ON A GENERALIZATION OF THE EUCLIDEAN ALGORITHM

By P. M. COHN

Received 25 April 1960

1. *Introduction.* In any valuated ring R, more specifically, a ring with a degree-function $d(a)$ as defined in § 2, the notion of right R-dependence may be defined as follows:

(i) The elements $a_1, \ldots, a_r$ of R are *right R-dependent* if there exist $b_1, \ldots, b_r \in R$ such that

$$d(a_1 b_1) = \ldots = d(a_r b_r) > d(\Sigma a_i b_i).$$

(ii) An element a of R is said to be *right R-dependent* on the elements $a_1, \ldots, a_r$ of R if $a = 0$ or if there exist $c_1, \ldots, c_r \in R$ such that

$$d(a - \Sigma a_i c_i) < d(a), \quad d(a_i c_i) \leqslant d(a) \quad (i = 1, \ldots, r).$$

The usual division algorithm for polynomial rings in a single variable over a field can then be expressed by saying that

(I) *Of any two non-zero elements of R, any one of maximal degree is right R-dependent on the other.*

The following condition is a natural generalization:

(II) *Any element of maximal degree in a right R-dependent set of elements of R is right R-dependent on the rest.*

A condition similar to (II) occurs in the study of free products of skew fields (2). However, the situation there is more complicated, and this makes it desirable to study abstract rings satisfying the condition (II). The present note is devoted to such a study; the results will be applied elsewhere to the free products of skew fields.

Our main result is a characterization of rings satisfying (I) (Theorem 2·1) or (II) (Theorems 3·4, 3·5). Of course such a characterization will depend on the definition of degree which is used. A fairly natural definition in this context—which, however, excludes the rings of algebraic integers possessing a division algorithm—is given in § 2 and using it we find that the rings satisfying (I) are just the non-commutative polynomial rings in a single variable over a skew field which were first generally defined by Ore (6). In § 3 we show that rings satisfying (II) are characterized by the fact that their elements have a certain normal form, somewhat like the normal form for elements in a free associative algebra. In fact we shall see that free associative algebras may themselves be characterized in terms of a generalized algorithm of the form (II) (Theorem 3·6). On the other hand, free commutative and associative rings, i.e. polynomial rings, in more than one variable, do not seem to have a place in this scheme.†

The division algorithm is usually applied to compute the highest common (right) factor, by means of the Euclidean algorithm. This means essentially that every right ideal is principal. Similarly, in a ring R with the generalized algorithm (II), every right

† Cf. however, Levi (3).

https://doi.org/10.1017/S0305004100034812 Published online by Cambridge University Press

ideal is free, *qua* R-module (Theorem 3·3) and moreover, (II) may be used to construct a free generating set, much in the same way in which (I) is used to compute the highest common right factor. We also give conditions under which (I) and (II) are equivalent (Theorem 3·1) and show that (II) (though not (I)) is actually left-right symmetric (Theorem 3·2).

A final remark concerns the set of degrees. This must necessarily be a semigroup, and with some mild restriction we find (Theorem 4·1) that the only possible types are the semigroup of a single element and the additive semigroup of non-negative integers. However, it may be of interest to consider wider classes of semigroups and one such class is also briefly indicated in § 4.

2. *Rings with a Euclidean algorithm.* Throughout this note, the term 'ring' means 'associative ring different from zero' and the term 'field' will be used in the sense of 'skew field', i.e. 'not necessarily commutative division ring'.

In order to give a meaning to the Euclidean algorithm we have to define the degree of an element. We shall say that a ring R has a *degree-function* if to each element a of R a degree $d(a)$ is assigned such that

D. 1 *for any* $a \neq 0$ *in* R, $d(a)$ *is a non-negative integer, and* $d(0) = -\infty$,

D. 2 $d(a-b) \leqslant \max(d(a), d(b))$,

D. 3 $d(ab) = d(a)+d(b)$.

Thus $d(a)$ is more than a filtration and less than a grading, in fact it just corresponds to a discrete rank one valuation on fields. By D. 2 we have, as for valuations (cf. Schilling (7), p. 9)

$$d(a) = d(-a) \tag{1}$$

and

$$d(a+b) \leqslant \max(d(a), d(b)), \tag{2}$$

with equality holding if $d(a) \neq d(b)$. From D. 1 and D. 3 it follows that the non-zero elements of R form a multiplicatively closed subset, i.e. R has no zero-divisors other than zero.

A ring R with a degree-function $d(a)$ is said to have a *division algorithm*, if the following condition holds in R:

E. 1 *Given* $a, b \in R$ *such that* $d(a) \geqslant d(b) \geqslant 0$, *there exists* $c \in R$ *such that*

$$d(a-bc) < d(a).$$

In a ring R satisfying this condition, let $a, b \in R$ and $b \neq 0$. If $q \in R$ is such that $d(a-bq)$ has its least value, then

$$d(a-bq) < d(b). \tag{3}$$

For if not, i.e. if $d(a-bq) \geqslant d(b)$, then by E. 1, there exists $c \in R$ such that

$$d(a-b(q+c)) < d(a-bq),$$

and this would contradict the definition of q. Hence, putting $r = a-bq$, we have

$$a = bq+r, \quad d(r) < d(b), \tag{4}$$

which is the more usual form of the division algorithm.

https://doi.org/10.1017/S0305004100034812 Published online by Cambridge University Press

Let R again be a ring with a degree-function satisfying E. 1. If a, b, c are as in E. 1, it follows by (1), (2) and E. 1, that

$$d(bc) \leqslant \max(d(a-bc), d(a)) = d(a).$$

Hence E. 1 is equivalent to saying that for any $a, b \in R$ such that $d(a) \geqslant d(b) \geqslant 0$, a is right R-dependent on b. Thus E. 1 is also equivalent to the condition (I) of § 1.

Let k be any field and σ an endomorphism of k. Then a *σ-derivation* of k is a mapping $\alpha \to \alpha'$ of k into itself such that

$$(\alpha+\beta)' = \alpha' + \beta', \tag{5}$$

$$(\alpha\beta)' = \alpha'\beta^\sigma + \alpha\beta' \tag{6}$$

(where $\alpha, \beta \in k$). If σ is the identity mapping on k, the σ-derivations are just the usual derivations in k.

Given a field k, an endomorphism σ and a σ-derivation D of k, we denote by $k[x; \sigma, D]$ the ring of polynomials over k in a single indeterminate x subject to the rule

$$\alpha x = x\alpha^\sigma + \alpha D \quad (\alpha \in k). \tag{7}$$

Every element of this ring can be written uniquely in the form

$$\Sigma x^\nu \alpha_\nu \quad (\alpha_\nu \in k, \text{ almost all } \alpha_\nu \text{ are zero}), \tag{8}$$

and the multiplication is completely determined by (7). This ring has been described by Ore (6), who showed that with the natural definition of degree the ring $k[x; \sigma, D]$ satisfies the division algorithm E. 1. In Theorem 2·1 below we generalize this result and establish the converse.

THEOREM 2·1. *Let R be a ring with a degree-function for which the division algorithm* (E. 1) *holds. Then the elements of non-positive degree form a field k, and R is either k or of the form $k[x; \sigma, D]$.*

Conversely, a ring of the form k or $k[x; \sigma, D]$, with any degree-function for which $d(x)$ is positive, satisfies the division algorithm.

Proof. Suppose that R is a ring with a degree-function satisfying E. 1, and let a be a non-zero element of least degree in R. By E. 1, $d(a-ae) < d(a)$ for some $e \in R$; since $d(a)$ is minimal, we have $a = ae$, and by D. 3, $d(e) = 0$. Thus R contains elements of degree zero. We denote by k the set of elements of R of non-positive degree, so that k contains the element e just found, which is different from zero. Now $a = ae = ae^2$, and hence

$$e^2 = e,$$

because R has no zero-divisors $\neq 0$. Hence for any $b \in R$,

$$(be-b)e = e(eb-b) = 0, \quad \text{i.e.} \quad be = eb = b.$$

Thus e is the unit-element of R; henceforth we denote this unit-element by 1. Now it follows from D. 2 and D. 3 that k is a subring of R which contains 1. Moreover, given $a \in k, a \neq 0$, we have, by E. 1,

$$1 = ac \quad (\text{for some } c \in k),$$

and this shows that k is a field (McCoy (4), p. 19).

https://doi.org/10.1017/S0305004100034812 Published online by Cambridge University Press

If R contains no elements of positive degree, then $R = k$ and the result follows. Otherwise we take an element, x say, of least positive degree in R and assert that every element of R is of the form (8). For if this is not so, let b be an element of least degree which is not of the form (8). By (3) there exists $q \in R$ such that $d(b - xq) < d(x)$. By the definition of x it follows that $b - xq \in k$; thus for some $\alpha \in k$ we have

$$b = xq + \alpha \tag{9}$$

and $d(q) < d(x) + d(q) = d(xq) = \max(d(b), d(\alpha)) = d(b)$; therefore, by the choice of b, q must be of the form $q = \Sigma x^{\nu}\alpha_{\nu}$. Inserting this in (9) we obtain

$$b = \Sigma x^{\nu+1}\alpha_{\nu} + \alpha,$$

which contradicts the assumption that b is not of the form (8). The form (8) is unique, for if we had a relation

$$x^n\alpha_n + \ldots + \alpha_0 = 0,$$

say, with $\alpha_n \neq 0$, then

$$d(x^n) = d(x^n\alpha_n) = \max\{d(x^{\nu}\alpha_{\nu}) \mid \nu = 0, \ldots, n-1\},$$

whence

$$n\,d(x) = (n-1)\,d(x),$$

in contradiction with the assumption $d(x) > 0$.

It only remains to derive an equation of the form (7) (which is enough to determine the multiplication in R). For any $\alpha \in k$ we have, by (4),

$$\alpha x = x\alpha_1 + \alpha_2,$$

where $d(\alpha_2) < d(x)$ and $d(\alpha_1) < d(\alpha x) - d(x) = d(\alpha) \leqslant 0$, hence $\alpha_1, \alpha_2 \in k$. Now it is easy to verify that the mapping $\sigma\colon \alpha \to \alpha_1$ is an endomorphism of k and the mapping $D\colon \alpha \to \alpha_2$ is a σ-derivation (cf. also Ore (6)). Thus $R = k[x; \sigma, D]$ and the first part of the theorem is established.

To prove the converse we consider for a moment any ring R with unit-element 1, which has a degree-function. Any invertible element of R must have degree zero, for if $ab = 1$, then

$$d(a) + d(b) = d(ab) = d(1) = 0,$$

and hence $d(a) = d(b) = 0$. In particular, if $R = k$ is a field, every non-zero element is of degree zero and E. 1 is clearly satisfied. If $R = k[x; \sigma, D]$, the argument shows that the non-zero elements of k must have degree zero. By hypothesis, $d(x) = \lambda > 0$, hence the degrees $d(x^n) = n\lambda$ are all different for different n. From the remarks after D. 1, D. 2 and D. 3 it follows that for $\alpha_n \neq 0$,

$$\begin{aligned} d(x^n\alpha_n + \ldots + \alpha_0) &= \max\{d(x^{\nu}\alpha_{\nu})\} \\ &= n\lambda. \end{aligned}$$

Thus all degrees are multiples of λ. We may therefore divide the degrees by λ and so obtain the usual degree-function on $k[x; \lambda, D]$. Now it is easily verified that the division algorithm holds for this degree-function (cf. Ore (6)), hence it also holds for the original degree-function and the proof is complete.

The actual form $k[x; \sigma, D]$ of the ring obtained in Theorem 2·1 still depends on the particular element x of least positive degree which is chosen. It is clear from the proof

https://doi.org/10.1017/S0305004100034812 Published online by Cambridge University Press

that the field k is unique, while x may be replaced by $x\alpha+\beta$ ($\alpha, \beta \in k$, $\alpha \neq 0$), but no other elements. Correspondingly the endomorphism σ is determined up to an inner automorphism of k (induced by α) and D is determined up to an inner derivation (with multiplication by α to account for the change of endomorphism).

3. *Rings with a generalized algorithm.* We now consider rings R with a degree-function for which the following *generalized algorithm* holds:

E. 2. *Given* $a_1, \ldots, a_r, b_1, \ldots, b_r \in R$ *satisfying*

$$d(a_1 b_1) = \ldots = d(a_r b_r) > d(\Sigma a_i b_i), \quad d(a_1) \geqslant d(a_i) \quad (i = 2, \ldots, r),$$

there exist $c_2, \ldots, c_r \in R$ *such that*

$$d(a_1 - \Sigma a_i c_i) < d(a_1), \quad d(a_i c_i) \leqslant d(a_1).$$

We note that condition (II) of § 1 is just a restatement of the generalized algorithm E. 2 in terms of the notion of R-dependence. This terminology will be used in the sequel, with the following extensions. According to the definition of § 1, a right R-dependent set is necessarily finite; moreover, as is easily seen, such a set must consist of more than one element and all its elements are $\neq 0$. A subset S of R is said to be *right R-independent*, if $0 \notin S$ and if S contains no finite right R-dependent subset. An element a of R is said to be *right R-dependent* on a set S if a is right R-dependent on a finite subset of S in the sense of § 1. The terms *left R-dependent* and *left R-independent* are defined analogously.

Any ring R satisfying the division algorithm E. 1 also satisfies the generalized algorithm E. 2. For if E. 1 holds in R, then of any two non-zero elements, one of maximal degree is right R-dependent on the other, hence in any finite set of R-dependent elements (which necessarily consists of more than one element) an element of maximal degree is right R-dependent on any other, so that E. 2 holds in R.

If R is commutative, or more generally, if R satisfies the Ore condition (5) for the existence of a right quotient ring, we have also the converse.

THEOREM 3·1. *Let R be a ring with a degree-function (and hence without zero-divisors) and suppose that any two non-zero elements of R have a common non-zero right multiple. Then the generalized algorithm holds in R if and only if the division algorithm holds.*

Proof. We have just seen that E. 1 implies E. 2; suppose now that R satisfies E. 2. Given any non-zero elements $a, b \in R$, by hypothesis there exist $a', b' \in R$ such that

$$ab' = ba' \neq 0.$$

Hence $d(ab') = d(ba') > d(ab' - ba')$. Further, let $d(a) \geqslant d(b)$ say, then by E. 2, there exists $c \in R$ such that $d(a - bc) < d(a)$, i.e. E. 1 holds, and the proof is complete.

It is well known that the division algorithm E. 1 is not left-right symmetric. For example, the ring $k[x; \sigma, 0]$, where σ is an endomorphism of k onto a proper subfield of k, satisfies the division algorithm for left division (as in (4)), but not for right division. In view of this fact and of Theorem 3·1, it is all the more surprising that the generalized algorithm *is* left-right symmetric. The explanation is of course that the hypothesis of Theorem 3·1 is not symmetric, i.e. a ring which has a right quotient ring need not have a left quotient ring.

https://doi.org/10.1017/S0305004100034812 Published online by Cambridge University Press

THEOREM 3·2. *Let R be a ring with a degree-function, then the following two conditions are equivalent:*

(i) *Any element of maximal degree in a right R-dependent set of elements of R is right R-dependent on the rest.*

(ii) *Any element of maximal degree in a left R-dependent set of elements of R is left R-dependent on the rest.*

Proof. By symmetry it is enough to show that (i) implies (ii). Suppose then that (i) holds and let $b_1, \ldots, b_r$ be a left R-dependent set in which $d(b_1) \geqslant d(b_i)$ $(i = 2, \ldots, r)$; we have to show that b_1 is left R-dependent on $b_2, \ldots, b_r$. Suppose this is false; then for any b_1' of degree at most $d(b_1)$ which is left R-dependent on $b_2, \ldots, b_r$ we have

$$d(b_1 + b_1') = d(b_1). \tag{10}$$

Let $b_1', \ldots, b_s'$ be any elements which are left R-dependent on $b_2, \ldots, b_r$, such that $d(b_i') \leqslant d(b_1)$ $(i = 1, \ldots, s)$ and $b_1 + b_1', b_2', \ldots, b_s'$ are left R-dependent. Such elements certainly exist, since we may take, for example, $s = r$, $b_1' = 0$, $b_i' = b_i$ $(i = 2, \ldots, r)$. Among all choices of $b_1', \ldots, b_s'$ we make one for which s has its least value. By the left R-dependence we have $a_1, \ldots, a_s \in R$ such that

$$d(a_1(b_1 + b_1')) = d(a_2 b_2') = \ldots = d(a_s b_s') > d(a_1 b_1 + \Sigma a_i b_i'). \tag{11}$$

By the hypothesis and (10), we have

$$d(b_i') \leqslant d(b_1) = d(b_1 + b_1'),$$

hence $d(a_1) \leqslant d(a_i)$ $(i = 2, \ldots, s)$ and as in every R-dependence, $s > 1$. Now R satisfies (i) and $d(a_s) \geqslant d(a_1)$, therefore by renumbering $a_2, \ldots, a_s$ and $b_2', \ldots, b_s'$ if necessary to ensure that

$$d(a_s) \geqslant d(a_i) \quad (i = 2, \ldots, s-1),$$

we find that a_s is right R-dependent on $a_1, \ldots, a_{s-1}$, i.e. there exist $c_1, \ldots, c_{s-1} \in R$ such that the element

$$a_s^* = a_s - \Sigma a_i c_i \tag{12}$$

has degree less than $d(a_s)$. By (10), $d(a_1(b_1 + b_1')) = d(a_1 b_1)$, hence by (11) we have

$$d(a_1 b_1 + \Sigma a_i b_i') < d(a_1 b_1),$$

and inserting from (12) we find

$$d(a_1(b_1 + b_1' + c_1 b_s') + \sum_{i=2}^{s-1} a_i(b_i' + c_i b_s')) < d(a_1 b_1). \tag{13}$$

In this inequality, $d(b_1 + b_1' + c_1 b_s') = d(b_1)$, again by (10); thus if we omit from (13) terms of degree less than $d(a_1 b_1)$, the first term will remain but we shall obtain a shorter left R-dependence between $b_1 + b_1' + c_1 b_s'$ and terms which are left R-dependent on $b_2', \ldots, b_s'$, and hence on $b_2, \ldots, b_r$. This contradiction shows that (ii) must hold in R and the theorem is established.

We now apply the generalized algorithm to show that right ideals are free R-modules. This involves the analogue of the Euclidean algorithm, although we shall not have to write this down explicitly. First we require a definition: If k is a field, then by a k-ring we understand a ring R containing k as a unital subring (i.e. such that the

https://doi.org/10.1017/S0305004100034812 Published online by Cambridge University Press

unit-element of k acts as unit-element of R). In case k lies in the centre of R, this is just the usual notion of k-algebra or algebra over k, but in general k need not belong to the centre of R, or even be commutative.

THEOREM 3·3. *Let R be a ring with a degree-function for which the generalized algorithm holds. Then*

(i) *the elements of non-positive degree in R form a field k over which R is a k-ring,*

(ii) *every right ideal of R is free, qua R-module, with a right R-independent generating set,*

(iii) *k is complemented in R by a right ideal.*

The assertions (ii) *and* (iii) *also hold, with 'right' replaced by 'left' throughout (and with 'R-module' replaced by 'left R-module').*

Proof. (i) Let a be a non-zero element of R of least degree. Since $a^2 - a^2 = 0$, there exists $e \in R$ such that

$$d(a - ae) < d(a),$$

and by the choice of a it follows that $a - ae = 0$. Now R has no zero-divisors $\neq 0$, by D. 3, and we conclude as in the proof of Theorem 2·1 that e is the unit-element of R and that the elements of non-positive degree form a subfield k including e. Thus R is a k-ring; we denote its unit-element again by 1.

Next we prove (ii) and (iii). For brevity we shall write 'R-dependent' and 'R-independent' in this part of the proof to mean 'right R-dependent' and 'right R-independent'. We also write R_n for the set of elements of degree at most n.

Let I be any right ideal of R; we put $B_0 = \emptyset$ and for $n > 0$, define B_n inductively as an R-independent subset of I consisting of B_{n-1} and elements of degree n, and which is maximal subject to these conditions. Such a maximal subset clearly exists, by Zorn's Lemma. The union $B = \bigcup_{n=1}^{\infty} B_n$ is again R-independent, and the right ideal J generated by B is a free R-module with B as free generating set. For if we had a relation

$$\Sigma b_i c_i = 0, \tag{14}$$

between elements $b_1, \ldots, b_r \in B$ with $c_1, \ldots, c_r$ not all zero, then by taking (14) mod R_{n-1}, where $n = \max\{d(b_i c_i)\}$, we get an R-dependence between elements of B, a contradiction. Next we prove

$$J + (I \cap k) = I. \tag{15}$$

Since $B \subseteq I$, we have $J \subseteq I$ and so $J + (I \cap k) \subseteq I$. Therefore if (15) is false, there must be an element of I which does not belong to the left-hand side. Let a be such an element of least degree, n say; then $n > 0$, because the left-hand side of (15) contains $I \cap k$. Further, $a \notin B$ and so by the maximality of B_n, $B_n \cup \{a\}$ contains an R-dependent subset, which must involve a. By the generalized algorithm, a is R-dependent on a subset of B_n, say

$$d(a - \Sigma b_i c_i) < d(a) \quad (c_i \in R).$$

Now by the choice of a, we have

$$a - \Sigma b_i c_i \in J + (I \cap k),$$

and so $a \in J + (I \cap k)$, a contradiction; this proves (15).

https://doi.org/10.1017/S0305004100034812 Published online by Cambridge University Press

Now to prove (ii) we may take $I \neq R$, since R itself is clearly free with 1 as a free generator. Then $I \cap k = 0$ and by (15), $I = J$ is a free R-module on B. To prove (iii) we take $I = R$, then $I \cap k = k$ and (15) becomes

$$J + k = R. \tag{16}$$

Now B consists of elements of positive degree only; by R-independence it follows that $1 \notin J$ and so $J \cap k = 0$. Hence the sum in (16) is direct and (iii) follows.

The last assertion of the theorem follows by symmetry from (ii) and (iii), using Theorem 3·2. This completes the proof.

If R is as in Theorem 3·3 and I is a right ideal in R, then the right R-independent generating set B of I constructed in the above proof is of course not necessarily unique. But it is not hard to see that the cardinal of the subset of B consisting of elements of a given degree n is independent of the choice of B.

Theorem 3·3 suggests the question whether k may always be complemented by a two-sided ideal in R. The answer is 'no', as may be seen by considering the ring $k[x; \iota, D]$, where ι is the identity automorphism of k and D is a derivation of k which is not inner.

From Theorem 3·3 it is now an easy matter to derive a normal form for the elements of a ring with a generalized algorithm.

THEOREM 3·4. *Let R be a ring with a degree-function satisfying the generalized algorithm. Denote by k the field of elements of non-positive degree and let $X = \{x_\lambda\}$ $(\lambda \in \Lambda)$ be a right R-independent generating set for a right ideal complementing k in R. Then every element of R can be written in just one way as*

$$\Sigma x_I \alpha_I \quad (\alpha_I \in k, \text{ almost all } \alpha_I \text{ are } 0), \tag{17}$$

where $I = (i_1, \ldots, i_n)$ runs over all ordered finite subsets of Λ and

$$x_I = x_{i_1} \ldots x_{i_n}.$$

(We note that since the x's belong to R, every expression of the form (17) does represent an element of R.)

Proof. Let R' be the subset of R consisting of all elements of the form (17) (for a given generating set X) so that $R' \supseteq k$. If $R' \neq R$, let a be an element of least degree in R which is not in R'. Now if J denotes the right ideal generated by X, then $R = J \oplus k$, and hence

$$a = \Sigma x_\lambda a_\lambda + \alpha \quad (a_\lambda \in R, \alpha \in k). \tag{18}$$

Since X is right R-independent, (18) implies that

$$d(x_\lambda a_\lambda) \leqslant d(a). \tag{19}$$

On the other hand, the x's are all of positive degree because $J \cap k = 0$. Therefore by (19),

$$d(a_\lambda) < d(a) \quad \text{for all } \lambda \in \Lambda.$$

By the choice of a, we have $a_\lambda \in R'$ for all $\lambda \in \Lambda$, and hence from (18), $a \in R'$, a contradiction, which shows that $R' = R$. Now the uniqueness of (17) follows because X is right R-independent and this completes the proof.

https://doi.org/10.1017/S0305004100034812 Published online by Cambridge University Press

As a converse to Theorem 3·4 we have

THEOREM 3·5. *Let k be a field and R a k-ring with a subset $X = \{x_\lambda\}$ $(\lambda \in \Lambda)$, such that every element of R can be uniquely expressed as*

$$\Sigma x_I \alpha_I \quad (\alpha_I \in k, \text{ almost all } \alpha_I \text{ are } 0), \tag{20}$$

where x_I is as in Theorem 3·4. Suppose further that R has a degree-function such that every element of degree zero belongs to k and at least one of the following conditions is satisfied:

(i) *Every element of positive degree in R is right R-dependent on X,*

(ii) *X is right R-independent.*

Then so is the other condition and the generalized algorithm holds in R.

Proof. We begin by showing that (i) implies (ii). Clearly we have $0 \notin X$ in any case; suppose now that (i) holds and let $x_1, \ldots, x_r$ be a right R-dependent subset of X. Then there exist $a_1, \ldots, a_r \in R$ such that

$$d(x_1 a_1) = \ldots = d(x_r a_r) > d(\Sigma x_i a_i). \tag{21}$$

If $d(\Sigma x_i a_i) = 0$, then we have

$$\Sigma x_i a_i + \alpha = 0 \quad (\alpha \in k),$$

whence by the uniqueness of (20), $\alpha = a_i = 0$, which contradicts (21). Therefore $d(\Sigma x_i a_i) = m > 0$ and by (i), $\Sigma x_i a_i$ is right R-dependent on X, i.e.

$$\Sigma x_i a_i = \Sigma x_\lambda b_\lambda \quad (d(x_\lambda b_\lambda) \leqslant m). \tag{22}$$

By the uniqueness of (20), the x's occurring on the two sides of (22) must be the same, with the same multipliers. But this contradicts the fact that for all i and all λ, by (22) and (21),

$$d(x_\lambda b_\lambda) \leqslant m < d(x_i a_i).$$

Hence X is right R-independent, i.e. (ii) holds.

Suppose next that (ii) holds and let

$$a = \Sigma x_I \alpha_I \tag{23}$$

be any element of positive degree. Then $\max\{d(x_I \alpha_I)\} > 0$; but by the R-independence of X, $\max\{d(x_I \alpha_I)\} \leqslant d(a)$ and so (23) expresses that a is right R-dependent on X, i.e. (i) holds.

We now assume (i) and (ii) and show that any element of maximal degree in a left R-dependent set is left R-dependent on the rest. The generalized algorithm then follows by symmetry (Theorem 3·3). Let $b_1, \ldots, b_r \in R$ be left R-dependent; thus

$$d(\Sigma a_i b_i) < d(a_1 b_1) = \ldots = d(a_r b_r) = n, \quad \text{say}, \tag{24}$$

for some $a_1, \ldots, a_r \in R$; we use induction on n to establish the result. If $n = 0$, then $b_1, \ldots, b_r \in k$ and the result is clear, so let $n > 0$. We may assume without loss of generality that $d(b_1) \geqslant d(b_i)$ $(i = 2, \ldots, r)$. It follows that

$$d(a_1) \leqslant d(a_i) \quad (i = 2, \ldots, r). \tag{25}$$

https://doi.org/10.1017/S0305004100034812 Published online by Cambridge University Press

If $d(a_1) = 0$, then $a_1 \in k$, $a_1 \neq 0$, and so

$$d\left(b_1 + \sum_{i=2}^{r} a_1^{-1} a_i b_i\right) = d(\Sigma a_i b_i) < d(a_1 b_1) = d(b_1),$$

and $$d(a_1^{-1} a_i b_i) = d(a_i b_i) = d(b_1) \quad (i = 2, \ldots, r);$$

i.e. b_1 is left R-dependent on $b_2, \ldots, b_r$. We may therefore assume that $d(a_1) > 0$; by (25), $a_1, \ldots, a_r$ are then all of positive degree and so by (i),

$$a_i = \sum_{\lambda} x_\lambda a_{\lambda i}, \quad d(x_\lambda a_{\lambda i}) \leqslant d(a_i). \tag{26}$$

Substituting from (26) into (24) we obtain

$$d(\Sigma x_\lambda a_{\lambda i} b_i) < n.$$

By (ii) it follows that $d(\sum_i x_\lambda a_{\lambda i} b_i) < n$ for each $\lambda \in \Lambda$, i.e.

$$d(\sum_i a_{\lambda i} b_i) < n - d(x_\lambda) \quad (\lambda \in \Lambda). \tag{27}$$

Now by (26), for each $\mu \in \Lambda$,

$$d(x_\mu a_{\mu 1} b_1) \leqslant d(a_1 b_1) = d(\sum_\lambda x_\lambda a_{\lambda 1} b_1) \leqslant \max_\lambda \{d(x_\lambda a_{\lambda 1} b_1)\}.$$

Hence for some $\lambda \in \Lambda$, say for $\lambda = 1$, we have

$$n = d(a_1 b_1) = d(\sum_\lambda x_\lambda a_{\lambda 1} b_1) = d(x_1 a_{11} b_1).$$

Together with (24), (26) and (27) this shows that $d(a_{1i} b_i) \leqslant d(a_{11} b_1)$ and

$$d(\Sigma a_{1i} b_i) < d(a_{11} b_1) < n.$$

Omitting terms $a_{1i} b_i$ of degree less than $d(a_{11} b_1)$, we obtain a left R-dependence of degree less than n between the remaining b's, which will certainly include b_1, by definition. By the induction hypothesis on n, b_1 is left R-dependent on the remaining b's and the conclusion follows. This completes the proof.

From Theorem 3·4 it follows that the conditions (i) and (ii) are necessary as well as sufficient for the existence of the generalized algorithm. The following example shows that they cannot be omitted entirely.

Let A be the free associative algebra on the free generators $x_1, \ldots, x_r$ ($r \geqslant 2$) over a commutative field F. The commutators in the x's span the free Lie algebra L on the x's, and if $u_1, u_2, \ldots$ is a basis of L, then the elements

$$u_I = u_{i_1} u_{i_2} \ldots u_{i_n} \quad (i_1 \leqslant i_2 \leqslant \ldots \leqslant i_n;\ n = 0, 1, \ldots) \tag{28}$$

form a basis of A (cf. Birkhoff (1), Witt (8)). If u_I is as in (28) we put $d(u_I) = n$, and generally if

$$a = \Sigma u_I \alpha_I,$$

we define $d(a) = \max\{d(u_I) | \alpha_I \neq 0\}$. In this way we obtain a degree-function on A such that the elements of degree zero belong to F. We also have a normal form of the

https://doi.org/10.1017/S0305004100034812 Published online by Cambridge University Press

type (20) (in terms of $x_1, \ldots, x_r$), but the generalized algorithm does not hold in A. For the elements x_1 and x_2 are right A-dependent

$$d(x_1x_2 - x_2x_1) < d(x_1x_2) = d(x_2x_1),$$

although neither is right A-dependent on the other.

Similarly, the condition that every element of degree zero belong to the coefficient field cannot be omitted from Theorem 3·5, as is shown by taking a free associative algebra and defining all non-zero elements to be of degree zero.

In any k-ring R whose elements have the normal form (20), relative to some subset X, the multiplication is determined completely by the way in which k acts on R from the left. Thus, by linearity, the multiplication in R is determined by formulae of the form

$$\alpha x_I = \Sigma x_J \phi_{JI}(\alpha) \quad (\alpha \in k), \tag{29}$$

where (ϕ_{JI}) is a column-finite matrix-function on k. If, moreover, R has a degree-function which satisfies condition (ii) of Theorem 3·5 relative to X, then for any expression (20) we have

$$d(\Sigma x_I \alpha_I) \geqslant \max\{d(x_I\alpha_I)\}.$$

Together with D. 2 this shows that

$$\begin{aligned} d(\Sigma x_I \alpha_I) &= \max\{d(x_I\alpha_I)\} \\ &= \max\{d(x_I)|\alpha_I \neq 0\}, \end{aligned}$$

and using D. 3 we see that the degree-function is completely determined by its values on the subset X of R. These values cannot be assigned arbitrarily; for in the first place, we must have

$$d(x_\lambda) > 0 \quad \text{for all } \lambda \in \Lambda. \tag{30}$$

Secondly, by (29), we have

$$d(x_J) \leqslant d(x_I) \quad \text{whenever } \phi_{JI} \neq 0. \tag{31}$$

Thus the matrix (ϕ_{JI}) is 'triangular'. Conversely, any degree-function satisfying (30) and (31) also satisfies the hypotheses of Theorem 3·5, so that the generalized algorithm holds with respect to this function. It follows from this that it will be possible to satisfy condition (ii) of Theorem 3·5 (and hence the generalized algorithm) for *every* degree-function satisfying (30), if and only if (ϕ_{JI}) is a 'diagonal' matrix, i.e. if and only if (29) reduces to

$$\alpha x_I = x_I \phi_I(\alpha) \quad (\alpha \in k). \tag{32}$$

As a further specialization of (32) we have the case of a free associative algebra over a commutative field, which may be characterized as follows:

THEOREM 3·6. *Let A be an algebra over a commutative field F, with a degree-function such that for any non-zero element a of A,*

$$d(a) = 0 \quad \textit{if and only if} \quad a \in F.$$

Then A is a free associative algebra over F with a right A-independent free generating set if and only if the generalized algorithm holds in A.

This result is an immediate consequence of Theorems 3·4 and 3·5.

https://doi.org/10.1017/S0305004100034812 Published online by Cambridge University Press

4. *The semigroup of degrees.* So far we have assumed the degrees $d(a)$ to be non-negative integers and we now examine whether the Euclidean algorithm may be generalized by relaxing this assumption. Since we shall still want D. 2 and D. 3 to hold, the set S of degrees will have to be a semigroup which has some ordering. If the division algorithm is to hold, S has to satisfy a further condition which will certainly hold if the ordering is induced by left-divisibility.† Moreover, for the Euclidean algorithm to terminate, the ordering has to be a well-ordering. Thus we have to consider semigroups with the following property:

S. 1. The relation '$\leqslant$' on S defined by

$$a \leqslant b \quad \text{if and only if} \quad ax = b \text{ for some } x \in S$$

is a well-ordering of S.

A further desirable (though not essential) property is the possibility of right-cancellation. This will ensure, for example, that if a and b are elements of positive degree in R, then the quotient q in (4) is of lower degree than a. We now show that the integers form the only semigroup with more than one element which satisfies these conditions.

THEOREM 4·1. *Let S be a semigroup with more than one element, which satisfies* S. 1 *and possesses right-cancellation*

$$ac = bc \quad \textit{implies} \quad a = b \quad \textit{for all } a, b, c \in S. \tag{33}$$

Then S is isomorphic to the additive semigroup of non-negative integers.

Proof. We shall write '$b \geqslant a$' to mean '$a \leqslant b$' and '$a < b$' or '$b > a$' to mean '$a \leqslant b$ and $a \neq b$'. Now let e be the first element of S. By hypothesis there exists $f \in S$ such that $ef = e$, and since $e \leqslant f$, we have $f = eg$ for some $g \in S$. Thus $e^2g = e$; it follows that $e^2 \leqslant e$, and by the definition of e, $e^2 = e$. Now for any $a \in S$, $ae^2 = ae$ and hence, by (33)

$$ae = a. \tag{34}$$

Next consider ea; if $ea \leqslant a$, let $a = eax$ $(x \in S)$, then $a = eax = e^2ax^2 = eax^2$, hence by (33),

$$ea = eax = a.$$

On the other hand, if $a \leqslant ea$, let $ea = ay$ $(y \in S)$, then $ay = ea = e^2a = eay = ay^2$, hence $a = ay = ea$; therefore in any case

$$ea = a.$$

Together with (34) this shows that the first element of S is also the unit-element of S. We denote this unit-element by 1; a similar argument applied to an arbitrary idempotent of S shows that any such idempotent must coincide with 1, in other words, S has no idempotent other than 1.

By hypothesis the set $S - \{1\}$ is not empty; let x be its first element and denote by S' the subsemigroup of S generated by x and 1. Since S has no idempotent $\neq 1$, the powers of x are all distinct and so S' is isomorphic to the additive semigroup of integers. Now suppose that $S' \neq S$, and let y be the first element of S which is not in S'. By the definition of y, we have $y > x$ and hence

$$y = xz \tag{35}$$

† In this section we write the semigroup of degrees multiplicatively.

https://doi.org/10.1017/S0305004100034812 Published online by Cambridge University Press

for some $z \in S$. Since $y \notin S'$, we have $z \notin S'$ and so

$$z \geqslant y, \tag{36}$$

again by the definition of y. Multiplying (36) on the left† by x and using (35), we obtain

$$y \geqslant xy,$$

and multiplying this repeatedly on the left by x, we get

$$y \geqslant xy \geqslant x^2y \geqslant \ldots.$$

By the well-ordering property, we must have $x^ny = x^{n+1}y$, for some $n \geqslant 0$, hence by (33), $x = 1$, which is a contradiction. This completes the proof.

It may be of interest to note that if instead of right-cancellation we impose left-cancellation, other types of semigroup can occur. The complete classification is given in

THEOREM 4·2. *For any ordinal number α, denote by S_α the semigroup with unit-element, generated by elements x_β $(1 \leqslant \beta < \alpha)$ with the defining relations*

$$x_\beta x_\gamma = x_\gamma \quad \text{if} \quad \beta < \gamma.$$

Then S_α has left-cancellation and satisfies the condition S. 1, *in fact the ordering of S_α is just the lexicographic ordering in the x's and the order-type of S_α is ω^α.*

Conversely, every semigroup with left-cancellation and satisfying S. 1 *is isomorphic to S_α, for some ordinal number α. Moreover, every element of S_α can be written uniquely as*

$$x_{\alpha_1}^{\nu_1} x_{\alpha_2}^{\nu_2} \ldots x_{\alpha_n}^{\nu_n} \quad (\alpha > \alpha_1 > \ldots > \alpha_n;\ n = 0, 1, \ldots;\ \nu_i \text{ positive integers}).$$

The proof is similar to those of Theorems 3·3 and 4·1. As we do not require Theorem 4·2, we omit the proof.

In conclusion we note that if neither left- nor right-cancellation is imposed, we can define a semigroup structure satisfying S. 1 on any well-ordered set. We need only put

$$ab = \max\{a, b\}.$$

REFERENCES

(1) BIRKHOFF, G. Representability of Lie algebras and Lie groups by matrices. *Ann. Math., Princeton*, 38 (1937), 526–32.
(2) COHN, P. M. On the free product of associative rings. II. *Math. Z.* 73 (1960), 433–56.
(3) LEVI, HOWARD. A characterization of polynomial rings by means of order relations. *Amer. J. Math.* 65 (1943), 221–34.
(4) MCCOY, N. H. *Rings and ideals* (Baltimore, 1948).
(5) ORE, O. Linear equations in non-commutative fields. *Ann. Math., Princeton*, 32 (1931), 463–77.
(6) ORE, O. Theory of non-commutative polynomials. *Ann. Math., Princeton*, 34 (1933), 480–508.
(7) SCHILLING, O. F. G. *The theory of valuations* (New York, 1950).
(8) WITT, E. Treue Darstellung Liescher Ringe. *J. reine angew. Math.* 177 (1937), 152–60.

THE UNIVERSITY
MANCHESTER 13

† The ordering is preserved under left-multiplication, by definition (cf. S. 1).

https://doi.org/10.1017/S0305004100034812 Published online by Cambridge University Press