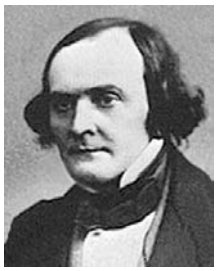
Basic Algebra

5. Algebras, Free Algebras



Arthur Cayley[†]
(1821-1895)

5.1. Let B be an algebra over a field and let $x \in B$.

a). The K–subalgebra $K[x] \subseteq B$ is a finite K–algebra if and only if the system of powers x^ν, $\nu \in \mathbb{N}$, of x is linearly dependent over K. In this case $\mathrm{Dim}_K K[x]$ is the smallest natural number $r \in \mathbb{N}$ such that $x^0, \ldots, x^r$ are linearly dependent over K. We say that x is algebraic over K (of degree r) if $\mathrm{Dim}_K K[x] = r < \infty$. If $K[x]$ is not finite dimensional then we say that x is transcendental over [1]) K. If B is finite dimensional over K, then every element of B is algebraic over K.

b). If x is nilpotent, then the K–subalgebra $K[x] \subseteq B$ is finite and $\mathrm{Dim}_K K[x]$ is the smallest natural number r with $x^r = 0$. (**Hint:** From $x^s + a_1 x^{s+1} + \cdots + a_{r-s-1}x^{r-1} = 0$ with $s < r$ and $a_1, \ldots, a_{r-s-1} \in K$ and so $x^s = 0$.)

c). If x is unipotent, then $K[x]$ finite K–algebra. If s is an integer, which is not a multiple of Char K, then $K[x] = K[x^s]$. (**Hint:** Without loss of generality we may assume that $s > 0$. Then $x = 1 + x'$, x' is nilpotent, and $x^s = 1 + x'e$ with $e \in K[x]^\times$. From $K[x] = K[x']$ and $K[x^s] = K[x'e]$ by using b) deduce that $\mathrm{Dim}_K K[x] = \mathrm{Dim}_K K[x^s]$.)

d). Let x be unipotent and let $y \in B$ be arbitrary. Suppose that $s \in \mathbb{Z}$ is not a multiple of Char K and that y and x^s commute, then y and x commute. (**Hint:** The elements which commute with y form a K–subalgebra of B!)

5.2. a). Let B be an algebra over a field k and let x be an element in B. Further, let $a_1, \ldots, a_n$ be pairwise distinct elements of k such that $x - a_1, \ldots, x - a_n$ are units in B. Show that $(x - a_1)^{-1}, \ldots, (x - a_n)^{-1}$ are linearly independent over k if and only if $1, x, \ldots, x^{n-1}$ are linearly independent over k. (**Hint:** Let $y_i := (x - a_i)^{-1}$ and $y := \prod_{i=1}^n (x - a_i)$. If the y_i are linearly independent, then the yy_i are also linearly independent in $k + k \cdot x + \cdots + k \cdot x^{n-1}$. Conversely, suppose that $1, x, \ldots, x^{n-1}$ are linearly independent and that $b_1 y_1 + \cdots + b_n y_n = 0$ with $b_i \in k$. Multiplying by y and comparing the coefficient of x^{n-1} on both sides we get $b_1 + \cdots + b_n = 0$. Therefore $0 = \sum_{i=1}^n b_i(y_i - y_n) = \sum_{i=1}^{n-1} b_i(a_i - a_n)y_i y_n$. Now use induction.)

b). Let L be a field and let K be a subfield of L. If $x \in L$ is not algebraic over K then show that the set $\{(x - a)^{-1} \mid a \in K\}$ is linearly independent over K. In particular, if K is uncountable then $\mathrm{Dim}_K L$ is uncountable. (**Hint:** Use the part a).)

5.3. Let B be an algebra over a subring A. Further, let M be a subset of B with $B = A[M]$, i.e. M is a set of generators for the A-algebra B. Suppose that either A or M is infinite. Then

---

[1]) In 1873 HERMITE, C. (1822-1901) proved that the real number $e := \sum_{i=0}^\infty \frac{1}{n!}$ is transcendental over $\mathbb{Q}$. This proof was later simplified by HILBERT, D. (1862-1943).

In 1882 LINDEMANN, C. L. F. proved that the real number π is transcendental over $\mathbb{Q}$. This proof is more difficult than that of e. One of the important consequence of this fact is that it is impossible to square the circle by using straightedge and compass only.

$|B| = \mathrm{Sup}\{|A|, |M|\}$. Moreover, if B is finitely generated over A and if A is infinite, then $|B| = |A|$.

5.4. Let L be a division ring and let k be a subdivision ring of L. Further, let M be a subset of L and K be the smallest subdivision ring of L which contain M and k. Suppose that either k or M is infinite. Then $|K| = \mathrm{Sup}\{|k|, |M|\}$. (**Hint :** Consider $A_0 := k[M]$, $M_0 := \{x^{-1} : x \in A_0 \setminus \{0\}\}$, $A_1 := A_0[M_1]$ and so on ...)

5.5. Let I be a set and let K be a field.

a). The K–algebra K^I is cyclic, i.e. $K^I = K[x]$ for some $x \in K^I$ if and only if I is finite and $x : I \to K$ injective. (see also exercise 5.6.)

b). An element $x \in K^I$ algebraic over K (see exercise 5.1a)) if and only if the image $x(I)$ of x is a finite subset of K. Moreover, in this case the degree of x over K is equal to the cardinality $|x(I)|$ of $x(I)$.

5.6. Let I be a finite set, K be a field and let B be a K-subalgebra of the function algebra K^I. Then $B = K^I$ if and only if it separates the elements of I, i.e. if for every pair $i, j \in I$ with $i \neq j$ there exists a function $x : I \to K$ in B such that $x(i) \neq x(j)$. (**Hint :** For a fixed $i \in I$, let $x_j \in B$, $j \neq i$ be the function such that $a_j := x_j(j) \neq x_j(i)$. Then $\prod_{j \in I,\, j \neq i} (x_j - a_j) \in B$ is a function which vanishes on $I \setminus \{i\}$ and $\neq 0$ at i. — Using this exercise give another proof of the exercise 5.5 a).)

5.7. Let I be a finite set, K be a field and let B be a K–subalgebra of the function algebra K^I.

a). Let R_B be a relation on I defined by " $(i, j) \in R_B$ if and only if $f(i) = f(j)$ for all $f \in B$ ". Show that R_B is an equivalence relation on I.

b). The map $B \mapsto R_B$ is a bijective map from the set of subalgebras of K^I onto the set of all equivalence relations on I. (**Hint :** For an equivalence relation R on I, let $B_R := \{f \in K^I \mid f$ is constant on each equivalence class of $R\}$. Then B_R is a K–subalgebra of K^I and the map $R \mapsto B_R$ is the inverse of the map $B \mapsto R_B$.) In paricular, the number of K–subalgebras of K^I is the Bell's number [1] β_n, where $n := |I|$.

5.8. A cyclic algebra B over a field K is a principal ideal ring. (**Hint :** Let $B = K[x]$. Either the powers x^i, $i \in \mathbb{N}$, are linearly independent over K or there exists a natural number $r \in \mathbb{N}$ such that $x^0, \ldots, x^{r-1}$ is a K–basis of B, see exercise 5.1a). If $f = \sum_{i=0}^{m} a_i x^i \in B$ with $a_m \neq 0$ (and $m < r$ in the second case), then m is called the degree of f resp. x. Let $\mathfrak{b}$ be an ideal in B, $\mathfrak{b} \neq 0$, and let $f \in \mathfrak{b}$ be an element $\neq 0$ with minimal degree m. Then the $x^i f$, $i \in \mathbb{N}$, resp. the $x^i f$, $0 \leq i < r - m$, in the second case forms a K–basis of $\mathfrak{b}$. Therefore $\mathfrak{b} = Bf$.) If $\mathrm{Dim}_K B$ is not finite, then B is a principal ideal domain.

5.9. (Boolean functions) Let A be a non-zero Boolean ring and let $K = \{0, 1\} \subseteq A$ be the prime ring of A. Let $n \in \mathbb{N}$. A polynomial function $f : A^n \to A$ is called a Boolean function

---

[1] **Bell's numbers.** (Bell, E. T. (1883-1960)) Let I be a finite set with $\mathrm{card}(I) = n$. The number of equivalence relations on I is called the n-th Bell number and and is denoted by β_n.

a). $\beta_0 = 1$ and $\beta_{n+1} = \sum_{k=0}^{n} \binom{n}{k} \beta_k$ for every $n \in \mathbb{N}$.

b). Let $m, n \in \mathbb{N}$ with $m \leq n$ and let $\beta_{m,n} := \sum_{i=0}^{m} \binom{m}{i} \beta_{n-i}$. Then

i). $\beta_{0,n} = \beta_n$ and $\beta_{0,n+1} = \beta_{n,n}$.

ii). $\beta_{m+1,n+1} = \beta_{m,n} + \beta_{m,n+1}$ for every $m, n \in \mathbb{N}$ with $m \leq n$.

iii). The power series expansion of the analytic function $e^{e^z - 1}$ at 0 is $\displaystyle\sum_{n=0}^{\infty} \beta_n \frac{z^n}{n!}$. In particular, $\displaystyle\beta_n = \frac{1}{e} \sum_{k=0}^{\infty} \frac{k^n}{k!}$.

c). Using the above formulas we have the following table :

n	0	1	2	3	4	5	6	7	8	9	10
β_n	1	1	2	5	15	52	203	877	4140	21147	115975

.

in n variables over A. We want to show that this A–algebra of these functions, is itself a Boolean ring, which is denoted here by $\mathrm{B}_n(A)$. Further, for $1 \leq i \leq n$ the i–th projection $(a_1, \ldots, a_n) \mapsto a_i$ is denoted by $p_i \in \mathrm{B}_n(A)$. Show that : $\mathrm{B}_n(A)$ is a free A–algebra of rank 2^n. The elements $p_H := \prod_{i \in H} p_i$, $H \subseteq \{1, \ldots, n\}$, form an A–(module–) basis of $\mathrm{B}_n(A)$. The map

$$\mathrm{B}_n(A) \to A^{K^n} \quad \text{mit} \quad f \mapsto f|K^n$$

is a bijetive map (and hence an A–algebra–isomorphism). The inverse map

$$g \mapsto \sum_{H \subseteq \{1,\ldots,n\}} b_H p_H \quad \text{mit} \quad b_H := \sum_{F \subseteq H} g(e_F)\,,$$

where for a subseteq $F \subseteq \{1, \ldots, n\}$, $e_F \in K^n$ denote the n–tuple, which has the value at $i \in F$ is 1 and the value at $i \notin F$ is 0. (This is the inverse formula for Boolean functions). The algebra $\mathrm{B}_n(A)$ is equal to the algebra of all A–valued functions on A^n if and only if $A = K$.

5.10. Let K be a field and let A be a K–algebra. For $x \in A$, let $\lambda_x : A \to A$ (respectively $\rho_x : A \to A$) be the left (respectively right) multiplication $y \mapsto xy$ (respectively $(y \mapsto yx)$ by x on A. Then

a). $\lambda_x\,,\ \rho_x \in \mathrm{End}_K(A)$, but $\lambda_x\,,\ \rho_x \notin \mathrm{End}_{K-\mathrm{alg}}(A)$, if $x \neq 1$, i.e., λ_x and ρ_x are not K-algebra endomomorphisms if $x \neq 1$.

b). The map $\lambda : A \to \mathrm{End}_K\, A$ defined by $x \mapsto \lambda_x$ is an injective A–algebra homomorphism.

c). Suppose that A is finite dimensional over K. Then show that the following statements are equivalent :

(i) x is a unit in A. (ii) λ_x is bijective. (iii) ρ_x is bijective. (iv) λ_x is injective.

(v) ρ_x is injective. (vi) λ_x is surjective. (vii) ρ_x is surjective.

(For the equivalence of the (i), (ii) and (iii) the assumption finite dimensional is not necessary.)

d). Suppose that A is finite dimensional over K. Then show that the following statements are equivalent :

(i) A is a division ring.

(ii) λ_x is injective for every $x \neq 0$, i.e. the left cancellation law holds in A.

(iii) ρ_x is injective for every $x \neq 0$, i.e. the right cancellation law holds in A.

Below one can see (simple) test-exercises.

Test-Exercises

T5.1. Let A be a commutative ring and let B be an A–algebra. On $C := B \times B$ the multiplication $(a, x)(b, y) := (ab,\ ay + xb)$ defines an A–algebra strukture such that $V := \{0\} \times B$ is a two sided ideal in C with $V^2 = 0$.

T5.2. Let A be a commutative ring, V be an A–module and let $B := A \times V$ be the idealisation of V.

a). The following statements are equivalent: (i) V is a finite A–module. (ii) B is a finite A–algebra. (iii) B is a finitely generated A–algebra.

b). Let V be a finitely generated A–module and let $W \subseteq V$ be not finitely generated A–submodule of V. Then the idealisation $A \times W$ of W is an A–subalgebra of the finite A–algebra $A \times V$, which is neither finite nor finitely generated.

T5.3. Let K be a finite field with q elements. The polynomial functions $t \mapsto t^i$, $0 \leq i < q$, form a K–basis of all polynomial functions on K into itself. (consider $t^q = t$ for all $t \in K$.) Every function on K into itself is a polynomial function.

T5.4. Let A be an algebra over an infinite field K, which has only finitely many K–subalgebras. Then A is a finite monogene K–algebra and in particular, commutative. (If $A_1, \ldots, A_r$ are all proper subalgebras of A, then every $x \in A \setminus \bigcup_{\varrho=1}^{r} A_\varrho$ is a primitive element of A over K. Such an element x exists! see exercise 3.6.)

T5.5. $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$–algebra.

T5.6. Let A be a commutative ring amd let $B \neq 0$ be a free A–algebra. Let $x_i,\ i \in I$, be an A–basis of B. Then $1_B = \sum_{i\in I}\ a_i x_i,\ a_i \in A$ and $\sum_{i\in I}\ Aa_i = A$. (**Hint :** Let $\mathfrak{a} := \sum_{i\in I}\ Aa_i$. Then $B = 1_B \cdot B \subseteq \mathfrak{a}B$.)

T5.7. Let K be a field. Every K–algebra B with $\mathrm{Dim}_K B \leq 2$ is commutative.

T5.8. Let p be a prime number and let A be a finite ring with p^2 elements. Then A is commutative. (**Hint :** Consider A as an algebra over $\mathbb{Z} \cdot 1_A$.)

T5.9. Let L be a finite dimensional division algebra over a field K with $\mathrm{Dim}_K L = p$ a prime number. Then $K \cdot 1_L$ and L are the only K-subalgebras of L and $L = K[x]$ for all $x \in L \setminus K$. In particular, L is commutative.

T5.10. Let A be a commutative ring and let B be a finite free A–algebra. Further, let I be a set. Then B^I is a finite free algebra over A^I. If $B \neq 0$ and $I \neq \emptyset$, then every free B^I–module has a rank. (**Hint :** If $x_1, \ldots, x_m$ is an A–basis of B, then consider the corresponding coordinate functions $x_i^* : B \to A$ and to every $F \in B^I$ the elements $x_i^* \circ F \in A^I$. — Repeat the footstep in the case $A := \mathbb{R},\ B := \mathbb{C},\ x_1 := 1,\ x_2 := \mathrm{i}$.)

T5.11. Let B be the $\mathbb{C}$–subalgebra $\mathbb{C}[F, \overline{F}]$ of the $\mathbb{C}$–algebra of all complex valued functions on $\mathbb{R}$, generated by the functions $F := \exp(\mathrm{i}t) = \cos t + \mathrm{i}\sin t$ and $\overline{F} = F^{-1} = \cos t - \mathrm{i}\sin t$. Further, let A be the $\mathbb{R}$–algebra $\mathbb{R}[\cos t,\ \sin t]$.

a). The functions $F^n, n \in \mathbb{Z}$, form a $\mathbb{C}$–vector space basis of B. (**Hint :** It is enough to show that the $F^n, n \in \mathbb{Z}$, are linearly independent.)

b). A is the $\mathbb{R}$–algebra of the real valued functions from B. The functions $\cos nt,\ n \in \mathbb{N}$, together with the functions $\sin nt,\ n \in \mathbb{N}^*$, form a $\mathbb{R}$–basis of A and a $\mathbb{C}$–basis of B.

c). The monogene $\mathbb{R}$–algebra $\mathbb{R}[\cos t]$ has the $\mathbb{R}$–vector space basis $\cos^n t,\ n \in \mathbb{N}$, resp. $\cos nt,\ n \in \mathbb{N}$. Deduce that $\sum_{n=0}^{m}\ \mathbb{R}\cos^n t = \sum_{n=0}^{m}\ \mathbb{R}\cos nt$ for all $m \in \mathbb{N}$.

---

† **Arthur Cayley (1821-1895)** Arthur Cayley was born on 16 Aug 1821 in Richmond, Surrey, England and died on 26 Jan 1895 in Cambridge, Cambridgeshire, England. Arthur Cayley's father Henry Cayley, although from a family who had lived for many generations in Yorkshire, England, lived in St Petersburg, Russia. It was in St Petersburg that Arthur spent the first eight years of his childhood before his parents returned to England and settled near London. Arthur showed great skill in numerical calculations at school and, after he moved to King's College School in 1835, his aptitude for advanced mathematics became apparent. His mathematics teacher advised that Arthur be encouraged to pursue his studies in this area rather than follow his father's wishes to enter the family business as merchants.

In 1838 Arthur began his studies at Trinity College, Cambridge from where he graduated in 1842. While still an undergraduate he had three papers published in the newly founded Cambridge Mathematical Journal edited by Duncan Gregory. Cayley graduated as Senior Wrangler and won the first Smith's prize. For four years he taught at Cambridge having won a Fellowship and, during this period, he published 28 papers in the Cambridge Mathematical Journal.

A Cambridge fellowship had a limited tenure so Cayley had to find a profession. He chose law and was admitted to the bar in 1849. He spent 14 years as a lawyer but Cayley, although very skilled in conveyancing (his legal speciality), always considered it as a means to make money so that he could pursue mathematics.

While still training to be a lawyer Cayley went to Dublin to hear Hamilton lecture on quaternions. He sat next to Salmon during these lectures and the two were to exchange mathematical ideas over many years. Another of Cayley's friends was Sylvester who was also in the legal profession. The two both worked at the courts of Lincoln's Inn in London and they discussed deep mathematical questions during their working day. During these 14 years as a lawyer Cayley published about 250 mathematical papers - how many full time mathematicians could compare with the productivity of this 'amateur'?

In 1863 Cayley was appointed Sadleirian professor of Pure Mathematics at Cambridge. This involved a very large decrease in income for Cayley who now had to manage on a salary only a fraction of that which he had earned as a skilled lawyer. However Cayley was very happy to have the chance to devote himself entirely to mathematics. As Sadleirian professor of Pure Mathematics his duties were to explain and teach the principles of pure mathematics and to apply himself to the advancement of that science. Cayley was to more than fulfil these conditions. He published over 900 papers and notes covering nearly every aspect of modern mathematics. The most important of his work is in developing the algebra of matrices, work in non-euclidean geometry and n-dimensional geometry.

As early as 1849 Cayley a paper linking his ideas on permutations with Cauchy's. In 1854 Cayley wrote two papers which are remarkable for the insight they have of abstract groups. At that time the only known groups were permutation groups and even this was a radically new area, yet Cayley defines an abstract group and gives a table to display the group multiplication. He gives the 'Cayley tables' of some special permutation groups but, much more significantly for the introduction of the abstract group concept, he realised that matrices and quaternions were groups.

Cayley developed the theory of algebraic invariance, and his development of n-dimensional geometry has been applied in physics to the study of the space-time continuum. His work on matrices served as a foundation for quantum mechanics, which was developed by Werner Heisenberg in 1925. Cayley also suggested that euclidean and non-euclidean geometry are special types of geometry. He united projective geometry and metrical geometry which is dependent on sizes of angles and lengths of lines.

In 1881 he was invited to give a course of lectures at Johns Hopkins University in the USA, where his friend Sylvester was professor of mathematics. He spent January to May in 1882 at Johns Hopkins University where he lectured on Abelian and Theta Functions.

In 1883 Cayley became President of the British Association for the Advancement of Science. In his presidential address Cayley gave an elementary account of his own views of mathematics. His views of geometry were

It is well known that Euclid's twelfth axiom, even in Playfair's form of it, has been considered as needing demonstration: and that Lobachevsky constructed a perfectly consistent theory, wherein this axiom was assumed not to hold good, or say a system of non-Euclidean plane geometry. My own view is that Euclid's twelfth axiom in Playfair's form of it does not need demonstration, but is part of our experience - the space, that is, which we become acquainted with by experience, but which is the representation lying at the foundation of all external experience. Riemann's view ... is that, having 'in intellectu' a more general notion of space (in fact a notion of non-Euclidean space), we learn by experience that space (the physical space of our experience) is, if not exactly, at least to the highest degree of approximation, Euclidean space. But suppose the physical space of our experience to be thus only approximately Euclidean space, what is the consequence which follows? Not that the propositions of geometry are only approximately true, but that they remain absolutely true in regard to that Euclidean space which has been so long regarded as being the physical space of our experience. Two descriptions of Cayley, both of him as an old man, are interesting. Macfarlane says : ... *I attended a meeting of the Mathematical Society of London. The room was small, and some twelve mathematicians were assembled round a table, among them was Prof. Cayley ... At the close of the meeting Cayley gave me a cordial handshake and referred in the kindest terms to my papers which he had read. He was then about 60 years old, considerably bent, and not filling his clothes. What was most remarkable about him was the active glance of his grey eyes and his peculiar boyish smile.*

Thomas Hirst, one of his friends, wrote: ... *a thin weak-looking individual with a large head and face marked with small-pox: he speaks with difficulty and stutters slightly. He never sits upright on his chair but with his posterior on the very edge he leans one elbow on the seat of the chair and throws the other arm over the back.*