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

Evaluation Weightage : Assignments : 20% **Seminars :** 30% **Final Examination :** 50%

Range of Marks for Grades (Total 100 Marks)						
	Grade S	**Grade A**	**Grade B**	**Grade C**	**Grade D**	**Grade F**
Marks-Range	> 90	76 — 90	61 — 75	46 — 60	35 — 45	< 35

	Grade A$^+$	**Grade A**	**Grade B$^+$**	**Grade B**	**Grade C**	**Grade D**	**Grade F**
Marks-Range	> 90	81 — 90	71 — 80	61 — 70	51 — 60	40 — 50	< 40

1. Modules and Algebras

Submit a solutions of $*$-Exercises ONLY. **Due Date : Wednesday, 30-08-2017**

1.1 Determine the quotient and the remainder of the division :

a) of $f \in K[X]$ by $X^2 - a$ in $K[X]$, where K is a field.

b) of $X^m - 1$ by $X^n - 1$ in $\mathbb{Z}[X]$ for $m, n \in \mathbb{N}^*$.

1.2 Let R be a commutative ring, $g \in A[X]$ be a polynomial of degree $n \geq 1$, with leading coefficient a unit and $\varepsilon_g : R[X] \to R[X]$ be the substitution homomorphism with $X \mapsto g$. Let $B = (R[X], \varepsilon_g)$ be the $R[X]$-algebra with the structure homomorphism. Then the $R[X]$-algebra B is free of rank n with basis $1, \ldots, X^{n-1}$. What is the kernel of the canonical $R[X]$-algebra homomorphism $(R[X])[Y] \to B$ with $Y \mapsto X$?

1.3 Let R be a commutative ring, $\mathrm{P} := R[X_i]_{i \in I}$ be the polynomial algebra and $f = \sum a_\nu X^\nu \in \mathrm{P}$.

a) f is nilpotent if and only if all the coefficients of f are nilpotent.

b) f is a unit in P if and only if a_0 is a unit in R and all coefficients a_ν, $\nu \neq 0$, of f are nilpotent. (**Hint :** We may assume that $\mathrm{P} = R[X]$. Let $m := \deg f > 0$. It is enough to prove that a_m is nilpotent. But $fg = 1$ with $g = b_0 + \cdots + b_n X^n$, and so by induction $a_m^{i+1} b_{n-i} = 0$ for $i = 0, \ldots, n$. **Variant :** Pass to the ring of fractions R_S, $S := \mathrm{S}(a_m)$, and apply the degree formula.)

c) (Theorem of McCoy) f is a zero-divisor in P if and only if there exists $a \in R$, $a \neq 0$ such that $af = 0$. (**Hint :** We may assume that I is finite with $|I| = n$. First, suppose that $n = 1$, i.e. $\mathrm{P} = R[X]$, $fg = 0$ with $g \in P$, $m := \deg f$, $\deg g > 0$. In the case $a_i g = 0$ for all i is the assertion is trivial. Otherwise, let r the maximum of i with $1 \leq i \leq m$ and $a_i g \neq 0$. Then $\deg(a_r g) < \deg g$ and $f \cdot (a_r g) = 0$. — Now, suppose that $n \geq 1$ and $f = \sum_{i=0}^m f_i X_n^i$ with $f_i \in \mathrm{Q} := R[X_1, \ldots, X_{n-1}]$. If $fg = 0$ with $g \in \mathrm{Q}$, $g \neq 0$, then $hg = 0$ for all $h = \sum_{i=0}^m f_i X_{n-1}^{s_i}$ in Q with $s_i \in \mathbb{N}$ arbitrary. Apply the induction hypothesis to h and choose s_i so that s_{i+1} enough bigger than s_i .)

d) f is idempotent if and only if $f = a_0$ is a constant polynomial and a_0 is idempotent in R. (**Hint :** We may assume that $\mathrm{P} = R[X]$. Since f is idempotent, so are a_0 and $(f - a_0)^2$ and hence $(f - a_0)^2 = 0$ and $f = a_0$.)

$*$**1.4** Let R be a commutative ring and $\mathbf{Z}_n$ be a cyclic group of the order $n \geq 1$. Then the R-algebras $R[\mathbf{Z}_n]$ and $A[X]/(X^n - 1)$isomorphic.

$*$**1.5** Let M be a regular totally ordered monoid with neutral element ι and $B = \sum_{\sigma \in M}^{\oplus} B_\sigma$ be an M-gradaded domain.

a) Every left- or right divisor of a homogeneous element $\neq 0$ of B is again homogeneous. In particular, all units in B are homogeneous.

b) Let B be commutative (and hence an integral domain), $\mathfrak{p} \subseteq B$ be a homogeneous prime ideal in B and $b = \sum_{\sigma \in M} b_\sigma \in B$ be an element $\neq 0$ with the leading form b_ω and initial form b_α, $\alpha \leq \omega$. If $b_\sigma \in \mathfrak{p}$ for all $\sigma \neq \omega$, $b_\omega \notin \mathfrak{p}$ and $b_\alpha \notin \mathfrak{p}^2$, then every divisor of b in B is homogeneous. In particular, if p is a homogeneous prime element $\neq 0$ in B and if $p \mid b_\sigma$ for $\sigma \neq \omega$ as well as $p \nmid b_\omega$ and $p^2 \nmid b_\alpha$, then all divisors of b in B are homogeneous. (**Remark :** This is so-called Lemma of Eisenstein (due to G. Eisenstein (1823-1852)) which has many variants.)

1.6 Let R be a commutative ring $\neq 0$ and $P := R[X_i, i \in I]$ be the polynomial algebra over R in indeterminates X_i, $i \in I$. Further, let $F = \sum_{\nu \in \mathbb{N}^{(I)}} a_\nu X^\nu \in P$.

a) It is $\nu!\, a_\nu = \left(\mathrm{D}_X^\nu F\right)(0)$, $\nu \in \mathbb{N}^{(I)}$. (Remember the definition $\nu! = \prod_i \nu_i!$. – It is enough to prove the formula for monomial $F = X^\mu$, $\mu \in \mathbb{N}^{(I)}$.)

b) Let $c=(c_i)\in S^I$. The polynomials $(X-c)^\nu=\prod_i(X_i-c_i)^{\nu_i}$, $\nu\in\mathbb{N}^{(I)}$, form an R-module basis of P. (The substitution homomorphism $P\to P$, $X_i\mapsto X_i-c_i$, $i\in I$, is an R-algebra automorphism of P, a so-called translation automorphism of P.)

If $F=\sum_{\nu\in\mathbb{N}^{(I)}}b_\nu(X-c)^\nu$, then prove the Taylor-Formula

$$\nu!\,b_\nu=\left(\mathrm{D}_X^\nu F\right)(c)\,.$$

(If $\mathbb{Q}\subseteq S$, then $b_\nu=(1/\nu!)\left(\mathrm{D}_X^\nu F\right)(c)$, $\nu\in\mathbb{N}^{(I)}$.)

c) Let $r\in\mathbb{N}^*$ and $n\in\mathbb{N}$. Using the Taylor-Formula in $\mathbb{Z}[X_1,\dots,X_r]$ prove the universal polynomial formula

$$(X_1+\cdots+X_r)^n=\sum_{\nu\in\mathbb{N}^r,|\nu|=n}\binom{n}{\nu}X^\nu$$

and the universal polarisation formulae

$$2^{r-1}r!\,X_1\cdots X_r=\sum_\varepsilon\varepsilon_2\cdots\varepsilon_r(X_1+\varepsilon_2X_2+\cdots+\varepsilon_rX_r)^r$$

(on the right hand side the sum runs through all the sign-tuples $\varepsilon=(\varepsilon_2,\dots,\varepsilon_r)\in\{1,-1\}^{r-1}$) and

$$(-1)^r r!\,X_1\cdots X_r=\sum_{H\subseteq\{1,\dots,r\}}(-1)^{|H|}X_H^r=\sum_e(-1)^{e_1+\cdots+e_r}(e_1X_1+\cdots+e_rX_r)^r$$

(in the last sum e runs through the tuples $(e_1,\dots,e_r)\in\{0\,,1\}^r$).

1.7 Let R be a commutative ring $\neq 0$ and $P:=R[X_i,i\in I]$ be the polynomial algebra over R in the indeterminates X_i, $i\in I$. The map $\mathrm{Der}_S P\xrightarrow{\sim}P^I$, $\delta\mapsto\left(\delta(X_i)\right)_{i\in I}$, is a P-module isomorphism. For every I-tuple $(G_i)\in P^I$ $\delta\colon F\mapsto\sum_{i\in I}\left(\mathrm{D}_{X_i}F\right)G_i$, is a R-derivation. In particular, if I is finite, then $\mathrm{Der}_S P$ is a free P-module of rank $|I|$ with basis D_{X_i}, $i\in I$.
(**Remark :**. In particular, it follows that for sets I,J with $|I|\neq|J|$ the R-algebras P and $Q:=R[X_j,j\in J]$ are not isomorphic if one of the sets is finite. However, this is also true if both sets I and J are not finite; this follows from $\mathrm{Rang}_S P=|\mathbb{N}^{(I)}|=|I|$ if I is infinite. Note that the R-algebras P and Q may be isomorphic even if $|I|\neq|J|$. For example, for infinite set I, P and $P[Y_k,k\in K]$ are isomorphic rings if $|K|\leq|I|$.)

1.8 Let K be a field. The K-algebra automorphisms of $K[X]$ are precisely the substitution homomorphisms $X\mapsto aX+b$, $a,b\in K$, $a\neq 0$. Therefore the group $\mathrm{Aut}_{K\text{-Alg}}K[X]$ of the K-algebra automorphisms of $K[X]$ is anti-isomorphic and hence isomorphic to the affine group $\mathrm{A}_1(K)=K\rtimes K^\times$ of K, see Example ???. (The K-automorphism gruoup of a polynomial algebra $K[X_1,\dots,X_n]$, $n\geq 2$, is much more complicated in more than one variable and is still an object of active rearch. For an important subgroup see the next Exercise.)

1.9 Let K be a field and L_i, $i\in I$, be a family of homogeneous polynomials of degree 1 in the polynomial algebra $P:=K[Y_j]_{j\in J}$. The substitution homomorphism $X_i\mapsto L_i$, $i\in I$, from $K[X_i]_{i\in I}$ into P is injective resp. surjective, resp. bijective, if and only if the L_i, $i\in I$, is linearly independent, resp. a generating system, resp. a basis of the K-vector space P_1 of all homogeneous polynomials of degree 1 in $K[Y_j]_{j\in J}$. In particular, in the case $I=J$ the substitution endomorphism $P\to P$, $Y_j\mapsto L_j$, $j\in J$, is a K-algebra automorphism if and only if its restriction to P_1 is a K-vector space automorphisms of P_1. (With this one can identify the general linear group $\mathrm{GL}_K(P_1)=\mathrm{Aut}_K(P_1)$ with the subgroup of $\mathrm{Aut}_{K\text{-Alg}}P$. Together with the translation automorphisms aus Aufg. 2.9.4b) they generate the so-called group of the affine K-algebra automorphisms of P.)

*__1.10__ **a)** Over an integral domain R every R-algebra automorphism φ of $A[X]$ is a linear automorphism. (**Hint :** We may assume that the constant term of $\varphi(X)$ is 0. Then the ideal $R[X]X$ is φ-invariant.)

b) Let R be a commutative ring and φ be an R-algebra endomorphism of $R[X]$. Then φ is an automorphism if and only if $\varphi(X)=a+gX$ with $a\in R$ and $g\in R[X]^\times$. (**Hint :** Suppose that φ is of the given form and $\mathfrak{a}$ be the ideal generated by the coefficients other than the constant term. Then $\mathfrak{a}$ is a niltoptent ideal by Exercise S.14 b). Now, pass to the residue-class ring is $(R/\mathfrak{a})[X]$ and apply Exercise 42, 6a).)

*__1.11__ For $m\in\mathbb{N}$, let $P_m:=K[X_1\dots,X_m]$ be the polynomial algebra in m indeterminates over the field K. If $\varphi\colon P_m\to P_n$ is an injective, (resp. surjectiv) K-algebra homomorphism, then $m\leq n$ (resp. $m\geq n$). In particular, $m=n$, if φ is an isomorphism. (If $\deg\varphi(X_i)\leq d$, $i=1,\dots,m$, then $\deg\varphi(F)\leq d\cdot\deg F$ for all $F\in P_m$. Further, use the fact that the polynomials in P_m of $\deg\leq r\in\mathbb{N}$ form a K-vector space of dimension $\binom{r+m}{m}$ bilden. – In the case of that φ surjective, one can reduce to the case of that φ is injective. – Another proof for $m=n$, if φ is a K-algebra isomorphism, one can find in Exercise 1.5. If $m\neq n$, then P_m and P_n are not isomorphic even as rings ; because every ring isomorphism induces an automorphism of K, since $K^\times=P_m^\times=P_n^\times$.)

1.12 Let K be an infinite field and F,G polynomials in $K[X_i,i\in I]$. If $F\neq 0$ and G vanish on $K^I\setminus\mathrm{V}_K(F)$, then $G=0$.

*__1.13__ Let R be a noetherian commutative ring $\neq 0$ and let $\Phi:R[X]\to R^R$ be the canonical homomorphism. (R noetherian is not necessary for this.)

a) If R is a finite ring, then Φ is not injective.

b) Φ is surjective if and only if R is a finite field. Moreover, in this case, the kernel of Φ is generated by $X^q - X = (X^{q-1} - 1)X$, where $q := |R|$. (R noetherian is not necessary for this.)

c) If Ker Φ contains a monic polynomial, then R is a finite ring. (Suppose on the contrary that R is infinite. Then by passing to the residue-class ring modulo an ideal in R which is maximal in the set of ideals with infinite residue-class rings, we may further assume that all residue-class rings of R are finite. There exist elements $a, b \in R$ with $a \neq 0$, $b \neq 0$, $ab = 0$. With R/Ra and R/Rb, the residue-class ring $R/Rab = R$ is also finite.)

d) Show that Φ is *not* injective if and only if there exists a maximal ideal $\mathfrak{m}$ in R and an element $a \neq 0$ with $a\mathfrak{m} = 0$ and the residue-class field $R/\mathfrak{m}$ is finite.

e) (P. Samuel) For every $n \in \mathbb{N}_+$, there exist only finitely many ideals $\mathfrak{a}$ in A with $|R/\mathfrak{a}| \leq n$ (**Hint :** Let $f := \prod_{i=0}^{n-1}(X^n - X^i)$ and $\mathfrak{c}$ be the intersection of ideals $\mathfrak{a}$ with $|R/\mathfrak{a}| \leq n$. Then $f(x) \in \mathfrak{c}$ for all $x \in R$ and hence by a) $R/\mathfrak{c}$ is finite. – **Remark :** The number theoretic function $\mathfrak{z}_R : \mathbb{N}_+ \to \mathbb{Z}$, $n \mapsto \mathfrak{z}_R(n) :=$ the number of ideals $\mathfrak{a}$ in R with $|R/\mathfrak{a}| = n$, is called the Dedekind's Funktion of R. It is multiplicative (Proof!). The associated Dirichlet's series

$$\zeta_R = \sum_{n=1}^{\infty} \frac{\mathfrak{z}_R(n)}{n^s}$$

is a complex-analytic function (in s) and is called the Dedekind's Zeta function ζ_R von R. For $R = \mathbb{Z}$, $\mathfrak{z}(n) = 1$ for all $n \in \mathbb{N}_+$; and hence $\zeta_{\mathbb{Z}}$ is the Riemann's Zeta function,.)

f) If V is a noetherian module over R and if $n \in \mathbb{N}_+$, then there exist finitely many submodules of W of V with $|M/N| \leq n$.

g) If B is a (not necessarily commutative) finitely generated R-algebra, then there exists only finitely many (left-, right-, resp. two-sided) ideals $\mathfrak{b}$ in B with $|B/\mathfrak{b}| \leq n$.

*__1.14__ Let K be an infinite field and V be a K-vector space. Every linearly independent family $f_i \in V^*$, $i \in I$, of K-linear forms $V \to K$ is algebraically independent in the K-Algebra K^V of K-valued functions on V. (**Hint :** One can reduce to the case that V is finite dimensional and use the Exercise 7.4, 2016 CSA-E0 219 Linear Algebra and Applications. — Often K-subalgebra of K^V (of all K-valued functions on V), generated by the K-linear forms $V \to K$ is called the algebra of polynomial functions on V. For $V = K^I$ and a *finite* index set I, this coincides with the usual definition.)

1.15 Let K be a field and A be a K-algebra. Further, let $x \in A^*$ be a non-zero divisor and integral (d.h. algebrac over K. Then $x \in A$, even a unit A and $x^{-1} \in K[x]$. (The multiplication by x on the finite K-algebra $K[x]$ is injective and hence bijective.) Determine the minimal polynomial $\mu_{x^{-1}}$ of x^{-1} with the help of the minimal polynomial μ_x of x. (The constant term of μ_x is $\neq 0$.) In particular, A is a division domain if A is a domain and integral over K.

1.16 Let $K \subseteq L$ be an extension of fields. Then the elements of L which are algebraic over K form a subfield of L which contains K. It is called the algebraic closure or the algebraic hull of K in L. If K is finite, then the algebraic hull of K in L is at most countable. If K is infinite, then K and the algebraic hull of K in L have the same cardinality. (The polynomial ring $K[X]$ have the same cardinality as K if K is infinite. – **Remark :** Elements L which are algebraic over the prime field of L are called just algebraic or absolute algebraic. The absolute algebraic elements of L form a countable subfield of L. In particular, the subfield $\overline{\mathbb{Q}}$ of the (absolute) algebraic numbers in $\mathbb{C}$ is countable. and then set $\mathbb{C} \setminus \overline{\mathbb{Q}}$ of transcendental (over $\mathbb{Q}$) complex numbers has the cardinality $\aleph$ of the continuum.In 1874 Cantor gave a proof for the existence of transcendental complex numbers, see Cantor, G.: Über eine Eigenschaft des Inbegriffs aller reellen algebraischen Zahlen, J. für die reine und angew. Math. **74**, 258-262 (1874). However, he did not provide any transcendental complex numbers explicitly. First time such numbers are produced in 1844 by J. Liouville (1809-1882). (Since $\mathbb{C}$ is algebraically closed by the Fundamental Theorem of Algebra, $\overline{\mathbb{Q}}$ is also algebraically closed.))

1.17 Let $K \subseteq L \subseteq M$ be an extension of fields. If M is algebraic over L and L is algebraic over K, then M is also algebraic over K with $\mathrm{Dim}_K M = \mathrm{Dim}_K L \cdot \mathrm{Dim}_L M$.

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

a) Let $G \in R[X]$ be a monic polynomial of degree $m \geq 1$. For every polynomial $F \neq 0$, there exist unique polynomials $P_0, \ldots, P_r$ with $P_r \neq 0$ and

$$F = P_0 + P_1 G + \cdots + P_r G^r, \quad P_i = 0 \quad \text{or} \quad \deg P_i < m, \quad i = 0, \ldots r.$$

(This expansion is the analog of the g-adic expansion of natural numbers and is called the G-adic expansion of F. For $G = X - c$ of degree 1, this is handled in the Taylor-expansion of F in c.)

b) Let $F \in S[X]$ be polynomial of degree n and $c \in S$. The coefficients $b_0, \ldots, b_{n-1}$ of the quotient $Q = b_{n-1} + b_{n-2}X + \cdots + b_0 X^{n-1}$ in the representation $F = F(c) + Q \cdot (X - c)$ are the values $F_0(c), \ldots, F_{n-1}(c)$ in the Horner's Scheme for computation of $F(c) = F_n(c)$ Applying this process to the polynomial Q instead

of F successively one can obtain the coefficients in the Taylor-expansion of F in c. – What are the expansions of the polynomial $X^4-3X^3+5X^2-X+2\in\mathbb{Z}[X]$ at $c=2$ and at $c=-1$.

1.19 Let R be a commutative ring $\neq 0$ and $G=c_0+c_1X+\cdots+c_{n-1}X^{n-1}+X^n\in R[X]$ be a monic polynomial of degree $n\in\mathbb{N}^*$. Assume that n is a unit in R. In the free residue-class R-algebra $R[x]=R[X]/(G)$ of rank n, the element $\widetilde{x}:=x+\frac{1}{n}c_{n-1}$ satisfies the equation $\widetilde{c}_0+\cdots+\widetilde{c}_{n-2}\widetilde{x}^{n-2}+\widetilde{x}^n=0$ with coefficients $\widetilde{c}_i$, $i=n-2,\ldots,0$, in R. In particular, $R[x]=R[\widetilde{x}]$ ~~$2pt\approx$~~ $R[X]/(\widetilde{G})$, where the coefficient of X^{n-1} in the monic polynomial $\widetilde{G}:=\widetilde{c}_0+\cdots+\widetilde{c}_{n-2}X^{n-2}+X^n\in R[X]$ is 0. (The polynomial $\widetilde{G}$ obtained from the polynomial G by the (linear) Tschirnhaus(en)-Transformation (due to W. Tschirnhaus(en) (1651-1708)).)

1.20 Let R be a noetherian commutative ring $\neq 0$ and G_j, $j\in J$, be arbitrary family of polynomials in the polynomial algebra $R[X_1,\ldots,X_n]$. Then there exists a *finite* subset $J'\subseteq J$ with the following property : For every commutative R-Algebra A, $\mathrm{V}_A(G_j, j\in J)=\{x\in A^n \mid G_j(x)=0,\ j\in J\}=\mathrm{V}_A(G_j, j\in J')$. (**Hint :** By Hilbert's Basis Theorem $R[X_1,\ldots,X_n]$ is also a noetherian ring.)

Supplement 1

Modules* and Algebras

* 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.

S1.1 Let A be an R-algebra over the commutative ring $R \neq 0$ and V be an A-left-right-biimodule with $rv = vr$ for all $r \in R$, $v \in V$. Then the direct sum $A \oplus V$ with the multiplication

$$(x,v)\cdot(y,w) = (xy, xw+vy)\,, \quad x,y \in A,\ v,w \in V,$$

is an R-algebra, in which $V = \{0\} \oplus V$ is a twosided ideal with $(A \oplus V)/V \xrightarrow{\sim} A$ and $V^2 = 0$. Further $(A \oplus V)^\times = A^\times \oplus V$. (**Hint :** It is $(x,v)^{-1} = (x^{-1}, -x^{-1}vx^{-1})$ for $x \in A^\times$, $v \in V$. – The R-algebra $A \oplus V$ is called the idealisation of V. If A is commutative, then the idealisation of an arbitrary A-module V is defined and is again commutative.)

S1.2 Let R be a commutative ring, $f_1, \ldots, f_n \in R[X]$ be polynomials of degrees $\leq n-2$ and $x_1, \ldots, x_n \in R$ be arbitrary. Then $\operatorname{Det}(f_i(x_j))_{1\leq i,j\leq n} = 0$.

S1.3 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 ϑ_a is bijective. **Hint:** Consider $\mathbb{Z}$-modules, i.e. Finite abelian groups.

S1.4 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 $U + (W \cap W')$.

S1.5 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*

$$\operatorname{Hom}_R\Big(V, \prod_{i\in I} W_i\Big) \xrightarrow{\sim} \prod_{i\in I} \operatorname{Hom}_A(V, W_i)\,, \quad f \mapsto (p_i f)_{i\in I}\,,$$

is a group isomorphism and if R is commutative, then an R-module isomorphism. The I-tuple $(f_i)_{i\in I} \in \prod_{i\in I} \operatorname{Hom}_R(V, W_i)$ 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 $\bigoplus_{j\in J} V_j := \{(x_j)_{j\in J} \in \prod_{j\in J} V_j \mid x_j = 0 \text{ for almost all } j \in J\}$ 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*

$$\operatorname{Hom}_A\Big(\bigoplus_{j\in J} V_j, W\Big) \xrightarrow{\sim} \prod_{j\in J} \operatorname{Hom}_A(V_j, W)\,, \quad g \mapsto (g\,\iota_j)_{j\in J}\,,$$

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

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

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

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

(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 A-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 p r o d u c t m a t r i x

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

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 $f\colon A^n \to A^m$ is given by an $m\times n$-matrix $\mathfrak{A} = (a_{ij}) \in \mathrm{M}_{m,n}(A^{\mathrm{op}}) = \left(A^{\mathrm{op}}\right)^{\{1,\dots m\}\times\{1,\dots,n\}}$.
It is – as usual common to denote – the elements $\mathfrak{x}\in A^n$ 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^{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 $\mathrm{M}_n(A^{\mathrm{op}})$ of the square $n\times n$-matrices with coefficients in R^{op}.* The identity of R^n is then represented by the u n i t m a t r i x $\mathfrak{E}_n = (\delta_{ij})) \in \mathrm{M}_n(A)$. In the important case when R is commutative, naturally one nedd not distinguish between R and R^{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 :

(D i r e c t s u m s o f s u b m o d u l e s) *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 $\sum_{I\in I}^{\oplus} U_i$.

S1.6 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.

S1.7 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 $i = 1,\dots,n$. Now, try to express $1/b^2$ as a linear combination of x_i, $i = 1,\dots,n$.)

S1.8 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 $(X,\le)$ is called a r t i n i a n if every non-empty subset of X has a minimal element. For example finite ordered sets are artinian. An ordered set is w e l l o r d e r e d 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.)

S1.9 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 $(a_i)_{i\in I} = \sum_{i\in I} a_i e_i$. Therefore the family e_i is a generated system for the R-module $R^{(I)}$. The R-module $R^{(I)}$ is called the f r e e R - m o d u l e 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

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

whose image is the submodule $\sum_{i\in I} Rv_i$ of V generated by v_i, $i \in I$.

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

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

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, $i \in I$.[1] Therefore

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

In particular, $R^{(I)}/\,\mathrm{Syz}_A(v_i, i\in I) \xrightarrow{\sim} V$, 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, $Rx \cong R/\mathrm{Syz}_R x = R/\mathrm{Ann}_R x$. 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.

a) A family of elements v_i, $i \in I$, of elements of the R-module V is called linearly independent over R if

S1.10 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 $e_0 + \cdots + e_n$, $n \in \mathbb{N}$.

S1.11 (Torsion submodule, Torsion modules and Torsion-free Modules) Let R be a commutative ring and let V be an R-module. An element $x \in V$ is called torsion if there exists a non-zero divisor $a \in R$ with $ax = 0$. *The set of all torsion elements in V* $\mathrm{t}(V) = \mathrm{t}_R(V) = \{x \in V \mid x$ *is a torsion element*$\}$ *is an R-submodule of V.* This submodule is called the torsion-submodule of V. An R-module V is called torsion-free if $\mathrm{t}(V) = 0$. If every element of V is torsion, i.e., if $\mathrm{t}(V) = V$ then V is called torsion-module. 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 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 Z_n, $n \in \mathbb{N}^*$, is not $\mathbb{Z}$-torsion module.

S1.12 Let R be an integral domain with quotient field K. Then :

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

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

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

S1.13 (Minimal number of generators and Minimal generating systems) Let R be a commutative ring and V be an R-module. 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

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

$\mu_R(V) \in \mathbb{N}$, 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:

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

b) 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.

c) 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.)

S1.14 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 $\mathrm{Q}(R)$ 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.

(Relation modules and linearly independent families) Let v_i, $i \in I$, be a family of elements of the R-module V.

S1.15 (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.

S1.16 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.)

S1.17 (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 $V = U$.

S1.18 (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 $\mathrm{Ann}_R V$ of V is the intersection of the maximal ideals $\mathrm{Ann}_R x$, $x \in V \setminus \{0\}$.

---

[2] **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.*

S1.19 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 S1.??. 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 ϑ_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.

S1.20 (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?)

S1.21 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.

S1.22 Let V be a module over the local ring R with the Jacobson-radical $\mathfrak{m}_A$ 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 $\operatorname{Syz}_R(v_i, i \in I) \subseteq \mathfrak{m}_R R^{(I)}$. In this case (Note that $R^\times = R \setminus \mathfrak{m}_R$), 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

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

In particular, for every finite R-module V, we have $\mu_R(V) = \operatorname{Dim}_{R/\mathfrak{m}_R}(V/\mathfrak{m}_R V)$ 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 $V/\mathfrak{m}_R V$.

S1.23 Let A be a ring $\neq 0$.

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

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

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

where all matrices are considered over the opposite ring A^{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 $A := \operatorname{End}_B V$ satisfying the equations (1) to (5) in b). In particular, the finite free A-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 $\operatorname{End}_A V$.)

S1.24 Let R be a commutative ring and $P := R[X_i]_{i\in I}$ mit $I \neq \emptyset$. Then the Jacobson-radical $\mathfrak{m}_P$ and the nil-radical $\mathfrak{n}_P$ of P are equal. (**Hint :** $1 + X_i\mathfrak{m}_P \subseteq P^\times$, see Exercise S1.4 b).)

S1.25 Let K be a field and F be a free abelian group. Then the Jacobson-radical of the group ring $K[F]$ is the zero-ideal. (**Hint :** The group ring $K[F]$ entsteht aus einem Polynomring über K durch Nenneraufnahme der Monome. Gradüberlegung wie in vorstehender Aufgabe.)

S1.26 Let R be a commutative ring, A be the formal power series ring $R[\![X]\!]$ in one indeterminate X over R and $f = \sum_{n=0}^{\infty} a_\nu X^\nu \in \mathrm{A}$.

a) If f is nilpotent, then all the coefficients of f are nilpotent. Is the converse true?

b) f is a unit in R if and only if a_0 is a unit in R.