PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 105, Number 1, January 1989

DISTRIBUTIVE FACTOR LATTICES IN FREE RINGS

P. M. COHN

(Communicated by Donald S. Passman)

ABSTRACT. For any field E with subfield k the free E-ring over k on a set X, $R = E_k\langle X\rangle$ is a fir. It is proved here that when E/k is purely inseparable, then the submodule lattice R/cR is distributive, for any $c \neq 0$ (R has distributive factor lattice); by contrast this is false when E/k is a nontrivial Galois extension and $X \neq \varnothing$.

1. INTRODUCTION

Let E be a skew field containing a subfield k in its centre. By the *free E-ring* over k on a set X one understands the ring $E_k\langle X\rangle$ generated by E and X with the defining relations

$$\alpha x = x\alpha \quad \text{for all } x \in X,\ \alpha \in k.$$

In particular, when $E = k$, one also writes $k\langle X\rangle$ and speaks of the *free k-algebra*. Free E-rings form an example of firs [5], but the free k-algebras also have other properties not shared by all firs. In particular the author conjectured in the early 1960s that $k\langle X\rangle$ has distributive factor lattice (see §2), and this was proved by G. M. Bergman in his thesis [1]; (see also [5, p. 208]). Moreover, in 1966 Bergman sent the author a 23 page manuscript which included a proof that $E_k\langle X\rangle$ has distributive factor lattice whenever E/k is a purely inseparable commutative field extension, and here the inseparability cannot be omitted. This proof was never published. In 1981 the author, using results of Bergman [2], found another shorter proof, and it is the object of this note to present this proof.

In the proof it is convenient to use the notion of a *conservative semifir* (defined in §2), in analogy with the conservative 2-fir introduced in the first edition of [5], (the term has a similar connotation in field theory, cf. [7]). In the terminology of [5], recalled below in §2, a conservative semifir is a persistent semifir R such that $R[t]$ is fully inert in $R \otimes k(t)$ (for a central indeterminate t).

Received by the editors February 5, 1988.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 16A06.
Contents was presented to the workshop on 'The Theyro of Rings' Warsaw, Poland, on March 28, 1988, organized by the Stefan Banach Math. Center.

0002-9939/89 $1.00 + $.25 per page

Now Dicks and Sontag have in [6] studied the class of rings satisfying Sylvester's law of nullity, under the name 'Sylvester domains', and they have shown in particular that for any free algebra $R = k\langle X\rangle$, the polynomial ring $R[t]$ is a Sylvester domain (cf. Theorem 5.5.12, p. 260 of [5]). Further, a connexion between conservative semifirs and Sylvester domains was established in [4], where the following result was proved.

Theorem 1.1. *In any ring R, each of the following properties implies the next:*

(a) *R is a conservative semifir;*
(b) *$R[t]$ is a Sylvester domain;*
(c) *R is a semifir with distributive factor lattice.*

In particular, this shows again that every conservative semifir has distributive factor lattice. Of course neither of the implications in the theorem can be reversed, as examples (loc. cit.) show.

Any free algebra $k\langle X\rangle$ is easily seen to be a conservative semifir, so the above theorem provides another proof that $k\langle X\rangle$ has distributive factor lattice.

After a preliminary section to explain the terminology we prove in §3 that for any purely inseparable commutative field extension E/k the free ring $E_k\langle X\rangle$ is a conservative semifir and so has distributive factor lattice. In §4 we give a representation of the free ring associated with a Galois extension and use it to give examples of free rings not possessing distributive factor lattice. I wish to thank G. M. Bergman, W. Dicks and the referee for pointing out flaws in earlier versions and in some cases suggesting remedies.

2. Preliminaries

We begin by recalling notation, terminology and results needed in the sequel. All our rings are associative, with a unit-element which is preserved by homomorphisms, inherited by subrings and which acts unitally on modules. A ring in which the nonzero elements form a nonempty set closed under multiplication is called an *integral domain* (not necessarily commutative). The group of units in any ring R is denoted by $\mathbf{U}(R)$.

If R is any ring, the set of all $m \times n$ matrices over R is denoted by ${}^mR^n$ and we write R^n for ${}^1R^n$ and ${}^mR$ for ${}^mR^1$. The ring of all $n \times n$ matrices over R is denoted by R_n or $\mathfrak{M}_n(R)$, and the group of all invertible $n \times n$ matrices is written $\mathbf{GL}_n(R)$. If A, B are any matrices over R, their *diagonal sum* $A \oplus B$ is defined by

$$A \oplus B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}.$$

A matrix C over a ring R is said to be *full* if it is square, say $n \times n$, and it cannot be written in the form $C = AB$, where $A \in {}^nR^r$, $B \in {}^rR^n$ and $r < n$.

Let R be a ring and R' a subring. An element c of R' is said to be *inert* in R if for every factorization $c = ab$, where $a, b \in R$, we can find a unit u in R such that $au, u^{-1}b \in R'$. If every nonzero element of R' is inert in R

we also say that R' is 1-*inert* in R. If every full matrix over R' is inert in the matrix ring over R we shall call R' *fully inert* in R.

We shall not repeat the definitions of fir and semifir (cf. [5]), but merely recall that if a product of matrices over a semifir R is zero, $AB = 0$, then this product can be *trivialized* in the sense that for some invertible matrix U, the first r columns of AU and all but the first r rows of $U^{-1}B$ are zero; the resulting relation $AU \cdot U^{-1}B = 0$ is said to be *trivial.*

A semifir R which is a k-algebra is said to be *persistent* over k if $R \otimes k(t)$ is again a semifir, and a *conservative* semifir is a persistent semifir R such that $R[t]$ is fully inert in $R \otimes k(t)$.

In any semifir (or even 2-fir) R the principal right ideals containing any fixed nonzero element form a modular lattice. If this lattice is actually distributive (for each nonzero element), R is said to have *distributive factor lattice* (DFL). We remark that the lattice of principal right ideals containing $c \neq 0$ can be interpreted as the lattice of left factors of c, ordered by divisibility. By the factorial duality valid in any integral domain (cf. 3.3, p. 166 of [5]), the condition DFL is left-right symmetric.

Every semifir R has a universal field of fractions U; this is a skew field with R as subring and it is generated as a skew field by R. It is characterized up to isomorphism by the fact that every full matrix over R becomes invertible over U (clearly a nonfull square matrix can never be mapped to an invertible matrix in any homomorphism to a field). We express this fact by saying that E has a *fully inverting homomorphism* to U. More generally, Dicks and Sontag have in [6] studied the precise class of rings which have a fully inverting homomorphism to a skew field. Such rings are called *Sylvester domains*, because they can also be characterized by a form of Sylvester's law of nullity, but we shall not need the explicit form of this law and may take the above as a definition. Dicks and Sontag also prove that for a commutative principal ideal domain P the free P-algebra $P\langle X\rangle$ is a Sylvester domain (cf. Theorem 5.5.12, p. 260 of [5]). This shows that for any free k-algebra $R = k\langle X\rangle$ (k a field), the polynomial ring $R[t] = k[t]\langle X\rangle$ is a Sylvester domain. This property will be generalized in Theorem 3.3 below.

3. Inertia for free E-rings

Our aim will be to show that for any purely inseparable field extension E/k the free ring $E_k\langle X\rangle$ is a conservative semifir. We begin by describing the structure of the tensor product by a purely inseparable extension. We shall use the notation $E[X|\Phi]$ for a commutative E-algebra with generators X and defining relations Φ.

Lemma 3.1. *Let E/k be a commutative field extension in finite characteristic p and let $F = k(\alpha)$, where α has the minimal polynomial $t^q - a$ over k, $q = p^r$. If $\alpha_1 = \alpha^s$ is the least power of α to lie in E and $q = ss'$, then*

$$E \otimes_k F = E[x, y | x^s = \alpha_1 - y,\ y^{s'} = 0]. \tag{1}$$

Proof. Regarded as E-space, $E \otimes F$ has the basis $1, x, x^2, \ldots, x^{q-1}$, where $x = 1 \otimes \alpha$. The defining relation is $x^q = a$; writing $y = \alpha_1 \otimes 1 - 1 \otimes \alpha_1$, we have $x^s = \alpha_1 \otimes 1 - y$, so the defining relation becomes

$$a = x^{ss'} = (\alpha_1 \otimes 1 - y)^{s'} = \alpha_1^{s'} - y^{s'} = a - y^{s'},$$

i.e. $y^{s'} = 0$, where we have used the fact that s' is a power of p. If we identify $c \otimes 1$ with $c \in E$, we thus obtain the presentation (1).

We next recall a result from [2]. In the form needed here it reads as follows, using $R *_k S$ to denote the ring coproduct of R, S over k:

Let R be an integral domain which is a k-algebra, and for any integer $q \geq 1$, write $S = k[y|y^q = 0]$. Then if $a, b \in R *_k S$ and $ab = 0$, we have

$$a = a_1 y^r u, \quad b = u^{-1} y^s b_1, \qquad r + s = q, \ u \in \mathbf{U}(R *_k S).$$

This follows from [2, Corollary 2.16], because R and S are both weakly 1-finite (i.e. $fg = 1$ implies $gf = 1$). Actually we shall need a slight variant of this result, generalized to matrices as follows:

Proposition 3.2. *Let R be a semifir which is a k-algebra, let $S = E \otimes_k F$ as in Lemma 1, and put $P = R *_k S$. Given $A, B \in P_n$, if $AB = 0$, then there exists $U \in \mathbf{GL}_n(P)$ such that $A = A_1 D_1 U$, $B = U^{-1} D_2 B_1$, where D_1, D_2 are diagonal matrices over S such that $D_1 D_2 = 0$.*

Proof. We recall from [2, Corollary 2.15] that $\mathbf{GL}_n(P)$ is generated by $\mathbf{GL}_n(R)$, $\mathbf{GL}_n(S)$ and by transvections based in R, S or k. Now A defines a homomorphism $\alpha: {}^nP \to {}^nP$, whose kernel contains the columns of B. By Corollary 2.17 of [2] we can apply an isomorphism λ to ${}^nP$ such that the kernel of $\alpha\lambda$ is in standard form, in terms of its restrictions to the components of ${}^nP$. Now over R any zero product of matrices can be trivialized (by the definition of semifir), while over S we obtain the stated decomposition.

We now come to the main result of this section.

Theorem 3.3. *Let E/k be a purely inseparable field extension. Then the free ring $R = E_k\langle X\rangle$ is a conservative semifir.*

Proof. We have $E \otimes_k k(t) = E(t)$; hence $E_k\langle X\rangle \otimes k(t) = E(t)_{k(t)}\langle X\rangle$ and this shows $E_k\langle X\rangle$ to be a presistent semifir (clearly this argument applies for any algebraic field extension E/k). It remains to show that $R[t]$ is fully inert in $R \otimes k(t)$.

Let C be a full $n \times n$ matrix over $R[t]$ which can be factorized over $R \otimes k(t)$; on clearing fractions in t, we obtain a relation

$$AB = fC, \qquad A, B, C \text{ over } R[t], \ f \in k[t]. \tag{1}$$

If f has a separable zero α, let F/k be a Galois extension containing α. Then $D = E \otimes_k F$ is a field and so

$$R_F = E_k\langle X\rangle \otimes_k F = D_F\langle X\rangle.$$

This is again a fir. The substitution $t \mapsto \alpha$ defines a homomorphism $\lambda: R[t] \to R_F$ which we shall write as $\lambda: c \mapsto \overline{c}$. Since $\overline{f} = 0$, we obtain from (1), $\overline{AB} = 0$, as an equation over R_F. Now R_F is free, hence a semifir, and so there is an invertible matrix U, which is a product of elementary matrices over R_F such that $\overline{A}U \cdot U^{-1}\overline{B} = 0$ is a trivial relation. Any elementary matrix can be lifted to $R[t]$; hence there is a matrix U_0 over $R[t]$, again product of elementary matrices, such that $\overline{U}_0 = U$. It follows that for some r, the first r columns of AU_0 and the last $n-r$ rows of $U_0^{-1}B$ are divisible by $t-\alpha$. But the entries of A, B, U_0 are in $R[t]$ and so are fixed under the action of the group $G = \mathrm{Gal}(F/k)$. It follows that the first r columns of AU_0 and the last $n-r$ rows of $U_0^{-1}B$ are also divisible by $t-\alpha'$, for any conjugate α' of α; hence these columns and rows are divisible by the minimal polynomial g of α over k. We replace A, B by $AV, V^{-1}B$, where $V = U_0(I_r \oplus gI_{n-r})$. Then AV is divisible by g, and in this way we can reduce the degree of f. We may thus assume that f has no separable zeros over k.

Secondly, consider the case where a zero α of f is purely inseparable over k, of degree q say. Writing $F = k(\alpha)$, we have

$$E_k\langle X\rangle \otimes F = (E \otimes_k F) *_F F\langle X\rangle,$$

and here $E \otimes F$ has the form described in Lemma 3.1. If λ is again the substitution homomorphism $t = \alpha$, we have $\overline{AB} = 0$; hence by Proposition 3.2,

$$\overline{A} = A_1 D_1 U, \qquad \overline{B} = U^{-1} D_2 B_1, \tag{2}$$

where U is invertible and D_1, D_2 are matrices over $E \otimes F$ such that $D_1 D_2 = 0$.

Let us write $S = E \otimes F$, $T = F\langle X\rangle$, so that $R_F = S *_F T$. We know from [2, Corollary 2.15] that $\mathbf{GL}_n(R_F)$ is generated by $\mathbf{GL}_n(S)$, $\mathbf{GL}_n(T)$ and transvections based in S, T or F. Since F and T are semifirs, their transvections are just elementary matrices [2, p. 9; 5, p. 75]. It follows that U is a product of elementary and diagonal matrices over S or T and transvections in S. Now any transvection in S can be written as a product of elementary matrices and diagonal transvections, because we have in S, as homomorphic image of the principal ideal domain $E[x]$, a diagonal reduction. In a diagonal transvection the diagonal elements have the form $1 + y^c a y^d$, where $c + d \geq s'$ and $a \in R_F$. Hence if P is any diagonal transvection, say $P = \mathrm{diag}(p_1, \ldots, p_n)$, where $p_i = 1 + y^{c_i} a_i y^{d_i}$ and $b \in R_F$, then

$$P^{-1}(I + be_{uv})P = I + (1 - y^{c_u} a_u y^{d_u}) b (1 + y^{c_v} a_v y^{d_v}) e_{uv}.$$

This shows that for any elementary matrix Q over R_F there is another elementary matrix Q' such that $QP = PQ'$; it follows that $U = PU_1$, where P is a product of diagonal transvections and U_1 is a product of elementary matrices over R_F. We replace U in (2) by PU_1 and obtain

$$\overline{A} = A_1 D_1 P U_1, \qquad \overline{B} = U_1^{-1} P^{-1} D_2 B_1.$$

We now lift U_1 to a product U_0 of elementary matrices over $R[t]$ and replace A, B by AU_0^{-1}, U_0B. Writing $D_3 = D_1P$, $D_4 = P^{-1}D_2$, we now have $\overline{A} = A_1D_3$, $\overline{B} = D_4B_1$, where D_3, D_4 are products of diagonal transvections in S and $D_3D_4 = 0$. Hence over $R[t]$ the product AB can be written

$$AB = A_2B_2(t-\alpha)^{s'} = fC.$$

Now we can cancel the factor $(t-\alpha)^{s'}$ and so reduce the degree of f.

In the general case let F be a Galois extension of k over which all the zeros of f are purely inseparable. Then $D = E \otimes_k F$ is a field and $R_F \cong D_F\langle X\rangle$. Suppose first that f is irreducible over k and that its different (possible multiple) zeros are $\alpha_1, \cdots, \alpha_\nu$, say $f = g_1 \cdots g_\nu$ where $g_i = (t-\alpha_i)^q$. By what has been proved, there is a matrix U over $R[t]$, product of elementary matrices, such that the first r columns of AU and the last $n-r$ rows of $U^{-1}B$ are divisible by g_1. Now A, B, U are fixed under the action of the Galois group $\mathrm{Gal}(F/k)$, while this group permutes the factors $g_1, \ldots, g_\nu$ of f transitively. Hence the first r columns of AU and the last $n-r$ rows of $U^{-1}B$ are also divisible by $g_1, \ldots, g_\nu$. Since the g_i are pairwise coprime, these columns and rows are divisible by $g_1g_2 \ldots g_\nu = f$. Writing again $V = U(I_r \oplus fI_{n-r})$, we find that $AV = fA_1$, $V^{-1}B = B_1$ and A_1, B_1 have entries in $R[t]$. Hence we obtain $fA_1B_1 = fC$ and $C = A_1B_1$ is the required factorization. If f is reducible, the same argument applied to each factor leads to the desired conclusion.

Applying Theorem 1.1 we obtain

Corollary 3.4. *If E/k is a purely inseparable field extension, then $E_k\langle X\rangle$ has distributive factor lattice.*

It would be interesting to know whether a generalization of Theorem 3.3 along the following lines holds (possibly under further hypotheses):

Let R be a k-algebra which is a semifir and remains one under all separable field extensions of k. Can one conclude that $R[t]$ is fully inert in $R \otimes k(t)$?

We observe that this is true with 'separable' replaced by 'algebraic', by Proposition 4.3.1, p. 205 and Example 4.3.4, p. 210 of [5].

4. The case of Galois extensions

Let us now consider the case of a Galois extension E/k. We shall then find that $E_k\langle X\rangle$ is not conservative unless $E = k$ or $X = \varnothing$, but some remarks on the structure of $E_k\langle X\rangle$ are necessary. We recall from [5, Theorem 2.2.4, p. 99] that $E_k\langle X\rangle$ is a fir. Further, for a Galois extension E/k of degree n it is well known (cf., e.g., [3, 6.10, Corollary 2, p. 246]), that

$$E \otimes_k E \cong E_1 \oplus E_2 \oplus \cdots \oplus E_n, \tag{1}$$

where the E_i are isomorphic copies of E. Explicitly, E_i is a free right E-module on one generator u_i such that $au_i = u_ia^{\sigma_i}$, where σ_i ranges over $\mathrm{Gal}(E/k)$.

Let M be an E-bimodule in which the two actions of k agree; we shall write $E_k\langle M\rangle$ for the tensor ring on M over E. The ambiguity arising from this double use of notation, $E_k\langle M\rangle$ and $E_k\langle X\rangle$, can usually be resolved by using different symbols for bimodules and free generating sets; thus $M = E \otimes_k E$ may be regarded as the free bimodule on one generator and we have

$$E_k\langle M\rangle = E_k\langle x\rangle, \quad \text{where } x = 1 \otimes 1 . \tag{2}$$

We also recall the well-known (and easily proved) formula

$$E_k\langle M \oplus N\rangle \cong E_k\langle M\rangle *_E E_k\langle N\rangle . \tag{3}$$

Let $G = \mathrm{Gal}(E/k)$ and for $\sigma \in G$ define a skew polynomial ring $A_\sigma = E[x_\sigma ; \sigma]$ with commutation rule $cx_\sigma = x_\sigma c^\sigma$ $(c \in E)$. Then it is clear that for the term E_i in (1), $E_k\langle E_i\rangle = A_{\sigma_i}$. Hence, using (2) and (3), we obtain

Theorem 4.1. *Let E/k be a Galois extension with group $G = \{\sigma_1, \ldots, \sigma_n\}$. Then*

$$E_k\langle x\rangle = A_{\sigma_1} *_E \cdots *_E A_{\sigma_n} . \tag{4}$$

To complete the argument we need a couple of lemmas.

Lemma 4.2. *Let R be a 2-fir with DFL and S a subring of R. If S is a 2-fir and $\mathbf{U}(S) = \mathbf{U}(R) \cap S$, then S again has DFL.*

Proof. If S fails to have DFL, then by Lemma 4.2.1, p. 200 of [5], there is an equation

$$uav + waz = 1 , \tag{5}$$

for some nonunit a of S. By hypothesis a is still a nonunit in R, so (5) shows that R cannot have DFL.

We also need to know under what conditions a skew polynomial ring over a field can have DFL. Let K be a skew field with an endomorphism α and an α-derivation δ (i.e. δ is additive and $(ab)^\delta = a^\delta b^\alpha + ab^\delta$). The skew polynomial ring $K[x ; \alpha, \delta]$ is defined as the ring of polynomials $\sum x^i a_i$ with the usual addition and commutation rule $cx = xc^\alpha + c^\delta$ $(c \in K)$.

Lemma 4.3. *Let $R = K[x ; \alpha, \delta]$ be a skew polynomial ring over a skew field K. Then R has DFL if and only if it is commutative, which is the case when K is commutative, $\alpha = 1$ and $\delta = 0$.*

Proof. It is clear that R is commutative precisely under the stated conditions, and then it has DFL (cf. [5, p. 202]). Conversely, if R has DFL, then no equation (5) with a nonunit a can hold, i.e. $uav + waz$ cannot be a unit. Now x is a nonunit and $ax - xa^\alpha = a^\delta$; hence $a^\delta = 0$ for all a, so $\delta = 0$. Similarly $x + 1$ is a nonunit and $a(x+1) - (x+1)a^\alpha = a - a^\alpha$, so $a^\alpha = a$ for all a, i.e. $\alpha = 1$. Finally, $x + c$ is a nonunit for any $c \in K$, and $a(x+c) - (x+c)a = ac - ca$, so $ac = ca$, and K must be commutative.

Corollary 4.4. *If E/k is a nontrivial Galois extension and x is an indeterminate, then $E_k\langle x\rangle$ does not have distributive factor lattice.*

For by Theorem 4.1, $E_k\langle x\rangle$ has a subring $A_\sigma = E[x_\sigma;\sigma]$, $\sigma \neq 1$, and no nonunit of A_σ becomes invertible in $E_k\langle x\rangle$. By Lemma 4.3, A_σ does not have DFL, and it is a principal ideal domain, hence a 2-fir. Therefore, by Lemma 4.2, $E_k\langle x\rangle$ also fails to have DFL.

It seems likely that a corresponding result holds for any nontrivial extension E/k that is not purely inseparable.

References

1. G. M. Bergman, *Commuting elements in free algebras and related topics in ring theory*, Thesis, Harvard Univ., 1967.
2. ____, *Modules over coproducts of rings*, Trans. Amer. Math. Soc. **200** (1974), 1–32.
3. P. M. Cohn, *Algebra* 2, Wiley, Chichester, 1977, Second edition in preparation.
4. ____, *Ringe mit distributivem Faktorverband*, Abh. Braunschweig. Wiss. Ges. **33** (1982), 35–40.
5. ____, *Free rings and their relations*, 2nd ed., London Math Soc. Monographs, no. 19, Academic Press, London, Orlando, 1985.
6. W. Dicks and E. D. Sontag, *Sylvester domains*, J. Pure Appl. Algebra **13** (1978), 243–275.
7. M. Eichler, *Einführung in die Theorie der algebraischen Zahlen und Funktionen*, Birkhäuser-Verlag, Basel, 1963.

Department of Mathematics, University College London, Gower Street, London WC1E 6BT, England