CHAPTER 9

Centralizers of Noncommutative Series and Polynomials

9.0. Introduction

It is a well-known and not too difficult result of combinatorics on words that if two words commute under the concatenation product, then they are both powers of the same word: they have a common *root*. This fact is essentially equivalent to the following one: the centralizer of a nonempty word, that is, the set of words commuting with it, is the set of powers of the shortest root of the given word.

The main results of this chapter are an extension of this latter result to noncommutative series and polynomials: Cohn and Bergman's centralizer theorems. The first asserts that the centralizer of an element of the algebra of noncommutative formal series is isomorphic to an algebra of formal series in one variable. The second is the similar result for noncommutative polynomials. Note that these theorems admit the following consequences: if two noncommutative series (resp. polynomials) commute, then they may both be expressed as a series (resp. a polynomial) in a third one. This formulation stresses the similarity with the result on words given above.

We begin by Cohn's theorem, since it is needed for Bergman's theorem. Its proof requires mainly a divisibility property of noncommutative series. The proof of Bergman's theorem is rather indirect: it uses the noncommutative Euclidean division of Cohn, the difficult result that the centralizer of a noncommutative polynomial is integrally closed in its field of fractions, its embeddability in a one-variable polynomial ring, which uses a pretty argument of combinatorics on words, and finally another result of Cohn characterizing free subalgebras of a one-variable polynomial algebra. The latter result is proved in the Appendix, since it is a result of commutative algebra, and for the sake of completeness, we have proved all the results on valuation rings which are needed for its proof. We have added a section on the defect theorem and free subalgebras: a result of Cohn, together with Bergman's centralizer theorem, shows that the defect theorem holds for two noncommutative polynomials. However, a counterexample of Bergman shows that it does not hold for more than two polynomials: this was proved by Kolotov, and for this, we give his theorem asserting that each free subalgebra of a free associative algebra is an anti-ideal.

9.1. Cohn's centralizer theorem

In all that follows, k will be a field (all fields are assumed to be commutative) and all algebras will be over k. Let X be an *alphabet*, that is, a set of noncommuting variables. We denote by $k\langle\langle X\rangle\rangle$ the algebra of noncommutative formal series in these variables with coefficients in k and by $k\langle X\rangle$ its subalgebra of noncommutative polynomials. We call an element of $k\langle X\rangle$ simply a *polynomial*.

THEOREM 9.1.1 (Cohn). *The centralizer of a nonscalar element in $k\langle\langle X\rangle\rangle$ is isomorphic to $k[[t]]$, for a single variable t.*

The isomorphism will be shown to be continuous, for the X and t-adic topologies. In other words we shall prove that for some series b in the centralizer, with zero constant term, each element in the centralizer has a unique representation of the form $\sum_{n\geq 0}\alpha_n b^n$, with the α_n in k.

Recall Levi's lemma for words over X: if u, v, u', v' are words over X such that $uv' = vu'$ and that u is not shorter than v, then $u = vm, mv' = u'$ for some word m. We need the following lemma, which is the analogue of Levi's lemma for series. Recall the well-known fact that a series is invertible if and only if its constant term is nonzero. As usual, X^* is the free monoid generated by X, and the *length* $|w|$ of a word w is the number of letters appearing in it. In other words, the length of a word is its $X-$degree. If a is a series, we denote it by $a = \sum_{w\in X^*} a_w w$, where a_w is the coefficient of the word w in the series a. Denote by $v(a)$ the *X-adic valuation* of a, that is, the length of the shortest word w such that a_w is nonzero (with $v(a) = \infty$ if $a = 0$). Note that $v(ab) = v(a) + v(b)$.

LEMMA 9.1.2. *If a, b, a', b' are nonzero series such that $ab' = ba'$ and $v(a) \geq v(b)$, then $a = bq$ for some series q.*

Proof. If b' is an invertible series, then the conclusion follows with $q = a'b'^{-1}$.

In the general case, let m be a fixed word of shortest length appearing (with nonzero coefficient) in the series b'. This length is equal to $v(b')$. Since $v(a) + v(b') = v(b) + v(a')$ and $v(a) \geq v(b)$, we have $v(b') \leq v(a')$, hence each word appearing in a' has length at least the length of m.

Now, since $ab' = ba'$, for any word w the two sums $\sum_{uv'=wm} a_u b'_{v'}$ and $\sum_{vu'=wm} b_v a'_{u'}$, over all words u, v', v, u', are equal. We have seen that in order for $b'_{v'} \neq 0$ and $a'_{u'} \neq 0$, the length of v' and u' cannot be smaller than that of m. In this case, the equalities $uv' = wm$ and $vu' = wm$ imply, by Levi's lemma for words, $v' = v_1 m, u' = u_1 m$ and $uv_1 = w, vu_1 = w$. Since in a sum one may disregard vanishing terms, we obtain $\sum_{uv_1=w} a_u b'_{v_1 m} = \sum_{vu_1=w} b_v a'_{u_1 m}$, where the sum is now over all words u, v_1, v, u_1. Define the series B and A by $B_{v_1} = b'_{v_1 m}$ and $A_{u_1} = a'_{u_1 m}$. Then the previous equality shows that $aB = bA$.

Finally, note that the constant term of B is b'_m, hence is nonzero, by the choice of m, and we are done by the beginning of the proof. ∎

Proof of the theorem. Let Z be the centralizer in $k\langle\langle X\rangle\rangle$ of a nonscalar element a. The constant term of a is in k and by subtracting it, we may suppose a to have constant term 0. We claim that if c_1, c_2 are nonzero elements of Z with $v(c_2) \geq v(c_1)$ then $c_2 = c_1 d$ for some $d \in Z$.

The claim being assumed, let b be an element of Z such that $v(b)$ is positive and minimal. We show that each element c in Z has a unique decomposition $c = \sum_{n\geq 0} \alpha_n b^n$, with the α_n in k. This will imply that Z is isomorphic to $k[[t]]$.

Note that uniqueness is clear, since the valuation of $\alpha_m b^m + \alpha_{m+1} b^{m+1} + \cdots$ is, for nonzero α_m, equal to $mv(b)$. In order to prove existence, let $c \in Z$. Then for $\alpha_0 =$ constant term of c, we have $v(c - \alpha_0) > 0$, hence $v(c - \alpha_0) \geq v(b)$, by the minimality of $v(b)$. Suppose that we have found scalars $\alpha_0, \alpha_1, \ldots, \alpha_n$ such that: (*) $v(c - \alpha_0 - \alpha_1 b - \cdots - \alpha_n b^n) \geq (n+1)v(b)$. Since $(n+1)v(b) = v(b^{n+1})$, the series on the left-hand side of (*) is, by the claim, equal to $b^{n+1}d$ for some series $d \in Z$. Now as before we choose a scalar α_{n+1} such that $v(d - \alpha_{n+1}) \geq 0$, hence $v(d - \alpha_{n+1}) \geq v(b)$, and we obtain $c - \alpha_0 - \alpha_1 b - \cdots - \alpha_n b^n - \alpha_{n+1} b^{n+1} = b^{n+1} d - \alpha_{n+1} b^{n+1} = b^{n+1}(d - \alpha_{n+1})$.

Therefore, this series has valuation $\geq (n+2)v(b)$, which concludes the induction step, and Eq.(*) holds for each n.

In Eq.(*), let n tend to ∞. Then we obtain that $c = \sum_{n\geq 0} \alpha_n b^n$, as desired.

It remains to prove the claim. Since a has zero constant term, we have $v(a^n) = nv(a) \geq v(c_2)$ for n large enough. Since c_1, c_2 are in Z, they commute with a, hence with a^n. Thus $a^n c_1 = c_1 a^n$ and $a^n c_2 = c_2 a^n$. From the latter equation and the lemma, we conclude that $a^n = c_2 q$, for some series q. Hence, we have $c_2 q c_1 = c_1 a^n$. Since $v(c_2) \geq v(c_1)$, the lemma implies that $c_2 = c_1 d$. Now $c_1 ad = ac_1 d = ac_2 = c_2 a = c_1 da$, and canceling c_1, we obtain $ad = da$, hence d is in Z. ∎

COROLLARY 9.1.3. *The centralizer of any nonscalar element in $k\langle\langle X\rangle\rangle$ or $k\langle X\rangle$ is commutative.*

This means that if two polynomials (or series) commute with a third nonscalar one, then they commute each with another.

9.2. Euclidean division and principal right ideals

The next result is Cohn's Euclidean division in $k\langle X\rangle$ (a particular case of his *weak algorithm*).

THEOREM 9.2.1. *If a, b, a', b' are polynomials such that $ab' = ba'$ and b, b' are nonzero, then $a = bq + r, deg(r) < deg(b)$ for some unique polynomials q, r.*

Proof. We totally order the free monoid on X in the following way: let $<$ be a fixed order on X and define: $u < v$ if either $\mid u \mid < \mid v \mid$, or $\mid u \mid = \mid v \mid = n$

and $u < v$ in the lexicographic order of X^n (from left to right). In any finite nonempty set of words the greatest element will be called its *leader*. Note that if u (resp. v) is the leader of A (resp.B), then $w = uv$ is the leader of the set AB consisting of all the products u_1v_1, $u_1 \in A$, $v_1 \in B$, and that w has a unique such decomposition. Likewise we call leader of a nonzero polynomial the leader of the words appearing in it. Then in a product of two nonzero polynomials, the leader is the product of the leaders.

Now let $ab' = ba'$. If $deg(a) < deg(b)$, we take $q = 0$, $r = a$ and we are done. Otherwise, let u, v' be the leaders of a, b' and v, u' be the leaders of b, a'. Then we must have have $uv' = vu'$. Since $deg(a) \geq deg(b)$, we have $\mid u \mid \geq \mid v \mid$ and therefore by Levi's lemma for words, $u = vu_1$ for some word u_1.

Hence, for some scalar α, the polynomial $a - \alpha bu_1$ has a smaller leader than a. Now, we have $ab' = ba'$, hence $(a - \alpha bu_1)b' = b(a' - \alpha u_1 b')$, and we conclude by induction that $a - \alpha bu_1 = bq' + r$ for some polynomials q', r with $deg(r) < deg(b)$. Thus $a = b(q' + \alpha u_1) + r$. Uniqueness is proved as in the commutative case. ∎

COROLLARY 9.2.2. *If I is a family of nonzero polynomials such that any two of them always have a nonzero right multiple, then the right ideal $Ik\langle X\rangle$ of $k\langle X\rangle$ is principal.*

Proof. We first prove that if two polynomials a, b have a nonzero right multiple, then the right ideal $ak\langle X\rangle + bk\langle X\rangle$ is principal. Indeed, we may suppose that $deg(a) \geq deg(b)$ and $ab' = ba'$, b, b' nonzero. Then the theorem shows that $a = bq + r$, with $deg(r) < deg(b)$. If $r = 0$, then the previous ideal is $bk\langle X\rangle$, and hence is principal. Otherwise, $rb' = b(a' - qb')$, r and b have a nonzero common right multiple (since r, b' are nonzero), and we conclude by induction that $rk\langle X\rangle + bk\langle X\rangle$ is principal. But since $a = bq + r$, the latter ideal is the same as the previous one, which concludes this part of the proof.

Now suppose that I is finite. We may suppose that it has at least two elements. Let $a \in I$ and $I' = I - \{a\}$. Then by induction, the right ideal $I'k\langle X\rangle$ is principal, equal to $bk\langle X\rangle$ say. We may choose some element c in I'. By hypothesis, a and c have a nonzero common right multiple, hence so have a and b, since $c \in bk\langle X\rangle$. By the first part, the right ideal $ak\langle X\rangle + bk\langle X\rangle$ is principal. But this ideal is equal to $ak\langle X\rangle + I'k\langle X\rangle = Ik\langle X\rangle$, which concludes the second part of the proof.

In the general case, for each nonempty finite subset I' of I, we have $I'k\langle X\rangle = ak\langle X\rangle$, for some nonzero polynomial a. Choose I' and a such that the latter has least possible degree. Then for any b in I, we have by the previous part of the proof, $ak\langle X\rangle + bk\langle X\rangle = I'k\langle X\rangle + bk\langle X\rangle = (I' \cup b)k\langle X\rangle = ck\langle X\rangle$, for some polynomial c. By the minimality of the degree of a, we must have $deg(a) \leq deg(c)$. Since $a \in ck\langle X\rangle$, we conclude that $a = \alpha c$ for some nonzero scalar α. Hence $ak\langle X\rangle$ contains c, hence b, hence any element of I. Thus $ak\langle X\rangle = Ik\langle X\rangle$. ∎

9.3. Integral closure of the centralizer

The next result, due to Bergman, asserts that the centralizer is integrally closed, and is one of the key ingredients in his proof of the centralizer theorem.

THEOREM 9.3.1. *Let Z be the centralizer in $k\langle X\rangle$ of some nonscalar polynomial. Let $\bar{Z}$ be the integral closure of Z in its field of fractions. Then $\bar{Z} = Z$.*

Note that we take for granted that Z is commutative (Corollary 9.1.3). We shall use the following lemma.

LEMMA 9.3.2. *Let r be a polynomial and $R = \{a \in k\langle X\rangle \mid ra \in k\langle X\rangle r\}$. If $a, ab \in R$, with a nonzero, then $b \in R$.*

Note that $k\langle X\rangle r$ is a left ideal of $k\langle X\rangle$, but not a two-sided one in general. We leave to the reader the verification of the following fact (not needed in the proof): R is the largest subring of $k\langle X\rangle$ containing $k\langle X\rangle r$ as a two-sided ideal. This is called the *idealizer* of $k\langle X\rangle r$ in $k\langle X\rangle$.

Proof. We may suppose that r and b are nonzero. Since $a, ab \in R$, we have $ra = a'r$ and $rab = b'r$ for some polynomials a', b'. Hence $a'rb = rab = b'r$. Thus rb and r have a nonzero common left multiple. If we choose such a nonzero multiple of least degree, then it is of the form $crb = dr$ and c, d have no common left factor (otherwise, we may cancel it and lower the degree).

Now let t be a new variable, and $A = k[t], K = k(t)$, respectively the algebras of polynomials and rational functions in t over k. We consider the ring $K\langle X\rangle$ of noncommutative polynomials in X over K and its subring $A\langle X\rangle$. Both have their degree function with respect to X and $A\langle X\rangle$ has also a degree with respect to t. Note that $A\langle X\rangle$ may be thought as the algebra of polynomials in the variable t over the ring of coefficients $k\langle X\rangle$.

We have in $A\langle X\rangle$ the equality $cr(t-b) = (ct-d)r$. Viewing this equality in $K\langle X\rangle$, we obtain by Corollary 9.2.2 (with K replacing k) that $crK\langle X\rangle + (ct-d)K\langle X\rangle$ is a principal right ideal of $K\langle X\rangle$. Let $E \in K\langle X\rangle$ be a generator of this ideal. Then we have $cr = EF$, $ct - d = EG$, for some elements F, G in $K\langle X\rangle$. We claim that E, F, G may be chosen in $A\langle X\rangle$.

Let us assume this for the moment. We view each element of $A\langle X\rangle$ as a polynomial in the variable t over $k\langle X\rangle$. Then the equality $cr = EF$, together with $cr \in k\langle X\rangle$, implies that E is in $k\langle X\rangle$. Moreover, the equality $ct - d = EG$, together with $c, d, E \in k\langle X\rangle$, implies that E divides c and d on the left in $k\langle X\rangle$. Hence $E \in k$, since c, d have no common left factor.

This shows that the ideal $crK\langle X\rangle + (ct-d)K\langle X\rangle$ is equal to $K\langle X\rangle$. Hence we may express 1 as a right linear combination over $K\langle X\rangle$ of cr and $ct - d$. By multiplying by a suitable element ϕ in $k[t]$, we obtain a relation

$$crP + (ct-d)Q = \phi,$$

with P, Q in $A\langle X\rangle$. Viewing again the elements of $A\langle X\rangle$ as polynomials in t over $k\langle X\rangle$, with their t-degree, let p, q be the leading coefficients of P, Q. We may also suppose that the leading coefficient of ϕ is 1, and that ϕ has t-degree n. If the t-degree of P is $m > n$, then Q must be of degree $m-1$ and we have, upon canceling c, $rp + q = 0$. Hence we have $cr(P - pt^m + bpt^{m-1}) + (ct - d)(Q - qt^{m-1}) = crP + (ct-d)Q - crpt^m + crbpt^{m-1} - cqt^m + dqt^{m-1} = \phi$, since $crbp = drp = -dq$. Hence in the relation above we may suppose that P has degree $\leq n$, and consequently Q has degree $\leq n-1$: let q' be the coefficient of t^{n-1} in Q. Looking at the coefficient of t^n in the previous relation, we obtain $crp + cq' = 1$, which implies $c(rp + q') = 1$, and so c is in k, since r, p, q' are in $k\langle X\rangle$.

Finally, we obtain $rb = c^{-1}dr$, which shows that $b \in R$.

It remains to prove the claim. This is very similar to Gauss' lemma for commutative polynomials. Call a nonzero polynomial $P \in A\langle X\rangle$ *primitive* if its coefficients have no nontrivial common divisor in A (A is a unique factorization domain as is $k[t]$). The product of two primitive polynomials is primitive: otherwise, let a be an irreducible common divisor of the coefficients of the product. Then by taking the images of these three polynomials in (A/a), we obtain that this ring has zero-divisors, which is a contradiction. Now, if $P \in K\langle X\rangle$ is nonzero (K is the field of fractions of A), we may write $P = aQ$, where $a \in K$ and $Q \in A\langle X\rangle$ is primitive. This representation is unique up to a unit in A. Choose such a representation for each nonzero P: $P = c(P)P'$, $c(P) \in K$, $P' \in A\langle X\rangle$ primitive. $c(P)$ is called the *content* of P. Then $c(PQ) = c(P)c(Q)$ and $(PQ)' = P'Q'$, up to a unit in A: indeed, $c(P)c(Q)P'Q' = PQ = c(PQ)(PQ)'$, $P'Q'$, $(PQ)'$ are primitive, and we are done by uniqueness up to a unit of the representation .

Coming back to the claim, we had $PK\langle X\rangle + QK\langle X\rangle = EK\langle X\rangle$ for some nonzero polynomials $P, Q \in A\langle X\rangle$, $E \in K\langle X\rangle$. Hence, $P = EF, Q = EG$ with $F, G \in K\langle X\rangle$. Then, with equalities holding up to a unit of A (that is, a nonzero element of k), $P' = E'F'$, $Q' = E'G'$, $P = E'(c(P)F')$, $Q = E'(c(Q)G')$, $EK\langle X\rangle = E'K\langle X\rangle$, and we are done since $E', F', G' \in A\langle X\rangle$, and $c(P), c(Q) \in A$. ∎

Proof of the theorem. We show that if C is a subring of F (the field of fractions of Z), and a finitely generated Z-module, then C is contained in Z. This will imply the theorem, since $\bar{Z}$ is the union of such C.

Since C is a finitely generated sub-Z-module of F, there exists a common denominator for the elements of C, that is a nonzero element z_0 of Z such that $z_0C \subset Z$. Let $I = z_0C$. This is a C-module, since C is a subring of F. It is also an ideal of Z, since C is a Z-module.

The right ideal $Ik\langle X\rangle$ of $k\langle X\rangle$ is principal: indeed, two nonzero elements of I always have a nonzero common right multiple, I being a subset of Z, which is commutative by Corollary 9.1.3, and to this we apply Corollary 9.2.2. Hence $Ik\langle X\rangle = rk\langle X\rangle$, for some $r \in k\langle X\rangle$.

We have $Zr \subset rk\langle X\rangle$. Indeed, $Zr \subset Zrk\langle X\rangle = ZIk\langle X\rangle \subset Ik\langle X\rangle$ (since I is an ideal of Z) $= rk\langle X\rangle$.

Since r is nonzero (indeed $1 \in C$, hence $C \neq 0$), there exists a well-defined function $f_0 : Z \to k\langle X\rangle$ such that $zr = rf_0(z)$ for any z in Z. Note that f_0 is an injective ring homomorphism.

Suppose that $c \in C$, with $c = z_1/z_2$, $z_i \in Z$. Then $rf_0(z_1) = z_1 r \in z_1 rk\langle X\rangle = z_1 Ik\langle X\rangle \subset z_1 CIk\langle X\rangle = z_2 cCIk\langle X\rangle \subset z_2 CIk\langle X\rangle \subset z_2 Ik\langle X\rangle$ (since I is a C-module) $= z_2 rk\langle X\rangle = rf_0(z_2)k\langle X\rangle$.

This shows that $f_0(z_1) \in f_0(z_2)k\langle X\rangle$, and there is a function $f : C \to k\langle X\rangle$ such that: (*) $f_0(z_1) = f_0(z_2)f(c)$, where $c = z_1/z_2$. This function is well-defined, since f_0 is a homomorphism. Furthermore, f extends f_0 (take $z_2 = 1$ in (*)) and f is an injective homomorphism $C \to k\langle X\rangle$: indeed, by (*), $f(c)$ commutes with every element of $f_0(Z)$, since Z is commutative and f_0 is a homomorphism, hence we have:

$$\begin{aligned} f_0(z_1 z_2' + z_1' z_2) &= f_0(z_1)f_0(z_2') + f_0(z_1')f_0(z_2) \\ &= f_0(z_2)f(c)f_0(z_2') + f_0(z_2')f(c')f_0(z_2) \\ &= f_0(z_2)f_0(z_2')(f(c) + f(c')) = f_0(z_2 z_2')(f(c) + f(c')) \,. \end{aligned}$$

Since $c + c' = (z_1 z_2' + z_1' z_2)/(z_2 z_2')$, we deduce that $f(c + c') = f(c) + f(c')$. Similarly, f preserves multiplication.

Let $R = \{a \in k\langle X\rangle \mid ra \in k\langle X\rangle r\}$. Then we know by the above lemma that $a, ab \in R$, with a nonzero, implies $b \in R$. Note that $f_0(z) \in R$. For c as above, and $a = f_0(z_2), b = f(c)$, we have $a \in R$, $ab = f_0(z_1) \in R$, hence $b = f(c) \in R$.

This implies that for each c in C, we may define $g(c) \in k\langle X\rangle$ by the condition $rf(c) = g(c)r$. Then g is an injective homomorphism $C \to k\langle X\rangle$, and for $z \in Z$, we have $zr = rf_0(z) = rf(z) = g(z)r$, which implies that g is the identity on Z. Hence $g : C \to k\langle X\rangle$ extends the identity mapping $Z \to k\langle X\rangle$, and we obtain that $g(C)$ is a commutative subring of $k\langle X\rangle$ containing Z. Since Z is a centralizer, it is necessarily a maximal commutative subring of $k\langle X\rangle$, thus $g(C) = Z$, and thus $C = Z$, for g being injective. ■

9.4. Homomorphisms into $k[t]$

The next result will allow us, still following Bergman, to embed the centralizer into a one variable polynomial algebra.

THEOREM 9.4.1. *Let Z be a finitely generated subalgebra of $k\langle X\rangle$. Then there exists a nontrivial homomorphism $Z \to k[t]$.*

Proof. Let X^+ denote the set $X^* \setminus 1$, the set of nonempty words on X. Denote by X^ω the set of right infinite words on X, order it lexicographically from left to right (where X is totally ordered) and for $u \in X^+$, denote by u^ω the infinite word $uuu\cdots$. For any set M of nonempty words, one has $u^\omega = v^\omega$ for each $u, v \in M$ if and only if the words in M are power of the same word, which is unique if of minimum length.

Let Y be a finite set of polynomials generating the subalgebra Z and let $m \in X^+$ be such that m^ω is the maximum of all u^ω, for all nonempty words u appearing with nonzero coefficient in all elements of Y. Take m of minimum length, and let $M = \{m^n \mid n \geq 0\}$. For each $a = \sum_{u \in X^*} a_u u \in Z$, let

$f(a) = \sum a_u u$, where the sum is over $u \in M$. Then f is a linear mapping from Z into the subalgebra of $k\langle X\rangle$ generated by m, which is isomorphic to a one variable polynomial algebra. We show below that f is an algebra homomorphism, necessarily nontrivial since some element of Y involves a word of the form m^n, $n \geq 1$.

We claim that for each nonempty words u, v such that $u^\omega \leq m^\omega$ and $v^\omega \leq m^\omega$, one has $(uv)^\omega \leq m^\omega$. If moreover, one of the two former inequalities is strict, then the latter is, too. Indeed, either $(uv)^\omega < (vu)^\omega$, and then $(vu)^\omega = v(uv)^\omega < v(vu)^\omega = v^2(uv)^\omega < v^2(vu)^\omega < \cdots < v^\omega$ (by taking the limit), hence $(uv)^\omega < m^\omega$, or $(vu)^\omega < (uv)^\omega$, and then similarly $(uv)^\omega = u(vu)^\omega < u(uv)^\omega < \cdots < u^\omega$, hence $(uv)^\omega < m^\omega$, or $(uv)^\omega = (vu)^\omega$, hence uv, vu are power of the same word and thus equal, so that u, v also are power of the same word, which implies $(uv)^\omega = u^\omega = v^\omega \leq m^\omega$. This ends the proof of the claim.

In order to finish the proof, it is enough to show that f preserves products. This will follow from the fact that $u, v \in M$ implies that $uv \in M$, and from the following fact: if u, v are words appearing in elements of Z, then $uv \in M$ implies that u and v are in M. We may suppose $u, v \neq 1$. Note first that each nonempty word w appearing in an element of Z is a product of elements appearing in Y. Hence, by the claim, $w^\omega \leq m^\omega$. Hence, again by the claim, if $u^\omega < m^\omega$ or if $v^\omega < m^\omega$, then $(uv)^\omega < m^\omega$, hence $uv \notin M$, which contradicts the assumption.

This proves the previous fact. ∎

9.5. Bergman's centralizer theorem

THEOREM 9.5.1. *The centralizer of a nonscalar polynomial is isomorphic to* $k[t]$.

We first prove a lemma.

LEMMA 9.5.2. *The centralizer of a nonscalar polynomial p is a finitely generated subalgebra of $k\langle X\rangle$, and also a finitely generated $k[p]$−module.*

Proof. We show first that if $\bar{p}$ is a nonscalar homogeneous polynomial, then there exists a homogeneous polynomial q such that each homogeneous polynomial commuting with $\bar{p}$ is a scalar multiple of some power of q. Indeed, the centralizer of $\bar{p}$ in $k\langle\langle X\rangle\rangle$ is of the form $k[[s]]$, for some series s with zero constant term (Theorem 9.1.1). Let q be the lowest homogeneous part of s. Now let r be a homogeneous polynomial commuting with $\bar{p}$. Then $r = \sum_{n\geq 0} \alpha_n s^n$, for some scalars α_n. In this sum, the lowest homogeneous part is $\alpha_n q^n$, where n with $\alpha_n \neq 0$ is chosen as small as possible. Thus by homogeneity $r = \alpha_n q^n$, which concludes the first part of the proof.

Now, let p be any nonscalar polynomial, of degree n. Let Z be its centralizer in $k\langle X\rangle$ and denote by $\bar{p}$ the highest homogeneous part of p. By what we have just seen, there exists a homogeneous polynomial q such that each homogeneous polynomial commuting with $\bar{p}$ is a scalar multiple of some power of q.

For $i = 0, \dots, n-1$ such that some element of degree $\equiv i$ mod. n exists in Z, let p_i denote such an element of least degree. If r is in Z, we may find l and i such that r and $p_i p^l$ have the same degree. Both polynomials are in Z, so that their highest homogeneous part commutes with $\bar{p}$, and they are a scalar multiple of some power of q, necessarily of the same power. Hence for some scalar α, $r - \alpha p_i p^l$ is of degree less than that of r, and we conclude by induction that Z is spanned over k by the polynomials $p_i p^l$.

This shows that Z is finitely generated as an algebra, and also a finitely generated $k[p]-$module. ∎

Proof of the theorem. Let Z be the centralizer in $k\langle X\rangle$ of a nonscalar polynomial p. By Corollary 9.1.3, Z is commutative. We know by the lemma that Z is a finitely generated subalgebra of $k\langle X\rangle$. Hence by Theorem 9.4.1, there exists a nontrivial homomorphism $f : Z \to k[t]$, that is, we have $f(Z) \neq k$. Since by the lemma, Z is a finitely generated $k[p]-$ module, it is of transcendence degree 1 over k. Hence f must be injective, otherwise $f(Z)$ would be of transcendence degree 0 over k (since noninjective homomorphisms decrease the transcendence degree) and thus would be equal to k (since no nonscalar polynomial is algebraic over k). We conclude that Z is isomorphic to $f(Z)$.

Now, by Theorem 9.3.1, Z, and hence $f(Z)$, is integrally closed. This implies by Theorem 7.3 in the Appendix that $f(Z)$, and hence Z, is isomorphic to $k[t]$. ∎

9.6. Free subalgebras and the defect theorem

The next result is due to Cohn.

THEOREM 9.6.1. *If a, b are elements of $k\langle\langle X\rangle\rangle$, without constant term, satisfying a nontrivial relation $S(a, b) = 0$ for some noncommutative series S in two variables, then a, b commute.*

Using Bergman's theorem (Theorem 9.5.1), we obtain the following corollary.

COROLLARY 9.6.2. *If P, Q are two polynomials in $k\langle X\rangle$ which do not freely generate a subalgebra of $k\langle X\rangle$, then they lie in a subalgebra of $k\langle X\rangle$ generated by a single polynomial.*

This is the defect theorem for two polynomials. We show below that it does not hold for more than two polynomials. Note that a similar result holds for two series, instead of polynomials (one has to use Cohn's theorem Th.1.1).

Proof. We may suppose that P, Q have zero constant term, and that P is nonscalar. If P, Q do not generate a free subalgebra, then we have $S(P, Q) = 0$ for some nonzero noncommutative polynomial S in two variables. Hence, by Theorem 9.6.1, they commute. Hence Q lies in the centralizer of P and we are done by Theorem 9.5.1, since this centralizer is generated by a single polynomial. ∎

Proof of the theorem. We show the result by contradiction, and induction on $v(ab-ba)$. Suppose that a,b do not commute. Then $a,b \neq 0$. Let $S(u,v)$ be a noncommutative series in two variables u,v, of smallest possible valuation, such that $S(a,b)=0$. Then we may write $S(u,v)=\alpha+uS_u(u,v)+vS_v(u,v)$ and we have the relation $\alpha+ab'+ba'=0$, where $a'=S_u(a,b), b'=S_v(a,b)$ are elements of $k\langle\langle X\rangle\rangle$. Then α must be equal to 0, since a,b have no constant term, and a',b' must be nonzero, by the minimal choice of S. We may apply Lemma 9.1.2: assuming without loss of generality that $v(a)\geq v(b)$, we have $a=bq$ for some series q in $k\langle\langle X\rangle\rangle$. Let $q=\beta+q_1$, where β is the constant term of q. Then $0\neq ab-ba=bqb-bbq=b(qb-bq)=b(q_1b-bq_1)$, so that $v(q_1b-bq_1)<v(ab-ba)$. Moreover, $S(a,b)=0$ implies a similar nontrivial relation for q_1 and b, since $a=\beta b+bq_1$, and gives the desired contradiction.

■

Consider the following example, due to Bergman: $f=xyxz+xy, g=xyx, h=zxyx+yx$. Then one has $fg=xyxzxyx+xyxyx=gh$. Hence f,g,h do not freely generate a subalgebra of $k\langle x,y,z\rangle$. We show that the three polynomials f,g,h do not belong to a free subalgebra generated by two polynomials in $k<x,y,z>$. This will imply that the defect theorem does not hold in general.

First, we need to prove a necessary condition satisfied by free subalgebras. Following Kolotov, we say that a subalgebra A of $k\langle X\rangle$ is an *anti-ideal* if for $a\in k\langle X\rangle$ and any nonzero $b,c\in A$, $ab,ca\in A$ implies $a\in A$. The next result is due to Kolotov.

THEOREM 9.6.3. *If A is a free subalgebra of $k\langle X\rangle$, then it is an anti-ideal.*

Proof. We know by Theorem 9.2.1 that one can perform the Euclidean division of u by v in $k\langle X\rangle$ whenever u,v have a nonzero right multiple in $k\langle X\rangle$. We claim that if u,v are in the free subalgebra A and if they have a nonzero right multiple in A, then the quotient and the remainder are also in A. This being assumed, let $a\in k\langle X\rangle$ and $b,c\in A$ with $b,c\neq 0$ and $ab,ca\in A$. We may suppose that a is nonzero. Since ca and c have the nonzero right multiple cab, and since ca,c,cab,b,ab are all in A, the claim implies that the quotient of the division of ca by c, which is a, is in A.

It remains to prove the claim. Suppose that A is freely generated by a set Y of polynomials in $k\langle X\rangle$, and denote by Deg the degree-function in A with respect to this set Y. Let u,v in A have a nonzero right multiple in A. Then we have by Theorem 9.2.1 applied to $k\langle X\rangle$ and $k\langle Y\rangle$ that $u=vq+r$, $u,v\in k\langle X\rangle$, $deg(r)<deg(v)$ and $u=vQ+R$, $Q,R\in A$, $Deg(R)<Deg(v)$. We prove by induction on $n=Deg(v)$ that $Q=q, R=r$, which will imply the claim. If $n=0$, this is clear. If $R=0$, the result is also clear, since the quotient and remainder of Euclidean division in $k\langle X\rangle$ are unique. Hence we may suppose that $R\neq 0$. We know that $uv'=vu'$ for some nonzero u',v' in A. Thus $(vQ+R)v'=vu'$, which implies $v(u'-Qv')=Rv'$. All the elements involved in this equation are in A, and since $Deg(R)<Deg(v)$, the induction hypothesis implies that $v=Rq'+r'$, with $q',r'\in A$ and $deg(r')<$

$deg(R)$, $Deg(r') < Deg(R)$. Since $Deg(R) < Deg(v)$, q' is not a constant, thus $deg(R) < deg(R) + deg(q') = deg(v)$. This implies by uniqueness of quotient and remainder that $Q = q, R = r$. ∎

We come back to the previous example: suppose that f, g, h lie in a free subalgebra A. Then, since $fg = gh$, the claim in the previous proof shows that $f = gq+r, q, r \in A, deg(r) < deg(g)$. Since evidently $f = gz+xy, deg(xy) = 2 < 3 = deg(g)$, we have by uniqueness that $z, xy \in A$. Furthermore, $g = (xy)x = x(yx), xy, yx = h - zg$ all lie in A, so that $x \in A$, since A is an anti-ideal. For the same reason, $xy, yx \in A$ implies that $y \in A$. Thus A contains x, y, z and is thus equal to $k\langle x, y, z\rangle$, which cannot be generated by two elements (since its commutative image $k[x, y, z]$ has transcendence degree 3).

9.7. Appendix: some commutative algebra

In this section, all rings and fields are commutative, without zero divisors, and all algebras are over the field k. We begin by Lüroth's theorem. Here t is a variable.

THEOREM 9.7.1 (Lüroth). *If F is subfield of $k(t)$ properly containing k, then it is isomorphic to $k(t)$.*

We need a lemma.

LEMMA 9.7.2. *If $u = f(t)/g(t) \in k(t)$ is nonscalar, with f, g relatively prime in $k[t]$, then t is algebraic over $k(u)$, of degree $deg(u) = max(deg(f), deg(g))$.*

Proof. Note that t is a root of the polynomial $f(x) - ug(x)$ in $k(u)[x]$, where x is a new variable. Since this is a nonzero polynomial in x (otherwise u is scalar), we deduce that t is algebraic over $k(u)$. Note that $k(t, x)$ is of transcendence degree 2 over k, so that $k(u, x)$ too. Hence u, x are algebraically independent. If the previous polynomial is not irreducible in $k(u)[x]$, then it may be factorized in $k(u)[x]$, and by Gauss' lemma, also in $k[u, x]$. Since it is linear in u, one factor must be independent of u, which is impossible because f, g are relatively prime. Hence, the polynomial is irreducible, and since its x-degree is $\max(deg(f), deg(g))$, the lemma follows. ∎

Proof of the theorem. There exists $u \in F \setminus k(t)$. By the lemma, t is algebraic over $k(u)$. Hence t is also algebraic over F. Let the minimal polynomial of t over F be

$$\phi(x) = x^n + u_1(t)x^{n-1} + \cdots + u_n(t),$$

where $u_i(t) \in F$. By multiplying the rational fractions $u_i(t)$ by their lowest common denominator, we obtain a polynomial

$$\Phi(x, t) = v_0(t)x^n + v_{n-1}(t)x^{n-1} + \cdots + v_n(t),$$

where the $v_i(t)$ are polynomials without common divisor, and $v_0 \neq 0$. This implies that Φ, considered as element of $k[t][x]$, is primitive. The u_i are not all constant, and we choose j such that $u_j \notin k$. By the lemma, t has degree $m = deg(u_j)$ over $k(u_j)$, while its degree over F is n. Thus $m = [k(t) : k(u_j)] = [k(t) : F][F : k(u_j)] = n[F : k(u_j)]$, and to complete the proof, we need only show that $m = n$, for then $F = k(u_j)$. Write $u_j = a(t)/b(t)$ with relatively prime polynomials a, b. Note that the t-degree of Φ is $\geq deg(a), deg(b)$. We may assume b is monic and we have by the lemma $m = max(deg(a), deg(b))$. The polynomial $a(x) - u_j b(x)$ in $F[x]$ has t as a root, so that it is divisible by $\phi(x)$ in $F[x]$. Hence we obtain $a(x) - u_j(t)b(x) = q(x)\phi(x)$, $q(x) \in F[x]$. Replace $u_j(t)$ in terms of $a(t), b(t)$ and multiply by $b(t)$. Then we obtain

$$a(x)b(t) - a(t)b(x) = Q(x,t)\Phi(x,t), \tag{$*$}$$

where Q is a polynomial in x. Since Φ and $a(x)b(t) - a(t)b(x)$ are polynomials in $k[t][x]$, and the first is primitive, we deduce by Gauss' lemma that Q is also such a polynomial. The polynomial $a(x)b(t) - a(t)b(x)$ has degree m in t, and Φ has degree at least m in t. This implies that Q is independent of t. Suppose that Q depends on x. Then it has a zero, α, in some extension of k. Thus $a(\alpha)b(t) - a(t)b(\alpha) = 0$. If $b(\alpha) = 0$, then $a(\alpha) = 0$, which implies that a, b are both divisible by the minimal polynomial of α over k, and they are not relatively prime. Hence $b(\alpha) \neq 0$. We thus have $u_j(t) = a(t)/b(t) = a(\alpha)/b(\alpha)$, and $u_j(t)$ is algebraic over k, hence t is too and we have a contradiction. This shows that Q is also independent of x. Hence $m = n$ by comparing the x- degree of both sides in (*). ∎

Finally, we shall prove Cohn's result characterizing the free subalgebras of $k[t]$.

THEOREM 9.7.3. *A subalgebra of $k[t]$ is free (and then isomorphic to k or $k[t]$) if and only if it is integrally closed.*

In order to prove the theorem, we need some results of valuation theory. Before that, recall that a *local* ring is a ring R which has a unique maximal ideal M, which is (necessarily) the set of noninvertible elements of R. If S is a commutative integral domain, and P a prime ideal of S, a classical construction in ring theory is the *local ring* at P, which is $S_P = \{a/b \mid a, b \in S, b \notin P\}$ (we view S as a subring of its field of fractions). Then S_P is a local ring, with maximal ideal $PS_P = \{a/b \mid a, b \in S, a \in P, b \notin P\}$. Observe that $PS_P \cap S = P$, since P is prime.

Recall also that a subring R of a field F is a *valuation ring* if for any x in F, either x or x^{-1} is in R.

THEOREM 9.7.4. *a. If R is a valuation subring of the field F, then it is a local ring with maximal ideal $\{x \in R \mid x^{-1} \notin R\}$.*

b. Each proper valuation subalgebra of $k(t)$ is either of the form $R_p = \{f/g \mid f \in k[t], g \in k[t] \setminus pk[t]\}$ for some irreducible polynomial p in $k[t]$, or of the form $D = \{a/b \mid a, b \in k[t], deg(b) \geq deg(a)\}$.

c. (Chevalley) *If R is a subring of a field F and P a prime ideal of R, then there exists a valuation subring S of F such that S contains R and $M \cap R = P$, where M is the maximal ideal of S.*

d. (Krull) *If $F \subset G$ is a field extension, and R a valuation ring of F, then there exists a valuation ring S of G such that $R = S \cap F$.*

e. (Krull) *If a ring is integrally closed, then it is an intersection of valuation subrings of its field of fractions.*

Note that the converse of Part e is also true, but we shall not use it.

Proof. a. It is enough to show that $\{x \in R \mid x = 0 \, or \, x^{-1} \notin R\}$ is an ideal of R. If x, y are in this set and r is in R, then rx is also, otherwise, $r^{-1}x^{-1}$ is in R, which implies that x^{-1} is in R, which is a contradiction. Furthermore, we have either $x^{-1}y \in R$, or $y^{-1}x \in R$, since R is a valuation ring. In the first case, we have $y = xr$ for some $r \in R$, hence $x + y = x(1 + r)$ is in the previous set. The other case is symmetric.

b. Let R be a proper valuation subalgebra of $k(t)$. Suppose first that R contains $k[t]$. If p, q are relatively prime polynomials such that p/q is in R, then $ap + bq = 1$ for some polynomials a, b, and thus $1/q = ap/q + b$ is in R. This implies that if p, q are distinct irreducible polynomials, then at least one of $1/p, 1/q$ is in R: indeed, since R is a valuation subring, either p/q is in R, hence $1/q$ is too, or q/p is, and $1/p$ too. Thus for at most one irreducible polynomial, $1/p$ is not in R. Since $R \neq k(t)$, there is exactly one such p, and $R = R_p$.

Suppose now that R does not contain $k[t]$. Hence R contains $x = 1/t$, thus R contains $k[x]$. By what we have just seen, R is of the form $S = \{a/b \mid a \in k[x], b \in k[x] \setminus qk[x]\}$, for some irreducible polynomial $q(x) \in k[x]$. Now, if $q = x$, it is easy to see that $S = D$, and if $q \neq x$, then $S = R_p$, where $p(t)$ is the reciprocal polynomial of $q(x)$.

c. We may suppose that $P \neq 0$. Let $\mathcal{F}$ denote the family of local subrings S of F, with maximal ideal M, such that S contains R and that $M \cap R = P$. This family is nonempty, since it contains R_P. Indeed R_P contains R, has the unique maximal ideal $M = PR_P$, and $M \cap R = P$, since P is prime.

This family $\mathcal{F}$ is inductive, as the reader may verify. Hence, by Zorn's lemma, there is a maximal element S in this family. We show that S is the required valuation ring. Suppose by contradiction that S is not a valuation subring of F. Then for some x in F, we have $x \notin S, x^{-1} \notin S$. For $S' = S[x]$ or $S' = S[x^{-1}]$, we have $S' \neq S$. Suppose that $S'M \neq S'$, where M denotes the unique maximal ideal of S. Then $S'M$ is contained in some maximal ideal M' of S', and $S'_{M'}$ would be in the family $\mathcal{F}$. Indeed $M'S'_{M'} \cap S = M'S'_{M'} \cap S' \cap S = M' \cap S$ is an ideal of S containing M, hence is equal to M by maximality of M (since $1 \notin M'S'_{M'}$). Thus $M'S'_{M'} \cap R = M'S'_{M'} \cap S \cap R = M \cap R = P$. This contradicts the maximality of S in the family $\mathcal{F}$, and we conclude that $S'M = S'$. This implies that one can write

$$1 = \sum_{0 \leq i \leq m} a_i x^i, \quad 1 = \sum_{0 \leq i \leq n} b_i x^{-i},$$

with a_i, b_i in M. We choose n, m minimal. Then if for example $n \le m$, we have $x^n = \sum_{0\le i\le n} b_i x^{n-i}$, hence $(1-b_0)x^n = \sum_{1\le i\le n} b_i x^{n-i}$. Since $b_0 \in M$, $1-b_0$ is not in M (otherwise $M = S$), it hence is invertible in S (since S is a local ring), and this shows that x^n is a linear combination with coefficients in M of $1, x, \ldots, x^{n-1}$. Hence $x^{n+1}, \ldots, x^m$ may also be written as such a linear combination, and using the first equality above, we would have $1 = \sum_{1\le i\le n-1} c_i x^i$, for c_i in M, which contradicts the minimality of m. This contradiction shows that we cannot have $x, x^{-1} \notin S$, and S must be a valuation ring.

d. Let P be the unique maximal ideal of R. It is a prime ideal, hence we may apply Part c, and obtain that there is a valuation subring S of G, with maximal ideal M, such that S contains R and $P = M \cap R$. Then $S \cap F$ contains R. Suppose that there exists some element x in $S \cap F$ and not in R. Then x^{-1} is in R, and by Part a even in P, hence in M, which contradicts by Part a the fact that x is in S.

e. Let R be integrally closed in its field of fractions F, and let $a \in F \setminus R$. We show that there is valuation subring S of F such that S contains R but not a (this will imply Part e). Note that $a \notin R[a^{-1}]$, otherwise $a = \sum_{0\le i\le n} r_i a^{-i}$, for some r_i in R, which implies $a^{n+1} = \sum_{0\le i\le n} r_i a^{n-i}$, hence a is integral over R, and thus belongs to R, which is a contradiction. Consider the family of subrings S of F such that $R[a^{-1}] \subset S$ and $a \notin S$. This family is nonempty, and is inductive. Hence, by Zorn's lemma, it has a maximal element, S say. We now show that S is a valuation subring of F.

Suppose that $x \in F, x \notin S$. Then S is strictly included in $S[x]$, which implies by maximality of S that $a \in S[x]$. Hence $a = s_0 x^n + \cdots + s_{n-1}x + s_n$, which implies after multiplying by $a^{-1}x^{-n}$ that $x^{-n}(1 - s_n a^{-1}) = s_{n-1}a^{-1}x^{1-n} + \cdots + s_0 a^{-1}$. We claim that S is a local ring. This being assumed for the moment, a^{-1} must be in its unique maximal ideal, hence $1 - s_n a^{-1}$ is invertible in S, which implies that x^{-1} is integral over S. Let S' denote the integral closure of S in F. If S was strictly included in S', then we would have $a \in S'$, by maximality of S. Hence $a^m = t_1 a^{m-1} + \cdots + t_m$, for some t_i in S, and $a = t_1 + \cdots + t_m a^{1-m} \in S$ (since $a^{-1} \in S$), which is a contradiction. Thus $S = S'$, $x^{-1} \in S$ and S is a valuation ring.

It remains to prove the claim. Since $a \notin S$, Sa^{-1} is strictly included in S. Hence for some maximal ideal P of S, one has $Sa^{-1} \subset P$. Then $S \subset S_P$, and $a \notin S_P$ (otherwise $a = b/c$ with $b, c \in S$, $c \notin P$, hence $c = a^{-1}b \in P$, which is a contradiction). Thus, by the maximality of S, we have $S = S_P$ and S is a local ring. ∎

Proof of Theorem 9.7.3. Let R be a free subalgebra of $k[t]$. Since it is free and commutative, it can be only k or isomorphic to $k[t]$. In both cases, it is integrally closed, as is well-known.

Conversely, suppose that R is an integrally closed subalgebra of $k[t]$. We may suppose that R is not equal to k. By Theorem 9.7.4.e, R is an intersection of valuation subalgebras of its field of fractions F. Now, by Theorem 9.7.4.d, each valuation subalgebra of F is of the form $S \cap F$, where S is a valuation subalgebra of $k(t)$. Hence R is the intersection of F with the family of valuation subalgebras of $k(t)$ containing R. These valuation subalgebras are given in Theorem 9.7.4.b: note that, with the notations of this theorem, $k[t] \subset R_p$, which implies that R_p contains R . Hence the only valuation subalgebra which possibly does not contain R is D, the second case of Theorem 9.7.4.b. But surely D cannot contain R, since the intersection of all valuation subalgebras of $k(t)$ is k, and we would have $R = k$, which was excluded. Hence R is the intersection of all valuation subalgebras of F, except $D \cap F$.

Now by Lüroth's theorem (Theorem 9.7.1), $F = k(x)$, for some x in $k(t) \setminus k$. Note that $k[x]$ is the intersection of all valuation subalgebras of $k(x)$, except $E = \{a/b \mid a, b \in k[x], deg_x(a) \leq deg_x(b)\}$ (a consequence of Theorem 9.7.4.b). Also note that x is in all valuation subalgebras of $k(x)$, except E (ibid.). Suppose that x is not in $D \cap F$: since x is in all valuation subalgebras of F except E, we must have $E = D \cap F$, and it implies that $R = k[x]$. If x is in D, then we claim that $y = 1/(x - \alpha) \notin D$, for suitable $\alpha \in k$. Then we have $F = k(y)$, and we conclude as before that $R = k[y]$.

For the claim, note that $x = f/g$, with $deg(f) \leq deg(g)$. For some $\alpha \in k$, $x - \alpha = f'/g$, with $deg(f') < deg(g)$. Then $g/f' \notin D$, which proves the claim and completes the proof. ∎

Notes

Bergman's centralizer theorem was conjectured by Cohn (Cohn 1963, p. 348). For its proof, we have followed the original proof (Bergman 1969), with the help of Cohn 1985. We did not make any real improvement, but hope to give a larger audience to this result and its proof. That is why we have also included in the Appendix all the results of commutative algebra which are needed in order to prove Cohn's characterization of free subalgebras of $k[t]$. For Lüroth's theorem, we have followed Cohn 1991, p.172-174. For valuation ring theory, we have followed Ribenboim 1965. For the proof of Th.3.1, we have followed Melançon 1993, which also gives a computational version of Cohn's weak algorithm. The proof of Lemma 4.2 is due to Cohn. It would be a real challenge to give to the centralizer theorem a proof that would be simpler that the one found by Bergman thirty years ago.

A result of Cohn (Theorem 9.1.1) allows one to deduce the defect theorem for two polynomials from the centralizer theorem. Then a result of Kolotov implies that the defect theorem does not hold in general (he works out an example of three polynomials due to Bergman). His result gives a necessary condition for a subalgebra to be free, which is similar to the condition of *stability*, necessary and sufficient for a submonoid of a free monoid to be free (see Chapter 6). Kolotov's condition is not sufficient in general, although it is in the one-variable case (see Kolotov 1978 and Cohn 1985).

No simple condition characterizing free subalgebras of a free associative algebra is known. It seems likely that there is no such condition, in view of Bergman 1979 (whose title is clear enough, so requires no further comments from the author of these lines).

Note that the centralizer theorem and the defect theorem have analogues in free monoids, free groups and free Lie algebras. See Th.6.2.1, Lyndon and Schupp 1977 (in the free group, it is a consequence of the theory of Nielsen transformations, see especially Prop.1.2.2 and Prop.1.2.5) and Reutenauer 1993 Th.2.2.10. A defect theorem (in the terminology of Lentin) in an algebraic structure is a theorem that asserts that if n elements generate a substructure which is not free, then they lie in some substructure generated by $n-1$ elements. For the free field the centralizer theorem is not known in general, but partial results exist, see Cohn 1985 Section 7.7.8, and Cohn 1978.