ON THE EMBEDDING OF RINGS IN SKEW FIELDS

By P. M. COHN

[Received 18 May 1960]

1. Introduction

It is well known that a commutative ring can be embedded in a field if and only if it has no zero-divisors.† A more general result, due to Ore (**11**), states that a ring R can be embedded in a (skew) field‡ provided that it satisfies the following two conditions:

O.1. *R has no zero-divisors*;

O.2. *any two non-zero elements of R have a non-zero common right multiple.*

Moreover, these conditions are necessary and sufficient for the elements of the containing field to have the form of right quotients ab^{-1} $(a, b \in R)$. For a ring to be embeddable in any field at all, O.2 is of course not necessary [B. H. Neumann (**10**); cf. also § 6 below], while O.1, though necessary, is not sufficient [Mal'cev (**8**)].

Apart from these two cases there is the method of power series which, for example, enables one to embed the group ring of an ordered group in a field [cf. Mal'cev (**9**), B. H. Neumann (**10**)]. Here the difficulties arising from the lack of commutativity are overcome by the fact that the multiplicative commutators in R are organized in a certain way (namely, by the ordering). Now it would be desirable to have a method of embedding which makes use of the additive commutators of R in a similar way. This suggests taking for R the associative enveloping algebra $A(L)$ of a Lie algebra L. When L is finite-dimensional, $A(L)$ is known to satisfy Ore's conditions and so is embeddable in a field [Tamari (**14**)], but unfortunately this excludes the interesting case of a free associative algebra (which arises as the associative enveloping algebra of a free Lie algebra).§

The purpose of this paper is to construct an embedding in fields for a class of rings which includes the associative enveloping algebra of a Lie algebra of arbitrary dimension. Any ring R with a filtration (R_i) has

† We do not count zero among the zero-divisors.

‡ Throughout we shall use the word 'field' to mean 'not necessarily commutative division ring'.

§ Note, however, that this case is covered by the Mal'cev–Neumann result.

associated with it a graded ring $G(R) = \sum (R_i/R_{i+1})$; our main result may now be stated as follows:

Any ring R with a filtration such that the associated graded ring $G(R)$ satisfies the Ore conditions O.1–2, is embeddable in a field.

The proof occupies § 4. This is preceded by an analogous result for semigroups in § 2, while § 3 describes a set of axioms for fields (in terms of multiplication and the operation $x \to 1-x$), which enables us to translate the results of § 2 to rings. Now the associative enveloping algebra $A(L)$ of a Lie algebra L may be described as a ring with a filtration whose associated graded ring is a polynomial ring in a number of indeterminates (over a commutative field), so that the above embedding theorem may be applied.

Any filtered algebra whose graded algebra is a polynomial ring, is called a *Birkhoff–Witt algebra*. Their structure is completely described in § 5, where it is shown that a Birkhoff–Witt algebra determines and is determined by a Lie algebra L and an 'invariant' alternating bilinear form on L. Finally, in § 6 we briefly consider the case of finite-dimensional Lie algebras treated by Tamari (**14**). Although this is, of course, covered by the result of § 4, it may be of interest to rederive Tamari's result by verifying the finite basis property for right ideals in $A(L)$ and applying a result of Goldie (**5**). This basis theorem for $A(L)$ is equivalent to the Hilbert basis theorem for polynomial rings, as has been observed by Cartier (**7**). Thus § 6 contains no new results, but it is hoped that the proofs given (which incidentally lead to a short proof of the Hilbert basis theorem) may be not without interest.

2. The embedding theorem for a class of inverse limit semigroups

The Ore conditions, stated in § 1, for the existence of a field of right quotients, do not involve the ring addition and in fact the result includes one on the embeddability of semigroups in groups, as has been observed by Dubreil (**3**). This result may be stated as follows:

Let S be a cancellation semigroup such that

$$aS \cap bS \neq \varnothing \quad \textit{for all } a, b \in S; \tag{1}$$

then S has a group of right quotients, i.e. there exists a group G containing S such that every element of G has the form ab^{-1} $(a, b \in S)$; thus

$$SS^{-1} = G. \tag{2}$$

The group of right quotients of a semigroup, when it exists, is unique. More generally we have

THEOREM 2.1. *Let S be a semigroup with a group G of right quotients. Then any homomorphism ϕ of S into a group H can be extended to a unique homomorphism $\bar{\phi}$ of G into H. If ϕ is 1–1, then so is $\bar{\phi}$.*

The existence and uniqueness of $\bar{\phi}$ follow if we observe that (i) the relations in G all follow from the defining relations in S and (ii) G is the group generated by S.

If $\bar{\phi}$ is not 1–1, then its kernel contains an element $u \neq 1$. By hypothesis, $u = ab^{-1}$ $(a, b \in S)$, so that $ab^{-1} \neq 1$ and $(ab^{-1})\bar{\phi} = 1$. Hence we have $a \neq b$ and $a\phi = a\bar{\phi} = b\bar{\phi} = b\phi$, which shows that ϕ cannot be 1–1 either.

From the second part of the theorem we obtain the

COROLLARY. *If S is a semigroup with a group of right quotients, then any two groups containing S and generated by S are isomorphic, under an isomorphism leaving S elementwise fixed.*

Theorem 2.1 may be used to extend the Ore–Dubreil result to inverse limits of semigroups, as follows.

THEOREM 2.2. *Let S be a semigroup and $\mathfrak{q}_\lambda$ $(\lambda \in \Lambda)$ a directed system of congruences on S (over the directed set Λ) such that*

(i) $\lambda \geqslant \mu$ *implies* $\mathfrak{q}_\lambda \subseteq \mathfrak{q}_\mu$,

(ii) $\bigcap \mathfrak{q}_\lambda = \Delta$, *where Δ is the diagonal on S,*

(iii) *for each $\lambda \in \Lambda$, $S/\mathfrak{q}_\lambda$ is a cancellation semigroup satisfying the right multiple condition* (1).

Then S may be embedded in a group; more precisely, there exists a complete topological group G containing S as a subsemigroup such that SS^{-1} is dense in G; the topology on G is not discrete unless S itself satisfies the condition (1).

Proof. Put $S/\mathfrak{q}_\lambda = S_\lambda$ and for $\lambda \geqslant \mu$, define the natural homomorphisms

$$\phi_{\lambda\mu}\colon S_\lambda \to S_\mu.$$

If G_λ is the unique group of right quotients of S_λ, then for $\lambda \geqslant \mu$ the homomorphism $\phi_{\lambda\mu}$ may be regarded as a homomorphism of S_λ into G_μ, and by Theorem 2.1 it may be extended to a unique homomorphism

$$\pi_{\lambda\mu}\colon G_\lambda \to G_\mu.$$

These homomorphisms are easily seen to be coherent: $\pi_{\lambda\lambda} = 1$ and $\pi_{\lambda\mu}\pi_{\mu\nu} = \pi_{\lambda\nu}$ whenever $\lambda \geqslant \mu \geqslant \nu$; so we may form their inverse limit G, with projections

$$\pi_\lambda\colon G \to G_\lambda$$

[cf. Eilenberg and Steenrod (4), ch. viii]. Let θ_λ be the natural homomorphism of S onto S_λ, and hence into G_λ, then it is clear that $\theta_\lambda \pi_{\lambda\mu} = \theta_\mu$, therefore† the θ_λ may be lifted to a homomorphism $\theta: S \to G$ such that

$$\theta\pi_\lambda = \theta_\lambda. \tag{3}$$

By (ii) any two distinct elements of S have distinct images under some θ_λ, hence by (3) their images under θ are distinct, i.e. θ is 1–1. Thus θ provides an embedding of S in G. Now G becomes a topological group if the subgroups $K_\lambda = \ker \pi_\lambda$ are taken as a neighbourhood base at 1. It is clear—from the definition of G as inverse limit—that G is complete in this topology, and given $x \in G$ and $\lambda \in \Lambda$ we have $x \equiv ab^{-1} \pmod{K_\lambda}$ for some $a, b \in S$ because $G/K_\lambda \cong G_\lambda$ and S_λ satisfies (1); hence SS^{-1} is dense in G. If G is discrete this means that $SS^{-1} = G$, i.e. S satisfies (2) and hence (1). This completes the proof.

Let $\mathfrak{q}_\lambda$ and K_λ be as in the proof of Theorem 2.2. Then by the last part of Theorem 2.1, for any $a, b \in S$,

$$a \equiv b \pmod{\mathfrak{q}_\lambda} \quad \text{if and only if} \quad a \equiv b \pmod{K_\lambda}.$$

It follows that for any $a, b, c, d \in S$,

$$ab^{-1} \equiv cd^{-1} \pmod{K_\lambda} \tag{4}$$

if and only if there exist $x, y \in S$ such that

$$ax \equiv cy \pmod{\mathfrak{q}_\lambda}, \qquad bx \equiv dy \pmod{\mathfrak{q}_\lambda}. \tag{5}$$

For (4) is equivalent to

$$b^{-1}d \equiv a^{-1}c \pmod{K_\lambda}. \tag{6}$$

Assume then that (6) holds; by hypothesis there exist $x, y \in S$ such that $ax \equiv cy \pmod{\mathfrak{q}_\lambda}$. Hence $xy^{-1} \equiv a^{-1}c \pmod{K_\lambda}$, and by (6), $xy^{-1} \equiv b^{-1}d \pmod{K_\lambda}$, i.e. $bx \equiv dy \pmod{\mathfrak{q}_\lambda}$; thus (5) holds. Conversely, from (5) we obtain $a^{-1}c \equiv xy^{-1} \equiv b^{-1}d \pmod{K_\lambda}$, hence (6) and with it (4).

3. A set of axioms for fields

In order to apply the results of § 2 to embed rings in fields we need a definition of fields which uses as little as possible of the additive properties. This is accomplished by the following lemma which defines fields in terms of multiplication and the operation $x \to 1-x$.

LEMMA 3.1. *Let G be a group with an element e and a mapping θ of the set $G_1 = \{x \in G \mid x \neq 1\}$ into itself such that*

(i) $(yxy^{-1})\theta = y(x\theta)y^{-1}$ $\quad (x \in G_1,\ y \in G)$,

(ii) $x\theta^2 = x$ $\quad (x \in G_1)$,

(iii) $(x^{-1})\theta = e(x\theta)x^{-1}$ $\quad (x \in G_1)$,

(iv) $(xy^{-1})\theta = (x\theta(y\theta)^{-1})\theta . (y^{-1})\theta$ $\quad (x, y \in G_1,\ x \neq y)$.

† Cf. Eilenberg and Steenrod (4) 218 for a parallel case.

Then there exists a unique field K such that the multiplicative group of K coincides with G, and on G,

$$x\theta = 1-x \quad (x \in G_1), \tag{1}$$

$$e = -1. \tag{2}$$

Proof. We begin by noting that from the definition of θ as a mapping of G_1 into itself, θ is only applied to elements of G_1. This is clear for (i)–(iii) and for (iv) it follows because θ is one-one, by (ii). Further, we may exclude the case $G = \{1\}$, in which the lemma holds trivially.

If K is a field with the required properties then the multiplicative group of K must coincide with G, as a group. Thus K is obtained by adjoining 0 to G and extending the multiplication on G by the rule

$$0x = x0 = 0 \quad (x \in K). \tag{3}$$

Let us extend the mapping θ to K by putting $1\theta = 0$, $0\theta = 1$, then if (1) and (2) are to hold we must have

$$1-x = x\theta \quad (x \in K),$$

and it follows that the subtraction on K—which together with the multiplication determines K completely—must be given by

$$x-y = \begin{cases} ey & \text{if } x = 0, \\ (yx^{-1})\theta . x & \text{if } x \neq 0. \end{cases} \tag{4}$$

Thus the field K, if it exists, is uniquely determined. We now show that (3) and (4) always define a field structure on $K = G \cup \{0\}$, when the hypotheses of the lemma are satisfied.

To define a field structure on K it is enough to define the additive group structure and verify the distributive laws. Now an abelian group, written additively, may be defined in terms of subtraction, a set of laws being

$$a-(a-b) = b, \tag{5}$$

$$(a-b)-c = (a-c)-b \tag{6}$$

[cf. Rabinow (**12**)], and the distributive laws are then equivalent to

$$(a-b)c = ac-bc, \tag{7}$$

$$a(b-c) = ab-ac. \tag{8}$$

Thus we have to verify (5)–(8), using the definitions (3) and (4). We begin with (7) and (8). If a or c vanishes, the two sides of (7) reduce both to ebc, so we may assume that $ac \neq 0$. Then we have

$$ac-bc = (bcc^{-1}a^{-1})\theta . ac = (ba^{-1})\theta . ac = (a-b)c$$

by the definition (4); hence (7) holds.

Before proving (8) we note that e belongs to the centre of G. For by (i), x commutes with $x\theta$ and $(x^{-1})\theta$, for any $x \in G_1$, and hence, by (iii),

$ex = (x^{-1})\theta x(x\theta)^{-1}x = xe$. If in (8) a or b vanishes, the two sides reduce to eac ($= aec$), so we may assume that $ab \neq 0$. Then (8) asserts

$$a(cb^{-1})\theta . b = (acb^{-1}a^{-1})\theta . ab,$$

i.e.
$$a(cb^{-1})\theta . a^{-1} = (acb^{-1}a^{-1})\theta. \tag{9}$$

But this is just (i), provided that $c \neq 0, b$. In these exceptional cases both sides of (9) reduce to 1 or 0 respectively, thus (9) and with it (8) holds in all cases.

The condition (ii) may be restated as

$$1-(1-x) = x;$$

in this form it still holds for $x = 1$ and $x = 0$. Multiplying on the left by an element a of K, we obtain, by (8),

$$a-(a-ax) = ax.$$

As x varies over K, so does ax, provided that $a \neq 0$; hence putting $ax = b$ we obtain (5) in case $a \neq 0$. When $a = 0$, (5) reduces to the form $-(-b) = b$, i.e. $e^2 b = b$, so that it is enough to show that

$$e^2 = 1. \tag{10}$$

Now by (iii) we have $e = (x^{-1})\theta . x(x\theta)^{-1}$, for any $x \in G_1$, and such elements exist because $G \neq \{1\}$. Therefore

$$e^2 = (x^{-1})\theta . x(x\theta)^{-1} . (x\theta)x^{-1}(x^{-1}\theta)^{-1} = 1.$$

This proves (10) and hence (5) for all $a, b \in K$.

We note that (iii), with x replaced by x^{-1}, may be written as

$$1-x = -(x-1);$$

clearly this still holds for $x = 1$ and by (10) it also holds for $x = 0$. Multiplying both sides by a we find

$$a-ax = -(ax-a).$$

As x varies over K, so does ax if $a \neq 0$; hence we obtain

$$a-b = -(b-a), \tag{11}$$

provided that $a \neq 0$; but for $a = 0$ it holds trivially and so (11) holds for all $a, b \in K$.

To prove (6) we write out (iv) with y replaced by $y\theta = 1-y$:

$$1-x(1-y)^{-1} = [1-(1-x)y^{-1}][1-(1-y)^{-1}].$$

Now multiply by $1-y$ on the right, using (7), (11), and (5) in turn:

$$\begin{aligned}(1-y)-x &= [1-(1-x)y^{-1}][(1-y)-1] = -[1-(1-x)y^{-1}][1-(1-y)] \\ &= -[1-(1-x)y^{-1}]y = -[y-(1-x)];\end{aligned}$$

hence
$$(1-y)-x = (1-x)-y. \tag{12}$$

Clearly this still holds for $x = 1-y$ and $x = 0$, while for $x = 1$ it follows by applying (11) and (5). Thus (12) holds for all x and similarly for all y in K. Putting $x = a^{-1}b$ and $y = a^{-1}c$ and multiplying by a on the left we thus obtain (6) when $a \neq 0$. But when $a = 0$, we have by (11) and (10),

$$eb-c = e(c-eb) = ec-b,$$

which establishes (6) in this case. This completes the proof.

We note in passing that by applying θ and taking inverses we obtain the six values of a cross-ratio from one of them; in fact (ii) and (iii) are part of the defining relations of the cross-ratio group. The remaining relation to make up a complete set, namely,

$$(((((x^{-1})\theta)^{-1})\theta)^{-1})\theta = x,$$

may be obtained directly by replacing x and y in (iv) by $x\theta$ and $y\theta$ respectively and applying (iv) again.

If R is any ring without zero-divisors, then the non-zero elements of R form a cancellation semigroup which we shall denote by R^* throughout. In case R also satisfies the second Ore condition (O.2, § 1), the semigroup R^* satisfies the right multiple condition [cf. (1), § 2], and it follows that R^* has a group of right quotients G, say. On G a unary operation θ may be defined as follows: if $u \in G$, $u \neq 1$, let $u = ab^{-1}$ ($a, b \in R^*$, $a \neq b$), then

$$u\theta = (b-a)b^{-1}. \tag{13}$$

This is a well-defined operation, for if $ab^{-1} = cd^{-1}$, let $x, y \in R^*$ be such that $bx = dy$, then $ax = cy$ and hence

$$(b-a)x = bx-ax = dy-cy = (d-c)y,$$

therefore $$(b-a)b^{-1} = (d-c)d^{-1}.$$

Now it may be shown without difficulty that the operation (13) satisfies all the conditions of Lemma 3.1. Of course, it is not suggested that the existence of a field of right quotients for R should be proved in this way, since the direct proof due to Ore is much shorter. However, in § 4 we shall encounter a situation where we shall have to proceed in this way.

4. The embedding theorem for a class of rings

A ring R is said to be *valuated* if a function $v(x)$ is defined on R taking the integers or $+\infty$ as values, such that

V.1. $v(x) = \infty$ if and only if $x = 0$,

V.2. $v(xy) = v(x)+v(y)$,

V.3. $v(x-y) \geqslant \min\{v(x), v(y)\}$.

The function v is also called a *valuation* on R. From V.1 and V.2 it follows that R has no zero-divisors, so that R^* is a cancellation semigroup, and from V.3 one deduces as in the case of valuations on fields that

$$v(-x) = v(x), \tag{1}$$

and $$v(x \pm y) = \min\{v(x), v(y)\} \quad \text{unless } v(x) = v(y) \tag{2}$$

[cf. Schilling (**13**) 9]. With these definitions we have the following embedding theorem for rings.

THEOREM 4.1. *Let R be a valuated ring such that for any a, $b \in R^*$ the function*

$$f(x,y) = v(ax-by)-v(ax)$$

is unbounded above. Then R can be embedded in a field.

Proof. In proving the theorem we may clearly assume that R contains more than one element; moreover, as we have seen, R can have no zero-divisors. In order to be able to apply Theorem 2.2 we define, for each $n > 0$, a relation $\mathfrak{q}_n$ on R^* by putting

$$a \equiv b \pmod{\mathfrak{q}_n} \quad \text{if and only if } v(a-b)-v(a) \geqslant n. \tag{3}$$

If $a \equiv b \pmod{\mathfrak{q}_n}$ then $v(a-b) > v(a)$ and hence

$$v(b) = v(a-(a-b)) = v(a),$$

by (2), i.e.

$$a \equiv b \pmod{\mathfrak{q}_n} \ (n > 0) \quad \text{implies} \quad v(a) = v(b). \tag{4}$$

The relation $\mathfrak{q}_n$ is obviously reflexive and by (4) it is also symmetric. Transitivity follows because from $a \equiv b$, $b \equiv c \pmod{\mathfrak{q}_n}$ we derive $v(a) = v(b) = v(c)$, by (4), and

$$v(a-c) \geqslant \min\{v(a-b),\, v(b-c)\} \geqslant n+v(a),$$

whence $a \equiv c \pmod{\mathfrak{q}_n}$. Thus each $\mathfrak{q}_n$ is an equivalence. Next we have to verify conditions (i)–(iii) of Theorem 2.2. Of these (i) is an immediate consequence of the definitions. To prove (ii), let $a \neq b$, then $v(a-b) \neq \infty$; hence k may be chosen so that $k > v(a-b)-v(a)$ and for this k, $a \not\equiv b \pmod{\mathfrak{q}_k}$. Turning to (iii), we take a, b, $c \in R^*$; then

$$v(a) = v(b) \Leftrightarrow v(ac) = v(bc) \Leftrightarrow v(ca) = v(cb);$$

further we have

$$\begin{aligned} v(ac-bc)-v(ac) &= v((a-b)c)-v(ac) \\ &= v(a-b)+v(c)-v(c)-v(a) \\ &= v(a-b)-v(a), \end{aligned}$$

and similarly $v(ca-cb)-v(ca) = v(a-b)-v(a)$. It follows that

$$a \equiv b \pmod{\mathfrak{q}_n} \Leftrightarrow ac \equiv bc \pmod{\mathfrak{q}_n} \Leftrightarrow ca \equiv cb \pmod{\mathfrak{q}_n},$$

and this shows $S/\mathfrak{q}_n$ to be a cancellation semigroup. Now the right multiple condition for $S/\mathfrak{q}_n$ is just a restatement of the hypothesis: given $a, b \in R^*$ and $n > 0$, there exist $x, y \in R^*$ such that

$$v(ax-by)-v(ax) \geqslant n$$

and hence $$ax \equiv by \pmod{\mathfrak{q}_n}.$$

Since all the hypotheses of Theorem 2.2 are satisfied, R^* may be embedded in a complete topological group G such that $R^*(R^*)^{-1}$ is dense in G. By the remark at the end of § 2,

$$ab^{-1} \equiv cd^{-1} \pmod{K_n} \tag{5}$$

holds if and only if there exist $x, y \in R^*$ such that

$$ax \equiv cy, \qquad bx \equiv dy \pmod{\mathfrak{q}_n}. \tag{6}$$

If this condition is satisfied, then $v(a)-v(b) = v(c)-v(d)$, so that the valuation may be extended to $R^*(R^*)^{-1}$ by putting

$$v(ab^{-1}) = v(a)-v(b). \tag{7}$$

By (4), (5), and (6), v is constant on the cosets of K_n in G, for every n, and it may therefore be extended in a natural way to a function defined on the whole of G and taking integer values. Like v, this function is again a homomorphism (into the additive group of integers) and we may, without ambiguity, denote this function on G again by v.

Let us denote the set $R^*(R^*)^{-1}$ by U, so that U is a dense subset of G, and write

$$G_1 = \{x \in G \mid x \neq 1\}, \qquad U_1 = \{ab^{-1} \in U \mid a \neq b\};$$

clearly $U = U_1 \cup \{1\}$, so that U_1 is dense in G_1. Now we define a mapping θ from U_1 to G_1 by the equation

$$(ab^{-1})\theta = (b-a)b^{-1}. \tag{8}$$

Of course we have to show that θ is single-valued: if

$$ab^{-1} = cd^{-1} \quad (a, b, c, d \in R^*),$$

then $b^{-1}d = a^{-1}c$ and there exist $x_n y_n^{-1} \in U$ such that $x_n y_n^{-1} \to b^{-1}d$. Thus $v(bx_n-dy_n)-v(bx_n) \to \infty$; this may be written

$$v((bx_n-dy_n)x_n^{-1})-v(b) \to \infty,$$

or since $v(b)$ is constant,

$$v((bx_n-dy_n)x_n^{-1}) \to \infty. \tag{9}$$

Similarly, since $x_n y_n^{-1} \to b^{-1}d = a^{-1}c$, we have

$$v((ax_n-cy_n)x_n^{-1}) \to \infty. \tag{10}$$

By (9) and (10), $\quad v([(b-a)x_n-(d-c)y_n]x_n^{-1}) \to \infty,$

whence $(b-a)x_n y_n^{-1} \to d-c$. Multiplying both sides by d^{-1} and observing that $x_n y_n^{-1} d^{-1} \to b^{-1}$, we obtain

$$(b-a)b^{-1} = \lim(b-a)x_n y_n^{-1} d^{-1} = (d-c)d^{-1}.$$

This shows θ to be single-valued on U_1. In order to extend θ to G_1 we require a lemma.

LEMMA. *If $u \in G_1$ and (u_n) is any sequence of elements of U_1 converging to u, then $\lim(u_n \theta)$ exists.*

To establish the convergence of $u_n \theta$ it is enough to show that $(u_n \theta)$ is a Cauchy-sequence; writing $u_n = a_n b_n^{-1}$ $(a_n, b_n \in R^*)$, we have to show that for any integer r there exists an integer n_0 such that

$$(b_m - a_m)b_m^{-1} \equiv (b_n - a_n)b_n^{-1} \pmod{K_r} \quad \text{for } m, n > n_0. \tag{11}$$

Since $a_n b_n^{-1} \to u$, we have

$$v(a_n b_n^{-1}) = v(u) = h \quad \text{say, for } n > n_1. \tag{12}$$

On the other hand, $u \neq 1$ and so there exist $k > 0$ and n_2 such that $a_n b_n^{-1} \not\equiv 1 \pmod{K_k}$ for $n > n_2$, i.e. $a_n \not\equiv b_n \pmod{K_k}$, whence

$$v((b_n - a_n)a_n^{-1}) < k \quad \text{for } n > n_2. \tag{13}$$

Now take a fixed r, put $\max\{r+k, r+k+h\} = s$ and choose n_3 so that

$$a_m b_m^{-1} \equiv a_n b_n^{-1} \pmod{K_s} \quad \text{for } m, n > n_3. \tag{14}$$

We assert that (11) holds for $n_0 = \max\{n_1, n_2, n_3\}$. For, by (14), there exist $x, y \in R^*$ such that

$$a_m x \equiv a_n y \pmod{K_s}, \tag{15}$$

$$b_m x \equiv b_n y \pmod{K_s}. \tag{16}$$

These congruences may be written

$$v((a_m x - a_n y)(a_m x)^{-1}) \geqslant s, \tag{17}$$

$$v((b_m x - b_n y)(b_m x)^{-1}) \geqslant s. \tag{18}$$

By (12), $v(b_m a_m^{-1}) = -h$, so that (18) may be rewritten as

$$v((b_m x - b_n y)(a_m x)^{-1}) \geqslant s - h. \tag{19}$$

Using (17), (19), and (13) we now find

$$\begin{aligned}
&v([(b_m - a_m)x - (b_n - a_n)y][(b_m - a_m)x]^{-1}) \\
&\quad = v(b_m x - a_m x - b_n y + a_n y) - v((b_m - a_m)x) \\
&\quad = v((a_m x - a_n y)(a_m x)^{-1} - (b_m x - b_n y)(a_m x)^{-1}) + v(a_m x) - v((b_m - a_m)x) \\
&\quad \geqslant \min\{v((a_m x - a_n y)(a_m x)^{-1}),\ v((b_m x - b_n y)(a_m x)^{-1})\} - v((b_m - a_m)a_m^{-1}) \\
&\quad \geqslant \min\{s, s-h\} - k = r;
\end{aligned}$$

hence

$$(b_m - a_m)x \equiv (b_n - a_n)y \pmod{K_r}. \tag{20}$$

Now $k > 0$; hence $s \geqslant r+k > r$ and so we deduce from (16)

$$b_m x \equiv b_n y \pmod{K_r}. \tag{21}$$

The congruences (20) and (21) hold for any m, $n > n_0$; taken together they imply (11) and the lemma is established.

Thus θ is a mapping from a dense subset of G_1 into G_1 such that $\lim u_n\theta$ exists whenever $u_n \to u$. Taking into account that G_1 satisfies the first axiom of countability (so that its topology may be defined by sequences) and that G is regular, we may extend θ in a unique manner to a continuous mapping of G_1 into itself [cf. Bourbaki (**2**) 38]; this extension will again be denoted by θ.

Now let $a \in R^*$ and consider the element $(-a)a^{-1}$ of G. If b is any other element of R^* and $n > 0$, then there exist x, $y \in R^*$ such that

$$v(ax-by)-v(ax) \geqslant n;$$

hence

$$v((-a)x-(-b)y)-v((-a)x) \geqslant n$$

and we conclude that

$$(-a)a^{-1} \equiv (-b)b^{-1} \pmod{K_n}$$

for all $n > 0$, in other words, $(-a)a^{-1} = (-b)b^{-1} = e$, say.

We complete the proof of the theorem by showing that G satisfies the conditions of Lemma 3.1, with the θ and e just defined.

(i) If $ab^{-1} \in U_1$ and $c \in R^*$, then

$$(cab^{-1}c^{-1})\theta = (ca(cb)^{-1})\theta = (cb-ca)(cb)^{-1}$$
$$= c(b-a)b^{-1}c^{-1} = c(ab^{-1})\theta c^{-1}.$$

Thus we have

$$(cxc^{-1})\theta = c(x\theta)c^{-1} \tag{22}$$

for all $x \in U_1$ and $c \in R^*$; by continuity (22) holds for $c \in R^*$ and any $x \in G_1$. Replacing x by $c^{-1}xc$ in (22) we obtain $x\theta = c((c^{-1}xc)\theta)c^{-1}$, i.e.

$$(c^{-1}xc)\theta = c^{-1}(x\theta)c \quad (c \in R^*,\ x \in G_1). \tag{23}$$

Combining (22) and (23) we have

$$(ab^{-1}x(ab^{-1})^{-1})\theta = ab^{-1}(x\theta)(ab^{-1})^{-1} \quad (x \in G_1,\ a, b \in R^*),$$

and hence, again by continuity,

$$(yxy^{-1})\theta = y(x\theta)y^{-1} \quad (x \in G_1,\ y \in G).$$

(ii) Let $ab^{-1} \in U_1$, then $a \neq b$ and $(ab^{-1})\theta = (b-a)b^{-1}$, hence

$$(ab^{-1})\theta^2 = ((b-a)b^{-1})\theta = ab^{-1}.$$

Thus (ii) holds on U_1, and by continuity on G_1. Similarly, we have

$$(ba^{-1})\theta . ab^{-1}((ab^{-1})\theta)^{-1}$$
$$= (a-b)a^{-1}ab^{-1}b(b-a)^{-1} = (-(b-a))(b-a)^{-1} = e;$$

hence $(x^{-1}\theta)x(x\theta)^{-1} = e$ for any $x \in G_1$, i.e. (iii).

(iv) We first note that for any $c \in R^*$, the set $cU = \{cab^{-1} \mid a, b \in R^*\}$ is dense in G. For, given $u \in G$ and $n > 0$, there exist $a, b \in R^*$ such that $u \equiv ab^{-1} \pmod{K_n}$. If x and y are chosen in R^* to satisfy $ax \equiv cy \pmod{K_n}$ then $ab^{-1} \equiv cy(bx)^{-1} \pmod{K_n}$ and hence

$$u \equiv cy(bx)^{-1} \pmod{K_n}$$

with $cy(bx)^{-1} \in cU$. Similarly, Uc^{-1} is dense in G. Now let $x, y \in G_1$ $(x \neq y)$. We can find a sequence $(c_n d_n^{-1})$ in U_1 which converges to y and elements a_n, $b_n \in R^*$ such that $a_n \neq c_n b_n$, $a_n \neq d_n b_n$ and $a_n(d_n b_n)^{-1} \to x$. If we put $a_n(d_n b_n)^{-1} = x_n$ and $c_n d_n^{-1} = y_n$, then $x_n y_n^{-1} = a_n(c_n b_n)^{-1}$ and

$$(x_n y_n^{-1})\theta = [x_n \theta(y_n \theta)^{-1}]\theta . (y_n^{-1})\theta,$$

as is easily verified. As $n \to \infty$, $x_n \to x$, and $y_n \to y$, hence

$$\lim(x_n \theta(y_n \theta)^{-1}) \neq 1,$$

and we obtain $$(xy^{-1})\theta = [x\theta(y\theta)^{-1}]\theta . (y^{-1})\theta.$$

Thus all the conditions of Lemma 3.1 are satisfied; hence we obtain a field K whose multiplicative group is G; in adjoining 0 to G (to obtain K) we may clearly use the zero-element of R. Then R, as multiplicative semigroup, is a subsemigroup of K. Let us denote the subtraction in K by $x \dot{-} y$ for the moment. By Lemma 3.1, we have

$$1 \dot{-} x = x\theta \quad (x \neq 0, 1).$$

In particular, if $x = ab^{-1} \in U_1$, then

$$1 \dot{-} ab^{-1} = (ab^{-1})\theta = (b-a)b^{-1}.$$

Multiplying both sides by b on the right, we find

$$b \dot{-} a = b - a. \tag{24}$$

If $a = b$, then the two sides of (24) are 0; for $b = 0$ they reduce to $-a$, by the definition of e, while for $a = 0$ they both reduce to b. Thus (24) holds for all a, $b \in R$. Hence the additive group of R is a subgroup of the additive group of K, i.e. R is a subring of K. This completes the proof of Theorem 4.1.

Let R be a filtered ring, i.e. a ring with a descending series

$$\ldots \supseteq R_{-1} \supseteq R_0 \supseteq R_1 \supseteq \ldots$$

of submodules such that $\bigcap R_n = 0$, $\bigcup R_n = R$, and $R_m R_n \subseteq R_{m+n}$. Then we can define a function v on R by putting

$$v(x) = \sup\{n \mid x \in R_n\}; \tag{25}$$

v satisfies the properties V.1, V.3 of valuations, while V.2 is replaced by

V.2′ $$v(xy) \geqslant v(x) + v(y).$$

Thus we have a *pseudo-valuation* on R. Conversely, any ring R with a pseudo-valuation v may be filtered by the submodules

$$R_n = \{x \in R \mid v(x) \geqslant n\}. \tag{26}$$

Now with any filtered ring R there is associated a graded ring $G(R)$ whose additive group is the direct sum $\sum (R_n/R_{n+1})$ and whose multiplication is induced by that of R [cf. (7), exposé 1]. It is not hard to verify that the function $v(x)$ defined on a filtered ring R by (25) is a valuation if and only if the graded ring $G(R)$ has no zero-divisors. In this case the hypotheses of Theorem 4.1 may be reformulated as follows.

THEOREM 4.2. *Let R be a ring with a valuation v; then the following three conditions are equivalent*:

(i) *For any a, $b \in R^*$ there exist x, $y \in R^*$ such that*

$$v(ax-by) > v(ax),$$

(ii) *for any a, $b \in R^*$, the function*

$$f(x,y) = v(ax-by)-v(ax) \tag{27}$$

is unbounded above,

(iii) *the graded ring $G(R)$ associated with R satisfies the Ore conditions.*

Proof. We note that (i) is a special case of (ii); (i) also follows directly from (iii), for if $a, b \in R^*$ and $\bar{a}$, $\bar{b}$ are the corresponding elements of $G(R)$, then by (iii) there exist x, $y \in R^*$ such that

$$\overline{ax}-\overline{by} = 0,$$

i.e. $v(ax-by) > v(ax)$. To complete the proof it remains to show that (i) implies (ii) and (iii).

(i) $\Rightarrow$ (ii). Let $a, b \in R^*$ and suppose that the function $f(x,y)$ given by (27) is bounded; let x, $y \in R^*$ be such that $f(x,y)$ has its maximum value. If $c = ax-by$, then $c \neq 0$, because $v(c)-v(ax)$ is finite. By (i), there exist u, $v \in R^*$ such that $v(cu-bv) > v(cu)$, i.e.

$$v(axu-b(yu+v)) > v(axu-byu).$$

It follows that

$$v(axu-b(yu+v))-v(axu) > v(axu-byu)-v(axu) = v(ax-by)-v(ax);$$

thus

$$f(xu, yu+v) > f(x,y),$$

which contradicts the definition of x and y.

(i) $\Rightarrow$ (iii). Let $a, b \in G(R)$, say

$$a = a_{k+1}+\ldots+a_{k+r},$$
$$b = b_{l+1}+\ldots+b_{l+s},$$

where a_i, $b_i \in R_i/R_{i+1}$ and a_{k+1}, a_{k+r}, b_{l+1}, b_{l+s} are all different from zero. When $r+s \leqslant 2$, the result holds by hypothesis, so we may assume that

$r+s > 2$ and use induction on $r+s$; further we may assume that $r \leqslant s$, without loss of generality. By hypothesis there exist homogeneous elements x, y in $G(R)$ which are not zero and satisfy

$$a_{k+1}x = b_{l+1}y.$$

The element $a_{k+1}x$ is again homogeneous and belongs to R_m/R_{m+1} say; since $r \leqslant s$, the only degrees for which $ax-by$ can have non-zero terms are $m+1,..., m+s-1$. By the induction hypothesis $ax-by$ and a have a non-zero common right multiple, say

$$(ax-by)u = av \neq 0;$$

hence $a(xu-v) = byu$, and this is not zero because $b, y, u \in G(R)^*$. Thus (iii) holds and the proof is complete.

Now we obtain the result stated in the introduction by combining Theorems 4.1 and 4.2.

THEOREM 4.3. *If R is a filtered ring such that the associated graded ring $G(R)$ satisfies the Ore conditions, then R can be embedded in a field.*

For when R is as stated, $G(R)$ has no zero-divisors, and therefore the filtration on R leads to a valuation; now we reach the conclusion by applying first Theorem 4.2 and then Theorem 4.1.

We also note the

COROLLARY. *If R is a filtered ring such that the associated graded ring $G(R)$ is a commutative integral domain, then R can be embedded in a field.*

5. Birkhoff-Witt algebras

A linear associative algebra A over a commutative field F is said to be a *Birkhoff–Witt algebra* (BW-algebra for short) if it has a filtration

$$0 = A_{-1} \subseteq A_0 \subseteq A_1 \subseteq ...$$

such that the associated graded algebra $\sum (A_n/A_{n-1})$ is isomorphic—as graded algebra—to a polynomial ring in a number of indeterminates over F. By Theorem 4.3, Corollary, every BW-algebra can be embedded in a field. We need only put

$$R_n = A_{-n} \quad (A_{-1} = A_{-2} = ... = 0)$$

to reach agreement with the notation used in § 4.

In the present section we shall study BW-algebras and show to what extent they generalize the concept of Birkhoff–Witt rings as used, e.g., by Tamari (**14**).

Let A be a BW-algebra over F; then $A_0 \cong F$ (*qua* algebra over F) and if e is the element of A_0 which corresponds to the unit-element of F under this isomorphism, while u_λ ($\lambda \in \Lambda$) is a set of elements of A_1 whose residue-classes mod A_0 form a basis of A_1/A_0, then A is generated by the elements e and u_λ ($\lambda \in \Lambda$) with the relations

$$e^2 = e, \tag{1}$$

$$eu_\lambda = u_\lambda + \alpha_\lambda e, \tag{2}$$

$$u_\lambda e = u_\lambda + \beta_\lambda e, \tag{3}$$

$$u_\lambda u_\mu - u_\mu u_\lambda = \sum \gamma_{\lambda\mu}^{\nu} u_\nu + \epsilon_{\lambda\mu} e, \tag{4}$$

where $\alpha_\lambda, \beta_\lambda, \gamma_{\lambda\mu}^{\nu}, \epsilon_{\lambda\mu} \in F$. If we multiply (2) by e on the left and use (1) we obtain

$$eu_\lambda = eu_\lambda + \alpha_\lambda e,$$

hence $\alpha_\lambda = 0$ and similarly $\beta_\lambda = 0$. Thus e is the unit-element of A and will henceforth be denoted by 1. Now (4) shows that mod A_0, A_1 admits the operation

$$[x, y] = xy - yx; \tag{5}$$

thus (5) may be used to define a bilinear multiplication on the space A_1/A_0. The resulting linear algebra is easily seen to be a Lie algebra, with basis u_λ ($\lambda \in \Lambda$) and structure constants $\gamma_{\lambda\mu}^{\nu}$. We denote this Lie algebra by L and on L define a bilinear form $b(x, y)$ by putting

$$b(u_\lambda, u_\mu) = \epsilon_{\lambda\mu}.$$

It follows from (4) and the linear independence of u_λ and e that b is an alternating form, i.e.

$$b(x, x) = 0 \quad (x \in L).$$

If we denote the multiplication in L by $[xy]$, we can rewrite (4) as

$$xy - yx = [xy] + b(x, y)1 \quad (x, y \in L), \tag{6}$$

and using this relation to express the Jacobi-identity in L we find that

$$b([xy], z) + b([yz], x) + b([zx], y) = 0. \tag{7}$$

An alternating bilinear form on a Lie algebra will be called *invariant* if it satisfies (7). Thus any BW-algebra A leads to a Lie algebra L with an invariant alternating bilinear form b defined on it,† and A is completely determined by L and b.

Conversely, let L be any Lie algebra over F with an invariant alternating bilinear form b defined on it. Then the associative algebra with unit-element 1 which is generated by the elements of L with the relations (6) is a BW-algebra which in turn leads to L with b as its invariant form. For the special case $b = 0$ this was proved by Birkhoff (**1**) and Witt (**15**). The proof in the general case is entirely analogous and will therefore be omitted.

† A may equally well be associated with a central extension of L by a one-dimensional algebra. The above definition seems more natural in the present context.

We shall denote the BW-algebra for a given Lie algebra L with invariant form b by $A(L;b)$. As special cases we note:

1. The associative enveloping algebra of a Lie algebra L, namely, $A(L;0)$. This is the algebra constructed by Birkhoff and Witt.

2. The free associative algebra X over F on $x_1,\ldots, x_r$ as free set of generators. X may be regarded as a Lie algebra, using the operation (5), and if L is the Lie algebra (in this sense) generated by $x_1,\ldots, x_r$ then $X \cong A(L;0)$. Taken together with Theorem 4.3, this provides another proof of the fact that X may be embedded in a field [cf. Mal'cev (**9**), Neumann (**10**)].

3. The 'Hamilton–Jacobi algebra' of quantum mechanics, defined by the generators $p_1,\ldots, p_n, q_1,\ldots, q_n$ and the defining relations

$$p_i q_j - q_j p_i = \delta_{ij}, \quad p_i p_j = p_j p_i, \quad q_i q_j = q_j q_i \qquad (i,j = 1,\ldots,n),$$

where δ_{ij} is the Kronecker delta. This is of the form $A(L;b)$, where L is an abelian Lie algebra of dimension $2n$ and b is any non-degenerate alternating bilinear form on L.

Let A be any BW-algebra and u_λ $(\lambda \in \Lambda)$ any set of elements which forms a basis of $A_1 \pmod{A_0}$. For simplicity we take Λ to be totally ordered. The algebra A is then spanned by the monomials

$$u_I = u_{i_1} \ldots u_{i_n} \quad (n \geqslant 0); \tag{8}$$

moreover, we may limit the suffix-sets $I = (i_1,\ldots, i_n)$ to be ascending, i.e.

$$i_1 \leqslant i_2 \leqslant \ldots \leqslant i_n. \tag{9}$$

If $n = 0$, u_I is interpreted as the unit-element of A. As in the special case $b = 0$ discussed by Birkhoff and Witt, the algebra $A(L;b)$ has a basis consisting of all u_I, where I runs over all ascending suffix sets. Our results may be summed up as follows:

THEOREM 5.1. *Let L be a Lie algebra over a commutative field F and b an invariant alternating bilinear form on L. Then the associative algebra $A = A(L;b)$ generated by the elements of L and 1 with the defining relations*

$$xy - yx = [xy] + b(x,y)1 \quad (x, y \in L)$$

is a Birkhoff–Witt algebra, and conversely, every Birkhoff–Witt algebra is of this form.

Moreover, if u_λ $(\lambda \in \Lambda)$ is a totally ordered basis of L, then the monomials u_I with ascending suffix-sets I (as in (9)) form a basis of A.

6. The embedding theorem for locally finite BW-algebras

A Lie algebra L is said to be *locally finite* if every finite subset of L is contained in a finite-dimensional subalgebra of L. Analogously a

BW-algebra $A(L;b)$ is called *locally finite* if the underlying Lie algebra L is locally finite. If L is actually finite-dimensional, $A(L;b)$ will be called *finite*.

Tamari has shown in (**14**), by a direct computation, that every locally finite BW-algebra of the form $A(L;0)$ satisfies the Ore conditions, and therefore has a field of right quotients. Now it has recently been proved by Goldie (**5**) that the Ore conditions hold in any ring without zero-divisors in which the right ideals satisfy the ascending chain condition. In view of this fact it is of interest to rederive Tamari's result by showing that any finite BW-algebra satisfies the ascending chain condition for right ideals, or equivalently, that its right ideals are finitely generated. For enveloping algebras of finite-dimensional Lie algebras this fact has been noted by Cartier [cf. (**7**), exposé 1], who obtains it as a corollary of the Hilbert basis theorem. Below it is proved by a direct method (Theorem 6.2).

THEOREM 6.1 (Goldie). *Any ring without zero-divisors whose right ideals are finitely generated has a field of right quotients.*

As this theorem is proved by Goldie in a more general context, we include a direct proof.

By Ore's result we need only show that for any a, $b \in R^*$, we have $aR \cap bR \neq 0$. We denote by R^1 the ring obtained by adjoining a unit-element to R (in case none exists in R). Now consider the right ideal $\mathfrak{r}$ of R generated by the elements $b^n a$ $(n = 0, 1,...)$; by hypothesis this ideal is finitely generated, say

$$\mathfrak{r} = (a, ba,..., b^k a).$$

Hence $$b^{k+1}a = ax_0 + bax_1 + ... + b^k a x_k \quad (x_i \in R^1),$$

and multiplying by a on the right, we obtain

$$b^{k+1}a^2 = ay_0 + bay_1 + ... + b^k a y_k \quad (y_i \in R). \tag{1}$$

Since the left-hand side is not zero, the y_i are not all zero. Let $i = h$ be the first suffix for which $y_i \neq 0$; cancelling the left factor b^h from (1) we obtain

$$b^{k+1-h}a^2 = ay_h + ... + b^{k-h}ay_k,$$

and hence $$ay_h = b(b^{k-h}a^2 - ay_{h+1} - ... - b^{k-h-1}ay_k). \tag{2}$$

Since $y_h \neq 0$, this is the required common right multiple of a and b.

COROLLARY. *A ring R has a field of right quotients provided that in every two-generator subring of R there are no zero-divisors and the right ideals are finitely generated.*

For by Theorem 6.1 this is enough to ensure that the Ore conditions hold for R.

It would be of interest to know if the sufficient condition of this corollary is also necessary, i.e. if in every ring which satisfies the Ore conditions the two-generator subrings have the finite basis property for right ideals.

Let $A = A(L;b)$ be a finite BW-algebra and let $x_1,\dots, x_k$ be a basis of L. Then a basis of A is given by the elements

$$x^a = x_1^{a_1} \dots x_k^{a_k}, \tag{3}$$

where $a_1,\dots, a_k$ are any non-negative integers. We write $|a| = \sum a_i$ and note

LEMMA 1. $$x^a x^b \equiv x^c \pmod{A_{r-1}},$$
where $c_i = a_i + b_i$ *and* $r = |c|$.

This follows immediately from the definition of A as a BW-algebra.

The k-tuples $a = (a_1,\dots, a_k)$ of integers may be partially ordered by writing
$$a \leqslant b \quad \text{if and only if } a_i \leqslant b_i \quad (i = 1,\dots, k).$$
A sequence of k-tuples a^1, a^2,... is said to be in *ascending order* if
$$a^1 \leqslant a^2 \leqslant \dots.$$
Then we have†

LEMMA 2. *Any infinite sequence of k-tuples contains an infinite ascending subsequence.*

For from any infinite sequence of k-tuples we can select an infinite subsequence whose first components are in ascending order, and by induction on k complete the proof.

In particular, it follows from Lemma 2 that any sequence of k-tuples a^ν such that
$$a^\mu \not\leqslant a^\nu \quad \text{for } \mu < \nu$$
must terminate.

As we saw, any finite BW-algebra $A(L;b)$ has a basis consisting of monomials x^a, where $x_1,\dots, x_k$ is a basis of L. We call $|a|$ the *degree* of x^a and order the monomials of the same degree lexicographically. Now the elements of A may be assigned a degree in the usual way, and for any $f \in A$ of degree $n \geqslant 0$ (i.e. $f \neq 0$), the last monomial term of degree n which has a non-zero coefficient is called the *leading term* of f. If this coefficient is 1 then f is said to be *monic*.

THEOREM 6.2. *In any finite BW-algebra the right ideals are finitely generated.*

Proof. Let $A = A(L;b)$ be a finite BW-algebra and let $x_1,\dots, x_k$ be a basis of L. Consider any right ideal $\mathfrak{r}$ of A; clearly $\mathfrak{r}$ is generated by its monic elements. These elements may be ordered by increasing degree

† Cf. Higman (6) for Lemma 2 and its proof.

and those of the same degree by their leading term. Since all possible terms (3) when taken in this order, form a countably well-ordered set, $\mathfrak{r}$ has a generating set of monic elements $f_1, f_2, \ldots$ such that for any n, $f_n \notin (f_1, \ldots, f_{n-1})$. We merely write down the sequence of all monic elements of $\mathfrak{r}$ and successively cross out redundant ones. If a^ν is the exponent of the leading term of f_ν, it follows that

$$a^\mu \not\leqslant a^\nu \quad \text{for } \mu < \nu. \tag{4}$$

For if $a^\mu \leqslant a^\nu$ then $a_i^\nu = a_i^\mu + b_i$ $(i = 1, \ldots, k)$ and $f_\nu - f_\mu x^b$ would have an earlier leading term than f_ν, by Lemma 1, and therefore belong to $(f_1, \ldots, f_{\nu-1})$. But then $f_\nu \in (f_1, \ldots, f_{\nu-1})$ because $\mu \leqslant \nu - 1$, and this contradicts the definition of f_ν. Now (4), with the remark following Lemma 2, shows that the sequence $f_1, f_2, \ldots$ terminates, i.e. $\mathfrak{r}$ is finitely generated, as we wished to show.

We note that this theorem, together with Lemma 2 which is used in proving it, provides another proof of the Hilbert basis theorem for polynomial rings.

It is easy to see that a BW-algebra has no zero-divisors. For by Lemma 1, the leading term of a product is the product of the leading terms.† Thus combining Theorems 6.2 and 6.1 we see that any finite BW-algebra has a field of right quotients. More generally, in a locally finite BW-algebra, any two elements belong to the subalgebra generated by a finite-dimensional Lie algebra, and hence belong to a subalgebra with finite basis property for right ideals. Applying Theorem 6.1, Corollary, we see that any locally finite BW-algebra has a field of right quotients.

Again it would be interesting to know if every BW-algebra possessing a field of right quotients is necessarily locally finite. It is easy to give examples of BW-algebras which do *not* possess a field of right quotients (and hence cannot be locally finite). We need only take the free associative algebra on r $(\geqslant 2)$ free generators. As remarked in § 5, this is of the form $A(L; 0)$, but it clearly does not satisfy the Ore condition since distinct generators cannot have a common right multiple other than zero.

Added in proof (30 *December* 1960). The answer to the question at the top of p. 528 is obviously 'no'. Let A be the free associative algebra on x and y over F and K a field containing A (whose existence was proved in § 5). Then K satisfies the Ore conditions, but the subring generated by x and y does not have the finite basis property for right ideals.

† Cf. also Theorem 4.3, Corollary.

REFERENCES

1. G. Birkhoff, 'Representability of Lie algebras and Lie groups by matrices', *Ann. of Math.* 38 (1937) 526–32.
2. N. Bourbaki, *Topologie générale*, chs. i–ii (Paris, 1940).
3. P. Dubreil, 'Sur les problèmes d'immersion et la théorie des modules', *C.R. Acad. Sci.* (*Paris*) 216 (1943) 625–7.
4. S. Eilenberg and N. Steenrod, *Foundations of algebraic topology* (Princeton, 1952).
5. A. W. Goldie, 'The structure of prime rings under ascending chain conditions', *Proc. London Math. Soc.* (3) 8 (1958) 589–608.
6. G. Higman, 'Ordering by divisibility in abstract algebras', ibid. (3) 2 (1952) 326–36.
7. Séminaire 'Sophus Lie' (première année 1954/5), Paris, 1955.
8. A. I. Mal'cev, 'On the immersion of an algebraic ring into a field', *Math. Ann.* 113 (1937) 686–91.
9. —— 'On the embedding of group algebras in division algebras' (Russian), *Doklady Akad. Nauk SSSR* (*N.S.*) 60 (1948) 1499–1501.
10. B. H. Neumann, 'On ordered division rings', *Trans. Amer. Math. Soc.* 66 (1949) 202–52.
11. O. Ore, 'Linear equations in non-commutative fields' *Ann. of Math.* (2) 32 (1931) 463–77.
12. D. G. Rabinow, 'Independent sets of postulates for abelian groups and fields in terms of the inverse operations', *Amer. J. Math.* 59 (1937) 211–24.
13. O. F. G. Schilling, *The theory of valuations* (New York, 1950).
14. D. Tamari, 'On the embedding of Birkhoff–Witt rings in quotient fields', *Proc. Amer. Math. Soc.* 4 (1953) 197–202.
15. E. Witt, 'Treue Darstellung Liescher Ringe', *J. reine angew. Math.* 177 (1937) 152–60.

The University
Manchester 13