

**0..1 Remark** Submodules of finitely generated modules need not be finitely generated!

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

**S1A.27** Let $R$ be a commutative ring. Then the $R$-module $R$ is always torsion-free. More generally, every free $R$-module is torsion-free.

**(a)** Direct sum of torsion-modules is again a torsion-module. A submodule of a torsion-module is a torsion-module.

**(b)** Direct product of torsion-free modules is again a torsion-free module. A submodule of a torsion-free module is a torsion-free module.

**(c)** In an abelian group (in any $\mathbb{Z}$-module) torsion-elements are precisely the set of elements of positive order. The $\mathbb{Z}$-module $\mathbb{Q}$ is torsion-free. Every finite abelian group if a $\mathbb{Z}$-torsion module. For $n \in \mathbb{N}^*$, let $\mathrm{Z}_n$ denote a cyclic group of order $n$. Then the direct product $\prod_{n \in \mathbb{N}^*} \mathrm{Z}_n$ of the $\mathbb{Z}$-torsion modules $\mathrm{Z}_n$, $n \in \mathbb{N}^*$, is not $\mathbb{Z}$-torsion module.

**S1A.28** Let $R$ be an integral domain with quotient field $K$. Then :

**a)** If $V$ is a torsion module over $R$, then $\operatorname{Hom}_R(V,R) = 0$.

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

**a)** If $K$ is an arbitrary direct sum of finite $R$-submodules, then $R = K$.

**S1A.29** (Maximal submodules) Let $R$ be a commutative ring and let $V$ be an $R$-module. Then maximal elements (with respect to the natural inclusion) in the set $\mathcal{S}_R(V)$ of all $R$–submodules of $V$ are called maximal $R$-submodules of $V$. Maximal $R$- submodules of the $R$-module $R$ are precisely are maximal ideals in $R$. Let $W$ be a maximal $R$-submodule of $V$ and let $x \in V, x \notin W$. Then $W \neq W + Rx$ and by the maximality of $W$, we have the equality $W + Rx = V$. Therefore $W$ is a cofinite $R$-submodule in the sense of the following definition :

An $R$-submodule $W$ of $V$ is called cofinite if there exists finitely many elements $x_1,\ldots,x_n \in V$ such that $V = W + Rx_1 + \cdots + Rx_n$. Equivalently, the quotient $R$-module $V/W$ is finitely generated.

If $W$ is a cofinite $R$-submodule of $V$, then every $R$-submodule $W'$ with $W \subseteq W' \subseteq V$ is also cofinite. Every $R$-submodule of a finite $R$-module is cofinite. Note that *in any $R$-module $V$ cofinite $R$-submodules different from $V$ exists if $V$ has maximal submodules.*

**a)** Prove the converse : Let $W$ be a cofinite $R$-submodule of an $R$-module $V$ with $W \neq V$. Then there exists a maximal $R$-submodule of $V$ which contain $W$. In particular, in a finite non-zero $R$-module $V$ there are maximal $R$-submodules.

**b)** Use a) to deduce the (Krull's Theorem): Let $R$ be a ring and let $\mathfrak{a}$ be an ideal in $R$ with $\mathfrak{a} \neq R$. Then there exists a maximal ideal $\mathfrak{m}$ in $R$ with $\mathfrak{a} \subseteq \mathfrak{m} \subsetneq R$. In particular, in every non-zero ring, there are maximal left-ideals.

**S1A.30** Let $R$ be a ring and let $V \neq 0$ be an $R$-module. If $R$, does not have maximal submodules, then $R$ does not have a minimal generating system. (**Hint :** If $x_i, i \in I$ is a minimal generating system for $V$, then $I \neq \emptyset$. Let $i_0 \in I$ and $W := \sum_{i \in I \setminus \{i_0\}} Ax_i$. Then $W$ is a cofinite submodule of $V$ and hence $V$ has maximal submodules.)

**S1A.31** (Jacobson-radical) Let $R$ be a commutative ring. The intersection of all maximal ideals of $R$ is called the Jacobson−radical of $R$ and is denoted by $\mathfrak{m}_R$. Note that $\mathfrak{m}_R \neq R$ if and only if there exists a maximal ideal in $R$. Equivalently, $R \neq 0$.

**a)** Let $V$ be an $R$-module and let $U$ be a cofinite submodule of $V$. If $V = U + \mathfrak{m}V$ for all maximal ideals $\mathfrak{m}$ of $R$, then $V = U$.

**b)** Let $R$ be a commutative ring and $V$ be a finite $R$-module. If $V = \mathfrak{m}V$ for all maximal ideals $\mathfrak{m}$ of $R$, then $V = 0$. (Apply a) with $U := 0$.)

**c)** (Lemma of Krull−Nakayama) Let $R$ be a commutative ring and $\mathfrak{a}$ be an ideal in $R$. Then the following statements are equivalent:

(i) $\mathfrak{a} \subseteq \mathfrak{m}_R$.

(ii) For every $R$-module $V$ and every cofinite submodule $U$ of $V$ the implication holds: If $V = U + \mathfrak{a}V$, then $V = U$.

**S1A.32** (Simple modules) Let $R$ a (commutative) ring $\neq 0$. An $R$-module $V$ is called simple, if $V \neq 0$ and the only submodules of $V$ are the trivial submodules 0 and $V$.

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

**b)** Let $V$ be simple $R$-module. Then the annihilator ideal $\operatorname{Ann}_R V$ of $V$ is the intersection of the maximal ideals $\operatorname{Ann}_R x$, $x \in V \setminus \{0\}$.

**S1A.33** Let $f\colon V \to W$ be a homomorphism of $R$-modules.

**a)** For a submodule $U \subseteq V$, it is $f^{-1}(f(U)) = U + \operatorname{Ker} f$ and

$$U/(U \cap \operatorname{Ker} f) \xrightarrow{\sim} (U + \operatorname{Ker} f)/\operatorname{Ker} f \xrightarrow{\sim} f(U).$$

**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 $\operatorname{Ker} f$ and the set of all submodules $X$ of $W$.

**c)** Let $V$ and $W$ be simple $R$-modules, see Exercise S1A.32. Then every $R$-homomorphism $V \to W$ is either the zero-homomorphism or an isomorphism. In particular, $\operatorname{End}_R V$ is a division domain (Lemma of (Issai) Schur).

**d)** If $R$ is commutative, then the modules $R/\mathfrak{m}$, $\mathfrak{m} \in \operatorname{Spm} R$, up to isomorphism, are the only simple $R$-modules and distinct maximal ideals of $R$ define non-isomorphic simple $R$-modules. (**Remark :** Note that $\operatorname{Ann}_R(R/\mathfrak{m}) = \mathfrak{m}$. – The classification of the simple modules over non-commutative rings is complicated. A local ring $R$ with Jacobson-radical $\mathfrak{m}_R$ has the residue-class division domain $R/\mathfrak{m}_R$ (as $R$-module), up to isomorphism, are the only simple $R$-modules.)

**e)** If $V$ is a $K$-vector space, $V \neq 0$, then $V$ is a simple $\operatorname{End}_K V$-module, see Example S1.?? The endomorphisms of $V$ as $\operatorname{End}_K V$-module are the homothecies $\vartheta_a$, $a \in K$, of $V$. Therefore $\operatorname{End}_{\operatorname{End}_K V} V \cong K$ the image of the action homomorphism $\vartheta\colon K \to \operatorname{End} V$.

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

**a)** $U$ is a direct summand of $V$ if and only if there exists a projection $p \in \operatorname{End}_R V$ with $\operatorname{Im} p = U$. In this case, $V = U \oplus W$ with $W := \operatorname{Ker} p$, $p = p_{U,W}$ is called the projection onto $U$ along $W$, and the complementary projection $q = q_{U,W} = \mathrm{id}_V - p_{U,W} = p_{W,U}$ is the projection along $U$ onto $W$.

**b)** If $R = K$ is a division domain, then every subspace $U \subseteq V$ has a complement.

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

**S1A.34** (Indecomposable Modules) Let $V$ be an $R$-module over the ring $R \neq 0$. We say that $V$ is indecomposable or irreducible, if $V \neq 0$ and there is no direct sum decomposition $V = U \oplus W$ with submodules $U \neq 0 \neq W$ of $V$.

**a)** $V$ indecomposable if and only if $V \neq 0$ and the endomorphism ring $\operatorname{End}_R V$ has no non-trivial idempotent elements. Every simple $R$-module is indecomposable. Give an example of a indecomposable module which is not simple. The

$R$-(left- or right-)module $R$ is indecomposable if and only if the ring $R$ has no non-trivial idempotent elements. (Note the explicit distinction of this with the indecomposability of $R$ as ring. This is equivalent to that $R$ has no non-trivial *central* idempotent elements.)

**b)** The only indecomposable vector spaces over a division domain $K$ are the 1 dimensional vector spaces. (In general it is difficult – if not impossible, to classify the indecomposable modules over a given ring $R$. 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 the substantial part of the main theorem the finitely generated abelian groups. However, there are many more indecomposable abelian groups, for example, all non-zero subgroups of $\mathbb{Q} = (\mathbb{Q}, +)$ are indecomposable and similarly, all Prüfer's $p$-groups $\mathrm{I}(p)$, $p \in \mathbb{P}$, are also indecomposable. Every abelian $p$-group with 1-dimensional (i.e. non-zero cyclic) $p$-socal is indecomposable. Up to isomorphism these are precisely the groups $\mathbf{Z}_{p^\alpha}$, $\alpha \in \mathbb{N}^*$, and $\mathrm{I}(p)$. Why?)

**S1A.35** A ring $R \neq 0$ is a division domain if and only if all $R$-(left-) modules (or if all $R$-right modules) are free.

**S1A.36** Let $V$ be a module over the local ring $R$ with the Jacobson-radical $\mathfrak{m}_R$ and $v_i$, $i \in I$, be a family of elements in $V$.

**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 $\mathrm{Syz}_R(v_i, i \in I) \subseteq \mathfrak{m}_R R^{(I)}$. In this case (Note that $R^\times = R \smallsetminus \mathfrak{m}_R$), the residue-classes $[v_i] \in V/\mathfrak{m}_R V$, $i \in I$, form a $(R/\mathfrak{m}_R)$-basis of $V/\mathfrak{m}_R V$, and it follows

$$\mu_R(V) = |I| = \mathrm{Dim}_{R/\mathfrak{m}_R}(V/\mathfrak{m}_R V)\,.$$

In particular, for every finite $R$-module $V$, we have $\mu_R(V) = \mathrm{Dim}_{R/\mathfrak{m}_R}(V/\mathfrak{m}_R V)$ and $V = 0$ if and only if $V = \mathfrak{m}_R V$ ist.

**b)** If $U \subseteq V$ is a submodule of $V$ such that the residue-class module $V/U$ is finite and if $V = U + \mathfrak{m}_R V$, then $V = U$ (Lemma of Nakayama). (Since $V/U = \mathfrak{m}_R(V/U)$, it follows $V/U = 0$.) If $V$ is finite, then the elements $v_i$, $i \in I$, generates $V$ if and only if their residue-classes generates the vector space $V/\mathfrak{m}_R V$.

**S1A.37** Let $R$ be a ring $\neq 0$.

**a)** If $R^m \cong R^{m+1}$ (as $R$-modules) for a natural number $m \in \mathbb{N}$, then $R^m \cong R^n$ for all $n \geq m$.

**b)** Elements $x, y \in R$ form a basis of the $R$-module $R$ if and only if there exist elements $a, b \in R$ such that (1) $ax + by = 1$, (2) $xa = 1$, (3) $xb = 0$, (4) $ya = 0$ und (5) $yb = 1$. (In the matrix notation

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

where all matrices are considered over the opposite ring $A^{\mathrm{op}}$.)

**c)** Let $B$ be a ring $\neq 0$ and $V$ be an $B$-module $\neq 0$ with $V \cong V \oplus V$ (e.g. a free $B$-module with infinite basis). Then there exist elements $a, b, x, y$ in the endomorphism ring $R := \mathrm{End}_B V$ satisfying the equations (1) to (5) in b). In particular, the finite free $R$-modules does not have rank. (Describe the isomorphisms $V \xrightarrow{\sim} V \oplus V$ and $V \oplus V \xrightarrow{\sim} V$ which are inverses to each other by matrices with coefficients in the ring $\mathrm{End}_R V$.)

**S1A.38** Let $V$ be an additive abelian group. Then $V$ is the additive group of a $\mathbb{Q}$-vector space if and only if $V$ is torsion free and divisible. Moreover, in this case, the $\mathbb{Q}$-vector space structure on $V$ is uniquely determined. (**Hint:** For $a, b \in \mathbb{Z}$, $b \neq 0$, it is $\vartheta_{a/b} = \vartheta_a\, \vartheta_b^{-1} = \vartheta_b^{-1}\, \vartheta_a$.)

If $V, W$ are arbitrary torsion free and divisible abelian groups, then $\mathrm{Hom}(V, W) = \mathrm{Hom}_{\mathbb{Z}}(V, W) = \mathrm{Hom}_{\mathbb{Q}}(V, W)$. (**Hint:** If $V$ torsion free and divisible, then the characteristic homomorphism $\mathbb{Z} \to \mathrm{End}\, V$ maps the $\mathbb{Z}^*$ into $\mathrm{Aut}\, V$ and hence it can be extended to a unique ring homorphism $\mathbb{Q} \to \mathrm{End}\, V$.)

Therefore, up to isomorphism, the torsion free and divisible abelian groups are precisely the direct sums $\mathbb{Q}^{(I)}$, $I$ arbitrary set. Since $|\mathbb{Q}^{(I)}| = |I|$ for infinite sets $I$, it follows, in particular, that two uncountable torsion free and divisible abelian groups are isomorphic if and only if they have the same cardinality. For example, the additive groups of the $\mathbb{R}$-vector spaces $\mathbb{R}^n$, $n \in \mathbb{N}^*$, as well as $\mathbb{R}^{(\mathbb{N})}$ and $\mathbb{R}^{\mathbb{N}}$ are all isomorphic to each other.