ON THE EMBEDDING OF BIRKHOFF-WITT RINGS IN QUOTIENT FIELDS

DOV TAMARI

1. Introduction and general idea. In this note a natural problem arising in connection with so-called Birkhoff-Witt algebras of Lie algebras is solved by a simple enumeration principle. It is shown that the algebra $F[X]$, where F is a commutative field, $X = (x_1, \cdots, x_n)$ a finite set of symbols, $ax = xa$ for $a \in F$, $x \in X$, and

$$[x_i, x_j] \equiv x_i x_j - x_j x_i = \sum_k \begin{bmatrix} i, j \\ k \end{bmatrix} x_k$$

with certain conditions on the

$$\begin{bmatrix} i, j \\ k \end{bmatrix} \in F,$$

is a ring, *regular on both sides*, and therefore embeddable in a field of right or left quotients, as we like, by the well known construction of Ore.

More generally we replace F by a ring R, regular on the right (say), and admit infinite, but *locally finite*, X. It is convenient to suppose

$$\begin{bmatrix} i, j \\ k \end{bmatrix} \in Z(R)$$

(center of R). The ring $R[X]$ need not be an algebra in the narrow sense. For any linear order of X every element of $R[X]$ has at least one *standard form*

$$\sum a_{\cdots n_i \cdots n_j \cdots} \cdots x_i^{n_i} \cdots x_j^{n_j} \cdots \text{ with } x_i < x_j,$$

and $R[X]$ is represented by the set of ordinary ("commutative") polynomials $R(X)$ with the degree theorem

$$\deg PQ = \deg P + \deg Q.$$

This suffices to solve the problem of common multiples. The only tool required is the general nontrivial solvability in R of a system of n right linear homogeneous equations in *more* than n unknowns. Given two polynomials P and Q, the problem of finding a C.R.M., i.e. of finding polynomials S and T such that $PS = QT$, reduces to the solution of a system of right linear homogeneous equations:

the coefficients of S and T are the unknowns, and every term of the C.R.M. determines an equation. One need consider only the "finite" Lie ring $R[\overline{Y}]$ where $\overline{Y}$ is the *commutator closure* of Y, the set of x_i appearing in P and Q. Let r be the unknown degree of the C.R.M.: for any

$$r \geqq c_v m \quad \left(c_v = \frac{1}{1 - 2^{-1/v}}, \ m = \max \ (\deg P, \deg Q), \ v = \operatorname{card} \overline{Y} \right)$$

the number of unknowns becomes greater than that of the equations, i.e. there are always C.R.M.'s of degree r.

This being a general approach without limitations, we can find in this way *all* possible solutions (also those with smaller r if they exist) as long as we dominate the solutions of systems of linear homogeneous equations in R. As a standard polynomial $\not\equiv 0$ might be $= 0$ in $R[X]$, a formally nontrivial solution could be a trivial one in $R[X]$. However, this can not happen if the 0 of $R[X]$ has only one standard form, namely the empty one, or, what is the same, if the representation by standard forms is unique. This is indeed the case of the Birkhoff-Witt algebras.

The theorem on systems of linear homogeneous equations as needed for our purpose is given in an appendix. Several important and well known algorithms are, of course, nothing else than methods of finding a particular solution. We shall give elsewhere other applications of the enumeration principle.

Professor Jacobson informs me that meanwhile C. W. Curtis has solved the problem for so-called *solvable* Lie algebras by a method based on an algorithm, while he himself has solved the case with commutative coefficient fields of characteristic $p \neq 0$ by showing that every element has a multiple in the center.[1]

2. **Polynomial rings.** Let R be a ring of coefficients ("numbers") and $X = \{x_i\}$, $i \in I$, a finite or infinite set of new distinct symbols (letters or "variables"). We postulate: *A number and a letter be always permutable*: $ax = xa$, $a \in R$, $x \in X$. As usual polynomials may be formed, added and multiplied. We note: n_v^d and $N_v^d = \sum_{i=0}^{d} n_v^i$ the number of possible (distinct) terms of a homogeneous, resp. non-homogeneous, polynomial (in standard form) in v letters and of degree d;

$R\{X\}$ the ring of *free* (formal or universal) polynomials with $n_v^d = v^d$;

$R[X]$ the ring of *Lie* polynomials, i.e., a non-commutative poly-

---

[1] The author is much obliged to Professor Jacobson for friendly advice.

nomial ring with *linear* commutators

$$[x_i,\ x_j] \equiv x_i x_j - x_j x_i = \sum_{x_k \in X} \begin{bmatrix} i,\ j \\ k \end{bmatrix} x_k, \qquad \begin{bmatrix} i,\ j \\ k \end{bmatrix} \in Z(R);$$

$R(X)$ the ring of ordinary ("commutative") polynomials with

$$n_v^d = \binom{d + v - 1}{d} = \binom{d + v - 1}{v - 1}$$

and

$$N_v^d = \binom{d + v}{d} = \binom{d + v}{v},$$

i.e., the special $R[X]$ with all

$$\begin{bmatrix} i,\ j \\ k \end{bmatrix} = 0.$$

Note that $R(X)$ is a commutative ring if and only if R is.

3. **Standard forms.** If a linear order of X by its index set I is fixed, a notion of standard form is induced. Evidently every element of $R[X]$ has representatives in $R\{X\}$. But we have also the

PROPOSITION. *Every element of $R[X]$ has a standard form of $R(X)$ of at most equal degree, but (generally) not in the same set of letters, as representant; as inversely every standard form of $R(X)$ is one of $R[X]$ too, $R[X]$ is represented on the standard forms of $R(X)$.*

PROOF.[2] By repeated applications of the substitutions

$$(*) \qquad\qquad x_i x_j \to x_j x_i + \sum \begin{bmatrix} i,\ j \\ k \end{bmatrix} x_k, \qquad\qquad i > j,$$

we do not change the elements of $R[X]$, but will arrive after a finite number of steps at a standard form: this process stops only at a standard form; we show that it must stop after a finite number of steps. For polynomials of degree ≤ 1 there is nothing to prove as they are ipso facto standard. Suppose the proposition proved up to degree $d-1$, and let P^d be a polynomial of degree $d \geq 2$ with at least one monomial M^d of highest degree which is not standard. As a word with inversions must have at least one neighbor inversion, M^d has the form $M^d \equiv aYx_ix_jZ$, $i > j$. Applying the above substitution we get

---

[2] This is essentially the first part of Birkhoff's proof.

$$M^d \to aY\left(x_j x_i + \sum \begin{bmatrix} i,\ j \\ k \end{bmatrix} x_k\right)z$$

$$= aY x_j x_i Z + \sum a\begin{bmatrix} i,\ j \\ k \end{bmatrix} Y x_k\, Z \equiv Q^d,$$

where $Y x_j x_i Z$ is still of degree d, but with one inversion less, while the rest of Q^d is of degree less than d. By the induction hypothesis the proposition is therefore true for M^d with one inversion only, and by an induction on the number of inversions for any M^d. As the number of possible distinct terms M^d of P^d is finite (at most v^d if v is the number of letters really appearing in P^d), we may apply the result simultaneously to all highest terms of P^d which are not standard.

REMARKS. The highest terms are standardized just as in $R(X)$.

Considering only standard forms we have

$$\text{pp. } (PQ) \equiv \text{pp. } (P{\cdot}Q) = (\text{pp. } P){\cdot}(\text{pp. } Q),$$

where pp. means *principal part* (highest homogeneous component), $\equiv$ means *graphically identical*, and $\cdot$ denotes the ordinary multiplication. This proves the degree theorem.

A *proper* Lie ring (i.e. one with unique standardization) has divisors of zero if and only if R has.

For the uniqueness of standard representation it is necessary and sufficient that, besides

$$\begin{bmatrix} i,\ j \\ k \end{bmatrix} \in Z(R),$$

$$\begin{bmatrix} i,\ j \\ k \end{bmatrix} + \begin{bmatrix} j,\ i \\ k \end{bmatrix} = 0$$

(1)

$$\left(\text{if } R \text{ has characteristic 2 add } \begin{bmatrix} i,\ i \\ k \end{bmatrix} = 0\right);$$

$$(2)\ \sum_s \left\{\begin{bmatrix} i,\ j \\ s \end{bmatrix}\begin{bmatrix} s,\ k \\ t \end{bmatrix} + \begin{bmatrix} j,\ k \\ s \end{bmatrix}\begin{bmatrix} s,\ i \\ t \end{bmatrix} + \begin{bmatrix} k,\ i \\ s \end{bmatrix}\begin{bmatrix} s,\ j \\ t \end{bmatrix}\right\} = 0.^3$$

4. Commutator closure and "locally finite."

DEFINITION. A subset Y of X is *commutator closed* if $x_i,\ x_j \in Y$,

$$\begin{bmatrix} i,\ j \\ k \end{bmatrix} \neq 0 \to x_k \in Y.$$

---

[3] Following the method of Birkhoff one proves that the process of "*monotonic descent*" by successive substitutions leads always to the same standard form, which is a *minimal* free polynomial in the *homogeneous quasi-ordering* of the ring $R\{X\}$ generated by the defining relations (*). To prove the uniqueness of standard representation in $R[X]$, Birkhoff's proof requires some additional remarks.

Subsets reduced to one element and the empty set are also closed.

Evidently, X is closed; the intersection of two closed sets is closed; any subset $Y \subset X$ is contained in a uniquely determined smallest closed set, called the closure $\overline{Y}$ of Y; for closed sets, Y, $Y = \overline{Y}$; the closure of $\overline{Y}$ equals $\overline{Y}$; any subset Y determines uniquely a *Lie-subring* $R[\overline{Y}]$.

DEFINITION. If the closure of every finite subset is a finite subset $R[X]$ is *locally finite*. Therefore, if $R[X]$ is locally finite, every finite subset $Y \subset X$ determines a natural number $v = \text{card } \overline{Y}$, the *range* of Y.

Closure can also be defined by recurrence and constructed step by step; in particular, in a locally finite $R[X]$ the range of every finite set of letters can be calculated in a finite number of steps.

5. Formally nontrivial common multiples in $R[X]$. Now let $R[X]$ be locally finite and R a ring in which the fundamental theorem on systems of right linear homogeneous equations holds.

THEOREM. *Any two elements of $R[X]$ have formally nontrivial C.R.M.'s.*

PROOF. Let P^m, Q^n be standard forms of degrees $m \geqq n$ and v the range of the letters appearing in both. We can find a natural number r and two standard forms S^{r-m}, T^{r-n} such that $P^m S^{r-m} \equiv Q^n T^{r-n} \equiv R^r$, i.e. $P^m S^{r-m} - Q^n T^{r-n} \equiv 0$, where R^r is a standard form of degree r. Indeed, the number of unknowns, i.e. of coefficients of S and T, is

$$\binom{v+r-m}{v} + \binom{v+r-n}{v} \geqq 2\binom{v+r-m}{v}.$$

They have to be the solutions of

$$\binom{v+r}{v}$$

right linear homogeneous equations expressing the coefficients obtained by successive multiplication, standardization, and grouping of terms. A sufficient condition for the existence of a solution is therefore

$$\binom{v+r-m}{v} + \binom{v+r-n}{v} > \binom{v+r}{v}.$$

For this it suffices to take, e.g., $r \geqq c_v m \geqq m/(1 - 2^{-1/v})$, c_v being a constant depending on v.

As rough as this estimate may appear, it gives for $v = 1$ exact (best) values: $r + 1 > m + n$, i.e. $r \geqq m + n$, and in particular, for $m = n$, $c_1 = 2$.

Other approximate values are $c_2 \sim 3.4$; $c_3 \sim 4.8$; $c_4 \sim 6.3$.

6. Appendix on one-sided linear homogeneous equations. An equation is a *right* (*left*) one if the unknowns are on the right (left) of the coefficients. *Solution* means nontrivial solution and *solvable* nontrivially solvable in the coefficient ring R. To avoid less useful complications we consider only finite systems and rings R without divisors of zero.

THEOREM. *A necessary and sufficient condition for the (nontrivial) solvability of a system S_n of n right linear homogeneous equations in $n+1$ (or more) unknowns is that R be regular on the right.*

PROOF. Regularity is equivalent to nontrivial solvability for $n = 1$. Suppose the solvability proved for systems S_{n-1}: the first $n-1$ equations of S_n will have solutions with an arbitrary unknown $= 0$. Let U' be one with $u_i' \neq 0$, U'' one with $u_i'' = 0$. Suppose $\sum_k a_{nk} u_k' = c'$ $\neq 0$, $\sum_k a_{nk} u_k'' = c'' \neq 0$ and solve $c'y' + c''y'' = 0$. $U^* = U'y' + U''y''$ solves the system.

REFERENCES

G. Birkhoff, Ann. of Math. vol. 38 (1937) p. 526.
E. Witt, J. Reine Angew. Math. vol. 177 (1937) p. 152.
O. Ore, Ann. of Math. vol. 32 (1931) p. 463.
N. Jacobson, Amer. J. Math. vol. 74 (1952) p. 357.
C. W. Curtis, Bull. Amer. Math. Soc. vol. 58 (1952) p. 562.

INSTITUTE HENRI POINCARÉ, UNIVERSITY OF PARIS