Basic Algebra

4.A. — Continued — Free modules with rank

4.17. 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 T4.6. 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.)

4.18. Let K be a field and let I be an infinite set. Then $\mathrm{Dim}_K(K^I) = |K^I|$. (**Hint:** (In view of[1]), it is enough to prove that $|K| \le \mathrm{Dim}_K K^I$. 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 $i \in I \smallsetminus \mathrm{im}\,\sigma$. Then by exercise 4.17, $(g_a)_{a\in K}$ 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!.)

4.19. 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 $b_1 = \cdots = b_n = 0$.)

4.20. 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).

(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) ⇒ (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 $f_n(j) \ne a_1f_1(j) + \cdots + a_{n-1}f_{n-1}(j)$. Now, choose $J := J' \cup \{j\}$. — For the equivalence (ii) ⇔ (iii) use the exercise 4.19.)

4.21. 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 4.20, $g_1, \ldots, g_n$ 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 $j \ge m+1$ is a linear combination of $h_0, \ldots, h_m$. Now again use the exercise 4.20.)

4.22. 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 exercises 4.17 and 4.21, the elements $h_j := (x_1^j, \ldots, x_{m+1}^j)$, $0 \le j \le m$, 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

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

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.)*

Below one can see (simple) test-exercises.

Test-Exercises

T4.10. Let A be a ring $\neq 0$ with finitely many elements and let V be an A–module with a generating system of n elements, $n \in \mathbb{N}$. Show directly (without using the theorem) that every $n+1$ elements of V are linearly dependent. (**Hint:** Proceed as in the Example given in the class which uses only cardinality argument.)

T4.11. What is the rank of $\mathbb{Q}$ as an abelian group?

T4.12. 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[2]) $m \neq 0$. 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 4.22. Now use [3]).)

T4.13. 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 ovwer 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.)

T4.14. 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 6 and and exercise 4.11(a).)

T4.15. Let A be a ring and let J be an indexed set with cardinality of the continuum. Then there exists a family x_j, $j \in J$, of A–linearly independent 0-1–sequences in $A^{\mathbb{N}}$. (**Hint:** (H. Brenner) Let P be the set of prime numbers. For a subset $R \subseteq \mathrm{P}$, let $\mathrm{N}(R)$ be the set of those positive natural numbers whose prime divisors belong to R, i.e. $\mathrm{N}(R) = \{n \in \mathbb{N}^* \mid \text{ prime divisors of } n \subseteq R\}$. Then the family x_R, $R \in \mathfrak{P}(\mathrm{P})$, is linearly independent, where x_R denote the indicator function of $\mathrm{N}(R)$.)

---

[2]) **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 $\mathrm{Exp}G$. For example, if G is a finite cyclic group, then $\mathrm{Exp}G = \mathrm{Ord}G$; $\mathrm{Exp}\mathfrak{S}_3 = \mathrm{Ord}\mathfrak{S}_3$; In general: Exp$G$ *and* Ord$G$ *have the same prime divisors.* (proof!).

[3]) **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 $\mathrm{Ord}G$ there are atmost d elements $x \in G$ such that $x^d = e$. Then G is a cyclic group.