$\mathbf{C_A}$ - 08 MA-312 Commutative Algebra / Jan-Apr 2008

Lectures: Monday/Thursday 11:30–1:00 ; Lecture Hall-II, Department of Mathematics

02. Modules [1]) — Generating Systems, Linear Independence and Free Modules

Max Noether†
(1844-1921)

Emmy Amalie Noether††
(1882-1935)

2.1. Let A be a ring.

a). If $V \neq 0$ is an A–module which does not have maximal submodules, then V does not have a minimal generating system. (**Hint:** Use)

b). Suppose that A be an integral domain and that the set of all non-zero ideals in A have a minimal element (with respect to the inclusion). Show that A is a field. In particular, an integeral domain such that the set of all ideals is an artinian ordered set (with respect to inclusion), is a field.

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

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

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

2.3. Let K_i, $i \in I$, be a family of fields. For every element $a = (a_i)_{i\in I} \in \prod_{i\in I} K_i$, let $\alpha(a)$ denote the zero-set $\{i \in I : a_i = 0\}$ of a. For an ideal $\mathfrak{a} \subseteq \prod_{i\in I} K_i$, let $\alpha(\mathfrak{a}) = \{\alpha(a) : a \in \mathfrak{a}\} \subseteq \mathfrak{P}(I)$. Show that: the map $\mathfrak{a} \mapsto \alpha(\mathfrak{a})$ is an isomorphism of the lattice [2]) of the ideals of $\prod_{i\in I} K_i$ onto the lattice of the filters [3]) defined on I. The ideal $\mathfrak{a}$ is maximal if and only if $\alpha(\mathfrak{a})$

---

[1]) 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.

[2]) **Lattice.** A partially ordered set $(X, \leq)$ is called a l a t t i c e if for every two elements $x, y \in X$, the supremum $\sup\{x, y\}$ and the infimum $\inf\{x, y\}$ exist. For example, the set of all left-ideals in a ring form a lattice with respect to the inclusion. What are $\sup\{\mathfrak{a}, \mathfrak{b}\}$ and $\inf\{\mathfrak{a}, \mathfrak{b}\}$ for left-ideals $\mathfrak{a}, \mathfrak{b}$ in A?

[3]) **Filter on a set.** Let X be any set and let $\mathfrak{P}(X)$ denote the power st of X. A f i l t e r on X is a subset $\mathfrak{F}$ of $\mathfrak{P}(X)$ such that: (1) $\mathfrak{F}$ is closed under finite intersections, i.e. intersection of finitely many elements of $\mathfrak{F}$ belongs to $\mathfrak{F}$. (In particular, the empty intersection $= X \in \mathfrak{F}$). (2) If $Y \in \mathfrak{F}$ and $Y \subseteq Z$, then $Z \in \mathfrak{F}$. Note that $\mathfrak{F} = \mathfrak{P}(X)$ if and only if $\emptyset \in \mathfrak{F}$.

is an ultra-filter [4]) on I. Deduce the following exercise [5]) from the Krull's theorem. Further, show that every finitely generated ideal in $\prod_{i\in I} K_i$ is a principal ideal.

2.4. Let V be a free module over a ring A. Further, let $a \in A$ be not a zero divisor in A. Then the homothecy $\vartheta_a : V \to V, x \mapsto ax$ is injective. Let B be a ring and let A be a subring of B such that B is a free A–module. Show that:

a). An element $a \in A$ is a zero divisor in A, if and only if a is a zero divisor in B. Further, show that $(\mathfrak{a}B) \cap A = \mathfrak{a}$ for all ideals $\mathfrak{a} \subseteq A$.

b). $A^\times = A \cap B^\times$. Moreover, if B is a field, then so is A. (**Hint:** If $a \in A \cap B^\times$, then $B = aB$.)

2.5. Let U, W be free A-submodules of the A–module V. Further, let x_i, $i \in I$, resp. y_j, $j \in J$, be a basis of U resp. W. Show that x_i, y_j, $i \in I$, $j \in J$ together form a basis of $U + W$, if and only if $U \cap W = 0$.

2.6. Let A be a non-zero commutative ring. Show that A is a principal ideal domain if and only if every ideal in A is a free A–submodule of A. (**Remark:** In general this assertion is not true for non-commutative rings. Counter example!)

2.7. Let K be a field and let A be a subring of K such that K is a finite A–module. Show that A is a field. (**Hint:** This is a generalisation of the Test-Exercise T2.5. Note that K contains a quotient field $\mathrm{Q}(A)$ of A. Let $x_1, \ldots, x_m$ be a A-generating system of K and let $y_1, \ldots, y_n$ be a $\mathrm{Q}(A)$–basis of K with $y_1 = 1$. Then $y_1^*(x_1), \ldots, y_1^*(x_m)$ is an A– generating system of $\mathrm{Q}(A)$, where y_1^* is the first coordinate function with respect to the basis $y_1, \ldots, y_n$. Now use the Test-Exercise T2.5.)

2.8. a). The $\mathbb{Z}$–mdoule $\mathbb{Q}$ 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 [6]) and hence every quoteint group of $(\mathbb{Q}, +)$ is also divisible. Further, *If H finitely generated divisible abelian group, then $H = 0$.*)

b). The $\mathbb{Z}$–algebra $\mathbb{Q}$ is not finite type over $\mathbb{Z}$.

2.9. Let x_i, $i \in I$, be a family of n–tuples from $\mathbb{Z}^n$. For a prime number p, let $\mathrm{K}_p (= \mathbb{Z}/\mathbb{Z}p$ denote the prime field of charateristic p. Show that the following statements are equivalent:

(i) The x_i are linearly independent over $\mathbb{Z}$.
(ii) The images of x_i, $i \in I$, in $\mathbb{Q}^n$, are linearly independent over $\mathbb{Q}$.
(iii) There exists a prime number p such that the images of x_i, $i \in I$, in K_p^n, are linearly independent over K_p.
(iv) For almost all prime numbers p, the images of x_i, $i \in I$, in K_p^n, are linearly independent over K_p.

— If $|I| = n$, then the above statements are further equivalent to the following statement:

---

[4]) **Ultra-filters on a set.** The set of filters on a set X is ordered by inclusion and it forms a lattice. Maximal elements in the set of filters on X different from $\mathfrak{P}(X)$ are called ultra-filters on X.

[5]) **Exercise.** Show that if $X \neq \emptyset$, then the set of of filters on X different from $\mathfrak{P}(X)$ is inductively ordered with respect to the inclusion and that every filter on X different from $\mathfrak{P}(X)$ is contained in an ultra-filter on X.

[6]) **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 finitern are not divisible.*

(v) There exists a non-zero integer m such that $m\mathbb{Z}^n \subseteq \sum_{i\in I} \mathbb{Z}x_i$.

2.10. Let x_i, $i \in I$, be a family of n–tuples from $\mathbb{Z}^n$. For every prime number p let K_p denote a field with p elements. Show that the following statements are equivalent:

(i) The x_i, $i \in I$, generate (the $\mathbb{Z}$–module) $\mathbb{Z}^n$. (ii) For every prime numebr p, the images of x_i, $i \in I$, in K_p^n, generate the K_p-vector space K_p^n. (**Hint:** ((ii) $\Rightarrow$ (i): Let $U := \sum_{i\in I} \mathbb{Z}x_i$. Note that by Exercise 2.11, there exists a non-zero integer m with $m\mathbb{Z}^n \subseteq U$. Further: to every prime number p and every $x \in \mathbb{Z}^n$ there exist $x' \in U$, $y \in \mathbb{Z}^n$ such that $x = x' + py$, i.e. $\mathbb{Z}^n \subseteq U + p\mathbb{Z}^n$ for every prime number p. From this deduce that $U = \mathbb{Z}^n$.)

2.11. Let I be a non-empty open interval in $\mathbb{R}$ and let $\mathrm{C}^{\omega}_{\mathbb{R}}(I)$ (respectively, $\mathrm{C}^0_{\mathbb{R}}(I)$) be the $\mathbb{R}$-vector space of all real-analytic[7] (respectively, continuous) real-valued functions on I. Then $\mathrm{C}^{\omega}_{\mathbb{R}}(I) \subseteq \mathrm{C}^0_{\mathbb{R}}(I)$ and if U is a $\mathbb{R}$-subspace of $\mathrm{C}^0_{\mathbb{R}}(I)$ with $\mathrm{C}^{\omega}_{\mathbb{R}}(I) \subseteq U$, then show that $\mathrm{Dim}_{\mathbb{R}}\, U$ has the cardinality of the continuum. (**Hint:** Without loss of generality let $I =]-1, 1[$. Let $(a_{ij})_{i\in\mathbb{N}}$, $j \in J$, be a linearly independent family of 0-1–sequences in $\mathbb{R}^{\mathbb{N}}$, where $|J| = \aleph := |\mathbb{R}|$, see Exercise 4.11. Then the functions $t \mapsto \sum_{i\geq 0} a_{ij}t^i$, $j \in J$, in $\mathrm{C}^{\omega}_{\mathbb{R}}(I)$ are linearly independent over $\mathbb{R}$. **Alternative hint:** the family of the functions $t \mapsto \exp(at)$, $a \in \mathbb{R}$, on I is linearly independent. Similarly, the rational functions $t \mapsto 1/(t-a)$, $a \in \mathbb{R}$, $|a| \geq 1$, are linearly independent in $\mathrm{C}^{\omega}_{\mathbb{R}}(]-1,1[)$.) Prove the analogous results for the complex vector space $\mathrm{H}(U)$ of holomorphic functions defined on a domain $U \subseteq \mathbb{C}$.

2.12. For a given $n \in \mathbb{N}$, let $a_1, \ldots, a_n \in K$ be n distinct elements in a field K. Then the sequences $g_i := (a_i^{\nu})_{\nu\in\mathbb{N}} \in K^{\mathbb{N}}$, $i = 1, \ldots, n$, are linearly independent over K. (**Hint:** Suppose that the g_i are linearly dependent. Without loss of generality we may assume that $\mathrm{Dim}_K(\mathrm{Rel}_K(g_1, \ldots, g_n)) = 1$, see Exercise T2.8-a). Let $(b_1, \ldots, b_n)$ be a basis element of relations. Then the element $(b_1a_1, \ldots, b_na_n)$ is also a relation of the g_i. This is a contradiction.)

2.13. Let K be a field and let I be an infinite set. Then $\mathrm{Dim}_K(K^I) = |K^I|$. (**Hint:** In view of[8]), it is enough to prove that $|K| \leq \mathrm{Dim}_K K^I$. Let $\sigma : \mathbb{N} \to I$ be injective and for $a \in K$, let g_a denote the I–tuple with $(g_a)_{\sigma(\nu)} := a^{\nu}$ for $\nu \in \mathbb{N}$ and $(g_a)_i := 0$ for $i \in I \setminus \mathrm{im}\,\sigma$. Then by Exercise 2.12, $(g_a)_{a\in K}$ are linearly independent.) Deduce that $\mathrm{Dim}_K K^I > \mathrm{Dim}_K K^{(I)}$. – **Remark:** This dimension formula for K^I is also valid for division rings K. Proof!.)

2.14. Let K be a division ring. Further, let $x_i = (a_{i1}, \ldots, a_{in}) \in K^n$, $i = 1, \ldots, n$. With the j–th components of this n–tuple we form the new n–tuples $y_j := (a_{1j}, \ldots, a_{nj})$, $j = 1, \ldots, n$. Show that : the elements $x_1, \ldots, x_n$ of the K–*Left*-vector space K^n are linearly independent if and only if the elements $y_1, \ldots, y_n$ of the K–*right*-vector space K^n are linearly independent. (**Hint:** Suppose that $x_1, \ldots, x_n$ are linearly independent and $y_1b_1 + \cdots + y_nb_n = 0$, $b_j \in K$. Then $x_1, \ldots, x_n \in \mathrm{Rel}_K(b_1, \ldots, b_n)$, and a dimension argument shows that $\mathrm{Rel}_K(b_1, \ldots, b_n) = K^n$, this means $b_1 = \cdots = b_n = 0$.)

2.15. Let K be a division ring, I be a set and let $f_1, \ldots, f_n \in K^I$, $n \in \mathbb{N}$. The following statements are equivalent:

(i) The $f_1, \ldots, f_n$ are linearly independent over K.
(ii) There exists a subset $J \subseteq I$ such that $|J| = n$ and that the restrictions $f_1|J, \ldots, f_n|J \in K^J$ are linearly independent (and hence form a basis of K^J).

---

[7]) A function $f : I \to \mathbb{R}$ is called real-analytic at $a \in I$, if there exist a open neighbourhood U of a and a convergent power series $\sum_{i=0}^{\infty} a_i(x-a)^i$ such that $f(x) = \sum_{i=0}^{\infty} a_i(x-a)^i$ for all $x \in U \cap I$. A function $f : I \to \mathbb{R}$ is called real-analytic if it is real-analytic at every $a \in I$.

[8]) Let A be a ring and let V be a free A–module of infinite rank. Then $|V| = |A| \cdot \mathrm{rank}_A V = \mathrm{Sup}\{|A|, \mathrm{rank}_A V\}$.

(iii) The value $-n-$tuples $(f_1(i),\ldots,f_n(i))\in K^n$, $i\in I$, generate K^n as a K–*right*-vector space.

(**Hint:** The implication (i) $\Rightarrow$ (ii) can be proved by induction on n: Suppose that there exists a subset $J'\subseteq I$ with $(n-1)$–elements is found for $f_1,\ldots,f_{n-1}$ such that $f_1|J',\ldots,f_{n-1}|J'$ are linearly independent over K and so form a basis of $K^{J'}$. Then $f_n|J'=a_1(f_1|J')+\cdots+a_{n-1}(f_{n-1}|J')$ with $a_1,\ldots,a_{n-1}\in K$. Now, by (i) there exists an element $j\in I\smallsetminus J'$ such that $f_n(j)\neq a_1f_1(j)+\cdots+a_{n-1}f_{n-1}(j)$. Now, choose $J:=J'\cup\{j\}$. — For the equivalence (ii) $\Leftrightarrow$ (iii) use the Exercise 2.15.)

2.16. Let K be a division ring and let $a_1,\ldots,a_n\in K$. Let $g_i:=(a_i^\nu)_{\nu\in\mathbb{N}}\in K^{\mathbb{N}}$ and $f_i:=(1,a_i,\ldots,a_i^{n-1})\in K^n$, $i=1,\ldots,n$. Then $g_1,\ldots,g_n$ are linearly independent over K if and only if $f_1,\ldots,f_n$ are linearly independent over K. (**Hint:** Let $h_j:=(a_1^j,\ldots,a_n^j)\in K^n$, $j\in\mathbb{N}$. Note that $f_i=g_i|\{0,\ldots,n-1\}$ and $(f_1(j),\ldots,f_n(j))=(g_1(j),\ldots,g_n(j))=h_j$ for all $j=1,\ldots,n$. Therefore by Exercise 2.17, $g_1,\ldots,g_n$ are linearly independent if and only if h_j, $j=1,\ldots,n$ generates the *right*-vector space K^n. Suppose that the elements $h_0,\ldots h_m$ are linearly independent in the K–*right*-vector space K^n, but the elements $h_0,\ldots,h_{m+1}$ are not linearly independent, so h_{m+1} and hence h_j for every $j\geq m+1$ is a linear combination of $h_0,\ldots,h_m$. Now again use the Exercise 2.15.)

2.17. 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 atmost m distinct elements $x\in K$, which satisfy the equation

$$0=b_0\cdot 1+b_1x+\cdots+b_mx^m\,.$$

(**Hint:** If $x_1,\ldots,x_{m+1}$ are distinct elements in K, then by Exercise 2.12 and Exercise 2.16, the elements $h_j:=(x_1^j,\ldots,x_{m+1}^j)$, $0\leq j\leq m$, 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 atmost m zeros in K.*)

2.18. 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 e x p o n e n t[9]) $m\neq 0$. 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 atmost m solutions in A by Exercise 2.17. 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* Ord$G$ *there are atmost d elements $x\in G$ such that $x^d=e$. Then G is a cyclic group.*))

2.19. A non-zero ring A is called i r r e d u c i b l e or c o n n e c t e d if it is not iosmorphic to a direct product of two non-zero rings. For example, Integral domains are ireducible rings.

a). For a non-zero ring A, the following statements are equivalent: (i) A is irreducible. (ii) there are no non- unit comaximal ideals $\mathfrak{a}$ and $\mathfrak{b}$ in A with $\mathfrak{a}\cap\mathfrak{b}=0$. (iii) The only idempotents in A are 0 and 1. (**Hint:** If $e\in A$ is idempotent, then $1-e$ is also idempotent in A and $1=e+(1-e)$, $e(1-e)=0$.)

b). The characteristic of an irreducible ring is 0 or a power of a prime number. The number of elements in a finite irreducible ring is a power of a prime number.

---

[9]) **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 e x p o n e n t o f G and usually denoted by Exp G. For example, if G is a finite cyclic group, then Exp $G=$ Ord G; Exp $\mathfrak{S}_3=$ Ord $\mathfrak{S}_3$; In general: Exp G *and* Ord G *have the same prime divisors.* (proof!).

c). Let I be a finite set and let A be an irreducible ring. Show that: 1) The canonical projections $\pi_i : A^I \to A$, $i \in I$ are the only A–algebra homomorphisms $A^I \to A$. 2) The map $\mathfrak{S}(I) \to \mathrm{Aut}_{A-\mathrm{alg}}\, A^I$ defined by $\sigma \mapsto (a_{\sigma^{-1}(i)})$ is an isomorphism of groups.

d). 1) For $n \in \mathbb{N}$, show that the canonical projections $\pi_i : \mathbb{Z}^n \to \mathbb{Z}$, $i = 1, \ldots, n$ are the only ring homomorphisms $\mathbb{Z}^n \to \mathbb{Z}$. 2) The projections $\pi_i : Z^{\mathbb{N}} \to \mathbb{Z}$, $i \in \mathbb{N}$ are the only ring homomorphisms $\mathbb{Z}^{\mathbb{N}} \to \mathbb{Z}$. 3) Compute the automorphism groups of the rings $\mathbb{Z}^n$, $n \in \mathbb{N}$ and $\mathbb{Z}^{\mathbb{N}}$.

2.20. Let $f : V \to W$ be an A–module homomorphism of modules over a ring A and for $\mathfrak{m} \in \mathrm{Max}\,(A)$, let $f_{\mathfrak{m}} : V/\mathfrak{m}V \to W/\mathfrak{m}W$, $\overline{x} \mapsto \overline{f(x)}$, be the $A/\mathfrak{m}$–homomorphism induced by f.

a). Suppose that $\mathrm{Im}\, f$ is a co-finite A–submodule of W and $f_{\mathfrak{m}}$ is surjective for every $\mathfrak{m} \in \mathrm{Max}\,(A)$, then f is also surjective.

b). Let V be a finite A–module and let $f \in \mathrm{End}_A(V)$. Then the following statements are equivalent: (i) f is bijective. (ii) $f_{\mathfrak{m}}$ is bijective for every $\mathfrak{m} \in \mathrm{Max}\,(A)$. (iii) $f_{\mathfrak{m}}$ is injective for every $\mathfrak{m} \in \mathrm{Max}\,(A)$. (iv) $f_{\mathfrak{m}}$ is surjective for every $\mathfrak{m} \in \mathrm{Max}\,(A)$.

Below one can see (simple) test-exercises which are meant to test the basic concepts and definitions.

Test-Exercises

T2.1. Let V be an A-module and let $a \in A$ be a unit. Then the homothecy $\vartheta_a : V \to V \;\; x \mapsto ax$ is bijective. Give an example of a non-zero A-module and a non-unit $a \in A$ such that the homothecy ϑ_a is bijective. (**Hint:** Consider $\mathbb{Z}$-modules.)

T2.2. Let U, W, U', W' be submodules of an A–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 $U + (W \cap W')$.

T2.3. Let A be a ring and let V_i, $i \in I$, be an infinite family of non-zero A–modules. Prove that $W := \bigoplus_{i \in I} V_i$ is not a finite A–module.

T2.4. Let K be a field and let A be a subring of K such that every element of K can be expressed as a quotient a/b with $a, b \in A$, $b \neq 0$. (i.e. K is the quotient field of A). If K is a finite A–module, then prove that $A = K$. In particular, $\mathbb{Q}$ is not a finite $\mathbb{Z}$–module. (**Hint:** Suppose $K = Ax_1 + \cdots + Ax_n$ and $b \in A$, $b \neq 0$, with $bx_i \in A$ for $i = 1, \ldots, n$. Now, try to express $1/b^2$ as a linear combination of x_i, $i = 1, \ldots, n$.)

T2.5. Let A be an integral domain. Then:

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

b). $\mathrm{Hom}_A(K, A) \neq 0$ if and only if $A = K$. In particular, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = 0$. (**Hint:** Every element $f \in \mathrm{Hom}_A(K, A)$ is a homothecy of K by the element $f(1)$.)If K is finite module, then $A = K$. (**Remark:** If K is a A–submodule of a arbitrary direct sum of finite A–modules, then $A = K$.)

T2.6. Let K be a field and let V be a K–vector space. Suppose that $V_1, \ldots, V_n$ be distinct K-subspaces of V. If K has at least n elements (in particular, if K is infinite), then $V_1 \cup \cdots \cup V_n \neq V$. (**Hint:** Induction on n. By induction we may assume that $V_n \not\subseteq V_1 \cup \cdots \cup V_{n-1}$. Then there exist an elements $x \in V_n$, $x \notin V_1 \cup \cdots \cup V_{n-1}$ and $y \in V$, $y \notin V_n$. Now, consider the linear combinations $ax + y$, $a \in K$.)

T2.7. a). An element a in the ring A is a basis of the A–module A, if and only if a is a unit in A.

b). The elements $1,\ a \in \mathbb{R}$ are linearly independent over $\mathbb{Q}$, if and only if a is irrational (i.e. not rational). (**Remark:** Two real numbers b, c, which are linearly independent over $\mathbb{Q}$ are called *incommensurable*. Classical example: the length of the side and the length of the diagonal of a square are incommensurable, since the real number $\sqrt{2} \in \mathbb{R}$ is irrational.)

c). Let $\mathbb{P}$ be the set of all prime numbers $p \in \mathbb{N}^*$. Show that the family $(\log p)_{p \in \mathbb{P}}$ is linearly independent over $\mathbb{Q}$.

d). Let $a, b \in \mathbb{N}^*$ and $d := \gcd(a, b)$. Then the relation submodule $\mathrm{Rel}_{\mathbb{Z}}(a, b)$ of $\mathbb{Z}^2$ is generated by $(bd^{-1}, -ad^{-1}) \in \mathbb{Z}^2$.

e). In the subspace U of the $\mathbb{R}$–vector space $\mathbb{R}^{\mathbb{R}}$ of all funktions from $\mathbb{R}$ into itself, generated by the functions $x \mapsto \sin(x + a),\ a \in \mathbb{R}$, show that the two functions $x \mapsto \sin x,\ x \mapsto \cos x (= \sin(x + \pi/2))$ form a basis of U.

f). Every $\mathbb{Q}$–vector space $V \neq 0$ is not free over the subring $\mathbb{Z}$ of $\mathbb{Q}$.

T2.8. Let K be a division ring and let V be a K– vector space. Then:

a). Let $x_1, \ldots, x_{n+1},\ n \in \mathbb{N}$, be linearly independent elements of V. Suppose that n elements among $x_1, \ldots, x_{n+1}$ are linearly independent over K. Then show that $\mathrm{Dim}_K(\mathrm{Rel}_K(x_1, \ldots, x_{n+1})) = 1$.

b). Suppose that V is finite dimensional over K. If $V_i,\ i \in I$, is a family of subspaces of V, then there exists a finite subset J of I such that $\bigcap_{i \in I} V_i = \bigcap_{i \in J} V_i$ and $\sum_{i \in I} V_i = \sum_{i \in J} V_i$.

c). Suppose that V is not finite generated. Then construct recursively a linearly independent sequence $(x_n)_{n \in \mathbb{N}}$ of elements in V. (**Hint:** Let $x_1, \ldots, x_n,\ x_{n+1},\ n \in \mathbb{N}$, be elements of V. Then $x_i,\ 1 \le i \le n+1$, are linearly independent if and only if x_i with $1 \le i \le n$ are linearly independent and x_{n+1} does not belong to the K– subspace of V generated by $x_1, \ldots, x_n$.)

d). Suppose that V is not finite dimensional K–vector space. Construct an infinite sequences $U_0 \subsetneq U_1 \subsetneq \cdots \subsetneq U_i \subsetneq \cdots$ and $W_0 \supset W_1 \supsetneq \cdots \supsetneq W_i \supsetneq \cdots$ of subspaces of V.

e). Suppose that $x_1, \ldots, x_n$ is a basis of V over K and $y := a_1x_1 + \cdots + a_nx_n$ with $a_i \in K$. Give necessary and sufficient condition on the coeficients $a_1, \ldots, a_n$ such that $x_1 - y, \ldots, x_n - y$ is a basis of V.

T2.9. Let V be a module over a ring A. Then:

a). If V is finite A–module, then every generating system of V contains a finite generating system for V.

b). If Y is an infinite generating system for V, then every generating system $x_i,\ i \in I$ contains a generating system $x_j,\ j \in J,\ J \subseteq I$, with $|J| \le |Y|$.

c). Every basis of a free A–module V is a minimal generating system for V.

d). If V is a free A–module and if V has an infinite basis, then every A–basis of V is infinite. Moreover, any two bases of V have the same cardinality. (**Hint:** Use the parts b) and c).)

e). If V is a free A–module and if V has a finite basis, then every A–basis of V is finite. Moreover, any two bases of V have the same cardinality. (**Hint:** For the first part use the parts a) and c).)

T2.10. (*Minimal generating systems*) A generating system $\mathfrak{X}$ of an A–module V is called *minimal generating system* for V if it is minmial (with respect to the natural inclusion) in the set $\{\mathfrak{Y} \mid \mathfrak{Y} \subseteq$ is a generating system for $V\}$. If V is finite A-module, then $\mu_A(V) := \min\{|\mathfrak{X}| \mid \mathfrak{X} \subseteq V$ is a generating system for $V\}$ is called the minimal number of generators for V. By Exercise T2.10-a) every minimal generating sysytem of a finite A–module is finite. More generally, a generating system $\mathfrak{X} = \{x_i \mid i \in I\}$ of an A– module V is called *minimal* if no proper subset $x_j \mid j \in J\}$, $J \subsetneq I$ generate V. For example, $\{1\}, \{2, 3\}, \{p, q \mid \gcd(p, q) = 1\}$ are minimal generateing systems for the Z–module $\mathbb{Z}$ and $\mu_{\mathbb{Z}}(\mathbb{Z}) = 1$. An arbitrary module need not have a minimal generating system. For example, see Exercise 2.??.

a). Let $f : V \to W$, be an A–module homomorphism of modules over a ring A. If $\ker f$ and $\mathrm{Im}\, f$ are finite A–modules, then V is also a finite A–module and $\mu_A(V) \le \mu(\ker f) + \mu_A(\mathrm{Im}\, f)$.

b). For every natural number $m \ge 1$, give a minimal generating system for the $\mathbb{Z}$–module $\mathbb{Z}$ consisting of m elements.

T2.11. Let I be a non-empty open interval in $\mathbb{R}$ and let $C^0_{\mathbb{R}}(I)$ be the $\mathbb{R}$-vector space of all continuous real-valued functions on I. Show that $|C^0_{\mathbb{R}}(I)| = |\mathbb{R}|$. (**Hint:** The map $C^0_{\mathbb{R}}(I) \to \mathbb{R}^{\mathbb{Q}}$ defined by $f \mapsto f|\mathbb{Q}$ is injective.)

T2.12. Let K be a division ring and let V be a non- zero vector space over K. Let $\mathfrak{G} = (g_i)_{i\in I}$ be a finite system of linear equations in n unknowns in V over K. Use Gauss elimination to show that:

a). If $L(\mathfrak{G}) \neq \emptyset$ and $g \in K^n \times V$ with $g \notin K\mathfrak{G}$, then $L(\mathfrak{G}) \neq L(\mathfrak{G} \cup \{g\})$.

b). Let $\mathfrak{H}$ be another finite system of linear equations in n unknowns in V over K. Suppose that $L(\mathfrak{G}) \neq \emptyset$ and $L(\mathfrak{H}) \neq \emptyset$. Then $L(\mathfrak{G}) = L(\mathfrak{H})$ if and only if $K\mathfrak{G} = K\mathfrak{H}$.

c). Suppose that k be a subfield of K and that $\mathfrak{G}$ is a finite system of linear equations in n unknowns over k and let $L_k(\mathfrak{G})$ denote the solution set in k^n. The system $\mathfrak{G}$ is also a system of linear equations over K and let the solution set of this system in K^n be denoted by $L_K(\mathfrak{G})$. Then $L_k(\mathfrak{G}) = k^n \cap L_K(\mathfrak{G})$ and use Gauss elimination process to prove: 1) $L_k(\mathfrak{G}) \neq \emptyset$ if and only if $L_K(\mathfrak{G}) \neq \emptyset$. 2) If $\mathfrak{G}$ homogeneous, then $L_K(\mathfrak{G}) = K \cdot L_k(\mathfrak{G})$. 3) If $\mathfrak{G}$ homogeneous, then $\mathfrak{G}$ has a non-trivial solution over k if and only if $\mathfrak{G}$ has a non-trivial solution over K.

T2.13. Let L be a division ring and let K be a sub-division ring of L. Further, let V_L be an L–vector space with the L–basis $x_1, \ldots, x_n$ and V be the K–vector space $Kx_1 + \cdots + Kx_n \subseteq V_L$.(For example: $V_L := L^n$; $x_1, \ldots, x_n$ is the standard basis; $V = K^n$.)

a). Show that : $y_1, \ldots, y_m \in V$ are linearly independent over K (resp. form a K–generating system of V resp. form a K–basis of V) if and only if they are linearly independent over L (resp. form a L–generating system of V_L resp. form a L–basis of V_L).

b). Let U be a K–subspace of V. Let U_L denote the L-subspace of V_L generated by U. Show that: $\mathrm{Dim}_K\, U = \mathrm{Dim}_L\, U_L$ and $U = V \cap U_L$. If W is another K–subspace of V, then $U \subseteq W$ (resp. $U = W$) if and only if $U_L \subseteq W_L$ (resp. $U_L = W_L$).

c). Prove the analogous assertions in the case V_L is not finite dimensional (over L).

T2.14. Let K be a field, I be a set and let $g \in K^I$ be a function on I into K, such that the image $\mathrm{im}(g)$ is an infinite subset of K. Then the powers g^ν, $\nu \in \mathbb{N}$ of g are linearly independent over K. (For example from this it follows that: the functions $t \mapsto \cos^\nu t$, $\nu \in \mathbb{N}$, from $\mathbb{R}$ to itself are linearly independent; similarly, the functions $x \mapsto x^\nu$, $\nu \in \mathbb{N}$, from K to itself for an arbitrary infinite field K, are linearly independent.)

T2.15. Let L be a division ring, K be a subdivision ring of L and I be a set. For an arbitrary family $(f_j)_{j\in J}$ of functions $f_j \in K^I$ show that: the f_j, $j \in J$, are linearly independent over K if and only if they are linearly independent over L as a family of functions in L^I. (Use the Exercise 2.17 and and Exercise T2.11(a).)

T2.16. Let A be anon-zero ring and let V be a free A – module of rank ≥ 2. Show that the endomomorphism ring $\mathrm{End}_A(V)$ of V is neither commutative nor an integral domain.

T2.17. Let A be a non-zero ring. Show that the following statements are equivalent:

(i) A is a field (ii) Every A–module is free (iii) Every cyclic A–module is free (iv) The A–module A, is simple.[10])

T2.18. Let V, W be two modules over a ring A.

a). For an A–module homomorphism, the following statements are equivalent: (i) f is surjective. (ii) f maps every generating system of V onto a generating system of W. (iii) f maps at least one generating system of V onto a generating system of W.

b). Suppose that $\mathfrak{X} = \{x_i \mid i \in I\}$ is a generating system of V and $f, g \in \mathrm{Hom}_A(V, W)$. Then $f = g$ if and only if $f(x_i) = g(x_i)$ for every $i \in I$.

c). Suppose that $\mathfrak{X} = \{x_i \mid i \in I\}$ is a family of elements in V and $f \in \mathrm{Hom}_A(V, W)$. Then:

[10]) **Simple Modules**. Let A be a ring and A–module V is called *simple* if 0 and V are the only A-submodules of V.

1) If x_i , $i \in I$ in V are linearly independent over A and if f is injective, then the images $f(x_i)$, $\in i \in I$ in W are also linearly independent over A .

2) If the images $f(x_i)$, $i \in I$ in W are linearly independent over A , then x_i , $i \in I$ in V are linearly independent over A and the restriction of f to the A–submodule of V generated by x_i , $i \in I$ is injective.

d). Suppose that V is a free A–module with basis x_i , $i \in I$ and $f : V \to W$ is an A–module homomorphism into an arbitrary A–module W . Then f is bijective if and only if $f(x_i)$, $i \in I$ is an A-basis of W .

e). Suppose that V is a free A–module with basis x_i , $i \in I$ and W is an arbitrary module. Then for every family y_i , $i \in I$ of elements in W , there exists a unique A-module homomorphism $f : V \to W$, such that $f(x_i) = y_i$ for every $i \in I$.

f). Suppose that V is a free A–module with basis x_i , $i \in I$ and W is an arbitrary module. Then the map $\sigma : \mathrm{Hom}_A(V, W) \to W^I$ defined by $f \mapsto (f(x_i))_{i \in I}$ is an isomorphism of A–modules.

g). Two free A-modules are isomorphic if and only if they have the same ranks. In particular, two vector spaces are isomorphic f and only if they have the same dimension.

T2.19. (Maximal submodules and Co-finite submodules) Let A be a ring and let V be an A–module.

1). Maximal elements (with respect to the natural inclusion) in the set $\mathcal{S}_A(V)$ of all A–submodules of , V are called maximal A–submodules of V . Maximal A– submodules of the A–module A are precisely are maximal ideals in A and by Krull's theorem maximal ideals exists if $A \neq 0$. If $A = 0$ is a zero ring, then the A–module A has no maximal A–submodules.

2). An A– submodule W of V is called co-finite if there exists finitely many elements $x_1, \ldots, x_n \in V$ such that $V = W + (Ax_1 + \cdots + Ax_n)$. Equivalently, the quotient A–module V/W is finitely generated. If W is a finite A–submodule of V , then every A–submodule W' with $W \subseteq W' \subseteq V$ is also co-finite. Every A–submodule of a finite A–module is co-finite. Prove that : *Let W be a co-finite A–submodule of an A–module V with $W \neq V$. Then there exists a maximal A–submodule of V which contain W . In particular, in a finite non-zero A–module V there are maximal A–submodules.* (**Remark :** As a corollary to the above assertion we note that : (Krull's Theorem) *Let A be a ring and let $\mathfrak{a}$ be an ideal in A with $\mathfrak{a} \neq A$. Then there exists a maximal ideal $\mathfrak{m}$ in A with $\mathfrak{a} \subseteq \mathfrak{m}$. In particular, in a non-zero ring $A|$,, there are maximal ideals.*

3). (Krull-Nakayama Lemma) let $\mathfrak{a}$ be an ideal in a ring A with $\mathfrak{a} \subseteq \mathfrak{m}_A (=$ Jacobson radical of , $A)$ and let U be a co-finite A–submodule of an A– module V . If $V = U + \mathfrak{a}V$, then $V = U$.

---

† **Max Noether (1844-1921)** Max Noether was born on 24 Sept 1844 in Mannheim, Baden, Germany and died on 13 Dec 1921 in Erlangen, Germany. Max Noether suffered an attack of polio when he was 14 years old and it left him with a handicap for the rest of his life. He attended the University of Heidelberg from 1865 and obtained a doctorate from there in 1868. After this he lectured at Heidelberg and moved from Heidelberg to a chair at Erlangen where he remained for the rest of his life.

Max Noether was one of the leaders of nineteenth century algebraic geometry. He was influenced by Abel, Riemann, Cayley and Cremona. Following Cremona, Max Noether studied the invariant properties of an algebraic variety under the action of birational transformations. In 1873 he proved an important result on the intersection of two algebraic curves. Nine years later, in 1882, his daughter Emmy Noether was born. Emmy became interested in many similar topics to her father and generalised some of his theorems.

†† **Emmy Amalie Noether (1882-1935)** Emmy Amalie Noether was born on 23 March 1882 in Erlangen, Bavaria, Germany and died on 14 April 1935 in Bryn Mawr, Pennsylvania, USA. Emmy Noether's father Max Noether was a distinguished mathematician and a professor at Erlangen. Her mother was Ida Kaufmann, from a wealthy Cologne family. Both Emmy's parents were of Jewish origin and Emmy was the eldest of their four children, the three younger children being boys.

Emmy Noether attended the Höhere Töchter Schule in Erlangen from 1889 until 1897. She studied German, English, French, arithmetic and was given piano lessons. She loved dancing and looked forward to parties with children of her father's university colleagues. At this stage her aim was to become a language teacher and after further study of English and French she took the examinations of the State of Bavaria and, in 1900, became a certificated teacher of English and French in Bavarian girls schools. However Noether never became a language teacher. Instead she decided to take the difficult route for a woman of that time and study mathematics at university. Women were allowed to study at German universities unofficially and each professor had to give permission for his course. Noether obtained permission to sit in on courses at the University of Erlangen during 1900 to 1902. Then, having taken and passed the matriculation examination in Nürnberg in 1903, she went to the University of Göttingen. During 1903-04 she attended lectures by Blumenthal, Hilbert, Klein and Minkowski.

In 1904 Noether was permitted to matriculate at Erlangen and in 1907 was granted a doctorate after working under Paul Gordan. Hilbert's basis theorem of 1888 had given an existence result for finiteness of invariants in n variables. Gordan , however, took a constructive approach and looked at constructive methods to arrive at the same results. Noether's doctoral thesis followed this constructive approach of Gordan and listed systems of 331 covariant forms. Having completed her doctorate the normal progression to an academic post would have been the habilitation . However this route was not open to women so Noether remained at Erlangen, helping her father who, particularly because of his own disabilities, was grateful for his daughter's help. Noether also worked on her own research, in particular she was influenced by Fischer who had succeeded Gordan in 1911. This influence took Noether towards Hilbert's abstract approach to the subject and away from the constructive approach of Gordan.

Noether's reputation grew quickly as her publications appeared. In 1908 she was elected to the Circolo Matematico di Palermo, then in 1909 she was invited to become a member of the Deutsche Mathematiker Vereinigung and in the same year she was invited to address the annual meeting of the Society in Salzburg. In 1913 she lectured in Vienna.

In 1915 Hilbert and Klein invited Noether to return to Göttingen. They persuaded her to remain at Göttingen while they fought a battle to have her officially on the Faculty. In a long battle with the university authorities to allow Noether to obtain her habilitation there were many setbacks and it was not until 1919 that permission was granted. During this time Hilbert had allowed Noether to lecture by advertising her courses under his own name. For example a course given in the winter semester of 1916-17 appears in the catalogue as: **Mathematical Physics Seminar:** Professor Hilbert, with the assistance of Dr E Noether, Mondays from 4-6, no tuition.

Emmy Noether's first piece of work when she arrived in Göttingen in 1915 is a result in theoretical physics sometimes referred to as Noether's Theorem, which proves a relationship between symmetries in physics and conservation principles. This basic result in the general theory of relativity was praised by Einstein in a letter to Hilbert when he referred to Noether's penetrating mathematical thinking. It was her work in the theory of invariants which led to formulations for several concepts of Einstein's general theory of relativity. At Göttingen, after 1919, Noether moved away from invariant theory to work on ideal theory, producing an abstract theory which helped develop ring theory into a major mathematical topic. Idealtheorie in Ringbereichen (1921) was of fundamental importance in the development of modern algebra. In this paper she gave the decomposition of ideals into intersections of primary ideals in any commutative ring with ascending chain condition. Lasker (the world chess champion) had already proved this result for polynomial rings. In 1924 B L van der Waerden came to Göttingen and spent a year studying with Noether. After returning to Amsterdam van der Waerden wrote his book Moderne Algebra in two volumes. The major part of the second volume consists of Noether's work. From 1927 on Noether collaborated with Helmut Hasse and Richard Brauer in work on non-commutative algebras. In addition to teaching and research, Noether helped edit Mathematische Annalen. Much of her work appears in papers written by colleagues and students, rather than under her own name.

Further recognition of her outstanding mathematical contributions came with invitations to address the International Mathematical Congress at Bologna in 1928 and again at Zurich in 1932. In 1932 she also received, jointly with Artin, the Alfred Ackermann-Teubner Memorial Prize for the Advancement of Mathematical Knowledge. In 1933 her mathematical achievements counted for nothing when the Nazis caused her dismissal from the University of Göttingen because she was Jewish. She accepted a visiting professorship at Bryn Mawr College in the USA and also lectured at the Institute for Advanced Study, Princeton in the USA.

Weyl in his Memorial Address said: *Her significance for algebra cannot be read entirely from her own papers, she had great stimulating power and many of her suggestions took shape only in the works of her pupils and co-workers.*

van der Waerden writes: *For Emmy Noether, relationships among numbers, functions, and operations became transparent, amenable to generalisation, and productive only after they have been dissociated from any particular objects and have been reduced to general conceptual relationships.*