602.

Normal forms, factorizations and eigenrings in free algebras

Mark Roberts

Bedford College

Thesis submitted for the degree of Ph.D to the University of London. 1981.

Abstract

The rings considered in this thesis are the free algebras $k\langle X\rangle$ (k a commutative field) and the more general rings $K_k\langle X\rangle$ (K a skew field and k a subfield of the centre of K) given by the coproduct of K and $k\langle X\rangle$ over k. The results fall into two distinct sections.

The first deals with normal forms; using a process of linearization we establish a normal form for full matrices over $K_k\langle X\rangle$ under stable association. We also give a criterion for a square matrix A over a skew field K to be cyclic - that is, for $xI - A$ to be stably associated to an element of $K_k\langle X\rangle$ (here k = centre(K)).

The second section deals with factorizations and eigenrings in free algebras. Let k be a commutative field, E/k a finite algebraic extension and P a matrix atom over $k\langle X\rangle$. We show that if E/k is Galois then the factorization of P over $E\langle X\rangle$ is fully reducible; if E/k is purely inseparable then the factorization is rigid. In the course of proving this we prove a version of Hilbert's Theorem 90 for matrices over a ring R that is a fir and a k-algebra; namely that $H^1(\mathrm{Gal}(E/k), GL_n(R\otimes_k E))$ is trivial for any Galois extension E/k. We show that the normal closure F of the eigenring of an atom p of $k\langle X\rangle$ provides a splitting field for p (in the sense that p factorizes into absolute atoms in $F\langle X\rangle$). We also show that if k is any commutative field and D a finite dimensional skew field over k then there exists a matrix atom over $k\langle X\rangle$ with eigenring isomorphic to D.

Contents

Acknowledgements

I should like to thank my supervisor, Professor P.M. Cohn for his help throughout this thesis.

Also the SRC for financial support.

Chapter 1 Background

This chapter contains the necessary background material for the rest of the thesis. The results are given without proof; most of them can be found (with their proofs) in 'Free rings and their relations' [1] and these are given page references in the text.

§1 contains the basic definitions of n-firs, semifirs and firs.

§2 deals with the weak algorithm (a generalization of the Euclidean algorithm). The main result is that any ring satisfying the weak algorithm is a fir (Prop^n 2.1). We define tensor bimodules and show that any tensor bimodule satisfies the weak algorithm (Prop^n 2.2); we deduce that free algebras are firs.

In §3 we define non-commutative unique factorization domains (UFDs); any fir is a UFD (Prop^n 3.3). We define stable association and give some equivalent conditions for two elements to be stably associated (Prop^n 3.4).

In §4 we consider rings satisfying DFL, that is, rings in which the lattice of factorizations of any element is distributive; free algebras satisfy DFL and hence factorizations in free algebras may be described particularly simply.

In §5 we generalize the results of §3 to the case of matrices over semifirs. We show that a full matrix over a semifir can be associated uniquely with a particular kind of right module, called a torsion module, and that the set of torsion modules over a semifir forms a full abelian subcategory of the category of modules (Prop^n 5.1). If R satisfies a suitable chain condition (e.g. if R is a fir) we can use this to deduce a unique factorization theorem for matrices (Prop^n 5.5). We then consider relations between matrices of the form AB = CD and give equivalent conditions for two matrices to be stably associated (Prop^n 5.6).

In §6 we define the important idea of the eigenring of an element (or matrix). The main results are; (i) the eigenring of an atom in a 2-fir is a skew field (Prop^n 6.3) (ii) the eigenring of an element in a persistent 2-fir is algebraic over the ground field (Prop^n 6.4) (iii) every element in $k\langle X\rangle$ has a commutative eigenring (Cor^y to Prop^n 6.7). There are also versions of (i) and (ii) for matrices over semifirs.

§1. Free ideal rings

Def^n Let R be a ring. R is a right fir if every right ideal of R is free of unique rank (considered as a right R-module). R is a left fir if every left ideal is free of unique rank and R is a fir if it is both a right and left fir. ('fir' stands for free ideal ring.)

We note that firs are a special case of hereditary rings. It is not hard to prove that if R is a fir then every submodule of a free right R-module is again free; hence firs are exactly those hereditary rings all of whose projectives are free. We make weaker definitions as follows;

Def^n Let R be a ring and n a positive integer. Then R is an n-fir if every right ideal of R generated by at most n elements is free of unique rank. R is a semifir if R is an n-fir for all positive integers n.

Although this definition is phrased in terms of right ideals, we have defined an n-fir and not a 'right n-fir'. This is because the condition is in fact left-right symmetric; if R is an n-fir then every left ideal on at most n generators is free of unique rank. This symmetry of course extends to semifirs but does not hold for firs; there are examples of right firs that are not left firs.

In the commutative case (or more generally for Ore rings) a fir reduces to a principal ideal domain and a 2-fir to a Bezout domain. Since a Noetherian ring is Ore, the only firs that are Noetherian are PIDs; however, firs do satisfy an ascending chain condition;

<u>Prop^n 1.1</u> Let R be a fir. Then R satisfies the ascending chain condition on n-generator right ideals (where n is any fixed integer). ([1] p.49)

There is another property of firs we shall need to use. A ring R is <u>weakly finite</u> if, given any two square matrices over R A and B with $AB = I$, we have that $BA = I$.

<u>Prop^n 1.2</u> Let R be a fir. Then R is weakly finite.

Some examples of firs are;

(i) a PID is a fir

(ii) a skew field is a fir

(iii) the coproduct of firs over a skew field is a fir (and the coproduct of n-firs is an n-fir) ([3] p.106)

(iv) the power series ring $k\langle\langle X\rangle\rangle$ in a set of indeterminates X is a semifir but not a fir.

Some more examples of firs (including the rings we are most interested in, namely free algebras) are given in the next section.

§2. The weak algorithm

We recall the Euclidean algorithm for commutative rings. Let R be a commutative ring with a degree function d. Then R satisfies the Euclidean algorithm if the following statement holds;

(i) for all $a, b \in R$ with $d(a) \geqslant d(b)$ there exists $c \in R$ such that $d(a - bc) < d(a)$.

We wish to generalize this to non-commutative rings. We use something slightly weaker than a degree function;

Def^n Let R be an integral domain (not necessarily commutative). A filtration v on R is a map $R \to \mathbb{N}$ such that;

(i) $v(1) = 0$

(ii) $v(a-b) \leqslant \max(v(a), v(b))$

(iii) $v(ab) \leqslant v(a) + v(b)$.

For notational convenience we set $v(0) = -\infty$. If equality holds in (iii) v is a degree function.

Def^n Let R be a ring with a filtration v. A family (a_i) of elements of R is right v-dependent if one of the a_i is zero or if there exists b_i, almost all zero, such that

$$v(\sum a_i b_i) < \max(v(a_i) + v(b_i))$$

Def^n An element a of R is right v-dependent on the family (a_i) of elements of R if a is zero or if there exist b_i, almost all zero, such that

$$v(a - \sum a_i b_i) < v(a) \quad \text{while} \quad v(a_i) + v(b_i) \leqslant v(a).$$

Def^n A ring R with a filtration v satisfies the n-term weak algorithm (with respect to v) if for any right v-dependent set $a_1, a_2, \ldots, a_m$ $(m \leqslant n)$ with $v(a_1) \leqslant v(a_2) \leqslant \ldots \leqslant v(a_m)$ some a_i is right v-dependent on $a_1, a_2, \ldots, a_{i-1}$.

As in the case of n-firs, this condition is equivalent to the corresponding condition on the left. The ring R is said to satisfy the <u>weak algorithm</u> (with respect to v) if it satisfies the n-term weak algorithm for all positive integers n.

<u>Prop^n 2.1</u> Let R be a ring with a filtration. Then if R satisfies the n-term weak algorithm R is an n-fir and if R satisfies the weak algorithm R is a fir. ([1] p.72)

A class of rings satisfying the weak algorithm is provided by the idea of a tensor bimodule. Let K be a skew field and let M be a K-bimodule. Let M^r denote the tensor product (over K) of r copies of M, and define the <u>tensor K-ring on M</u>, denoted T(M), as

$$T(M) = M^0 \oplus M^1 \oplus M^2 \oplus \ldots \qquad (M^0 = K)$$

The addition on T(M) is the obvious component-wise operation and the multiplication is that induced by the isomorphism

$$M^r \otimes_K M^s = M^{r+s}$$

These definitions make T(M) into a ring. There is an obvious filtration v on T(M) defined as follows;

if $m = m_o + m_1 + \ldots + m_r \quad (m_i \in M^i,\ m_r \neq 0)$ then $v(m) = r$.

<u>Prop^n 2.2</u> Let v be the filtration on R = T(M) (as defined above). Then R satisfies the weak algorithm with respect to v and hence is a fir. ([1] p.82)

Free algebras can be constructed as tensor K-rings;

(i) Let k be a commutative field and X a set of indeterminates. Then the <u>free k-algebra on X</u>, denoted $k\langle X\rangle$, is the k-algebra universal for mappings of X into k-algebras. We can also construct it as a tensor ring; let M be the k-bimodule consisting of the direct sum of X copies of k. Then $k\langle X\rangle$ is T(M); hence $k\langle X\rangle$

satisfies the weak algorithm with respect to the filtration giving the value 1 to each element of X (in fact this filtration is a degree function). Thus $k\langle X\rangle$ is a fir.

(ii) More generally, let L be a skew field and k a subfield of the centre of L. Let M be the L-bimodule consisting of the direct sum of X copies of $L \otimes_k L$. Then T(M) is a fir, denoted $L_k\langle X\rangle$. The elements of $L_k\langle X\rangle$ can be thought of as sums of monomials involving elements of X and elements of L, where only the elements of k commute with X. The filtration (which is again a degree function) attaches the value r to the monomial

$$h_1 x_{f(1)} h_2 x_{f(2)} h_3 \cdots x_{f(r)} h_{r+1} \qquad (x_{f(i)} \in X,\ h_i \in L)$$

$L_k\langle X\rangle$ can be shown to be isomorphic to the coproduct (over k) of the free algebra $k\langle X\rangle$ and L.

Clearly case (i) is a special case of case (ii). In either case we call the value of the filtration the degree of the element. An element is <u>homogeneous</u> if it is the sum of monomials of the same degree (thus m is homogeneous of degree r if $m \in M^r$ in T(M)). By construction every element can be written uniquely as the sum of its homogeneous components; we define the <u>leading term</u> of an element f, denoted f^{ℓ}, to be the homogeneous component of f of greatest degree.

§3. Unique factorization domains

We start by defining a (non-commutative) unique factorization domain. Let R be an integral domain. An element a of R is an atom if in any factorization $a = bc$ exactly one of b and c is invertible. R is atomic if each non-zero element of R can be expressed as the product of a finite number of atoms. Two elements a and b of R are stably associated (denoted $a \sim b$) if the right R-modules R/aR and R/bR are isomorphic; stable association is clearly an equivalence relation on R.

Def^n A ring R is a unique factorization domain if;

(i) R is atomic

(ii) if $a = p_1 p_2 \cdots p_n$ and $a = q_1 q_2 \cdots q_m$ are two factorizations of an element a into atoms then $m = n$ and there exists a permutation σ such that $p_i \sim q_{\sigma(i)}$ $(i = 1, 2, \ldots, n)$.

We note that if R is commutative this does reduce to the definition of a commutative UFD, for then $R/aR \cong R/bR$ iff $aR = bR$.

A useful concept for dealing with UFDs (and one that extends to the more general case of factorizations of matrices; cf §5) is that of a strictly cyclic module. A right R-module M is strictly cyclic if $M \cong R/cR$ for some non-zerodivisor c of R. For a fixed integral domain R the set of strictly cyclic right R-modules (with R-module homomorphisms as morphisms) forms a category, denoted $\mathcal{C}_R$. We similarly define the category ${}_R\mathcal{C}$ of strictly cyclic left R-modules.

Prop^n 3.1 The categories $\mathcal{C}_R$ and ${}_R\mathcal{C}$ are dual. ([1] p.118)

Cor^y Let R be an integral domain and let a and b be non-zero elements of R. Then $R/aR \cong R/bR$ iff $R/Ra \cong R/Rb$.

This corollary justifies the antisymmetry in the definition of stable association given above.

<u>Prop^n 3.2</u> Let R be a 2-fir. Then $\mathcal{C}_R$ is a full abelian subcategory of $\mathcal{M}_R$, the category of right R-modules. ([1] p.120)

<u>Cor^y</u> Let R be a 2-fir and c a non-zero element of R. Then the set of strictly cyclic submodules of R/cR form a modular lattice.

The factorization properties of an element c of R are reflected in the subobjects (in $\mathcal{C}_R$) of R/cR, for if $c = ab$ then

$$R/cR = R/abR \supseteq aR/abR \cong R/bR \supseteq 0$$

Thus if we impose a chain condition of R so that the set of subobjects of R/cR form a modular lattice of finite height we can use the Jordan-Hölder Theorem (see e.g. [1] p.316) to deduce unique factorization in R.

<u>Prop^n 3.3</u> Let R be an atomic 2-fir. Then R is a UFD. ([1] p.120)

Using Prop^n 1.1 (in the case $n = 1$) we can deduce;

<u>Cor^y</u> Let R be a fir. Then R is a UFD.

Thus in particular the free algebras $k\langle X\rangle$ are UFDs. We now consider the relation of stable association in 2-firs.

<u>Def^n</u> Let R be a ring and let $ca = bd$ be a relation between elements of R. The relation is said to be

(i) <u>right comaximal</u> if $cR + bR = R$

(ii) <u>left comaximal</u> if $Ra + Rd = R$

(iii) <u>right coprime</u> if a and d have no common right factor

(iv) <u>left coprime</u> if b and c have no common left factor.

The relation is <u>comaximal</u> if it is both left and right comaximal

<u>coprime</u> if it is both left and right coprime.

It is easily seen that any comaximal relation is coprime; in a 2-fir the converse is also true. We also note that in any relation in a 2-fir we can cancel left and right factors to get a coprime relation.

<u>Prop^n 3.4</u> Let R be a 2-fir and a and b elements of R. Then the following are equivalent;

(i) $a \sim b$

(ii) there exists a comaximal relation $ca = bd$

(iii) there exists a coprime relation $ca = bd$.

([1] p.126)

§4. Distributive factor lattice

Let R be a 2-fir and c a non-zero element of R. We have seen that the set of $\mathcal{C}_R$-submodules of R/cR forms a modular lattice and we shall refer to this as the <u>factor lattice of c</u>. If every element of R has a distributive factor lattice, R is said to <u>satisfy DFL</u>.

<u>Def^n</u> Let $R \subseteq S$ be a ring embedding. This embedding is <u>1-inert</u> if for any $a \in R$ and any factorization $a = bc$ $(b,c \in S)$ there exists an invertible element u of S such that both bu and $u^{-1}c$ lie in R.

<u>Def^n</u> Let R be a k-algebra (k any commutative field). R is a <u>conservative 2-fir</u> if both R and $R \otimes_k k(t)$ are 2-firs and R is 1-inert in $R \otimes_k k(t)$.

<u>Prop^n 4.1</u> Let R be a conservative 2-fir. Then R satisfies DFL. ([CU p.159)

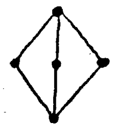
It is easily checked that $k\langle X\rangle$ is a conservative 2-fir; it is also atomic, so the factor lattice of any element is a distributive lattice of finite height. Such lattices have a very simple description in terms of partially ordered sets, which we now give.

Let L be a distributive lattice of finite height. An element a of L is <u>join-irreducible</u> if a has no non-trivial representation as the join of two elements. Let P(L) denote the set of join-irreducible elements of L; it has a partial order inherited from L. Given any partially ordered set T, let Q(T) denote the set of upper segments of T, that is subsets M such that $a \in M$, $b \geqslant a$ implies $b \in M$. Then Q(T) forms a lattice (join being union and meet intersection of sets).

Prop^n 4.2 There is a 1-1 correspondence between distributive lattices of height n and partially ordered sets with n elements, given by the maps P and Q described above. ([5] p. 61)

We define two particular kinds of lattices of factorization. If the corresponding partially ordered set is the unordered set of n elements, then the lattice is the Boolean algebra of subsets of this set, and we call the factorization completely reducible. If the corresponding partially ordered set is a chain of length n then the lattice is also a chain of length n, and the factorization is then called rigid.

Now let R be any atomic 2-fir. If R does not satisfy DFL, then there is a sublattice of a factor lattice of the form



([5] p. 59). It follows that there exist a,b,c,d R such that $ab = cd$ and $a \sim b \sim c \sim d$. Less obviously the converse is true;

Prop^n 4.3 Let R be an atomic 2-fir satisfying DFL. Then there are no elements a,b,c,d such that $ab = cd$ is a comaximal relation (and hence $a \sim b \sim c \sim d$). ([1] p.153)

§5. Matrices

The factorization results of the previous sections can be extended (in a somewhat weaker form) to the factorizations of matrices over firs. Any $m \times n$ matrix A over a ring R determines a mapping $\phi_A: {}^nR \to {}^mR$ (by premultiplication) and hence an exact sequence of right R-modules;

$$ {}^nR \xrightarrow{\phi_A} {}^mR \longrightarrow M \longrightarrow 0 $$

We identify the matrix A with the right R-module M ($\cong$ coker ϕ_A); this of course generalizes the idea of associating an element c with the strictly cyclic module R/cR. Two matrices A and B of the same characteristic are said to be stably associated if their associated right R-modules are isomorphic. We wish to consider the factorizations of a matrix by considering the submodules of its associated module; however we must restrict attention to a particular kind of module (corresponding to torsion modules in the element case).

Def^n Let $0 \longrightarrow {}^nR \longrightarrow {}^mR \longrightarrow M \longrightarrow 0$ be a presentation of the right R-module M. The characteristic of the presentation is defined to be $m-n$. If R is a semifir the characteristic of a module is independent of the presentation chosen, and we call this the characteristic of the module M, denoted $\chi(M)$.

Def^n Let R be a semifir and M a right R-module. M is a torsion module if;

(i) $\chi(M) = 0$

(ii) for any submodule N of M, $\chi(N) \geq 0$.

Let $\mathcal{T}_R$ denote the set of torsion R-modules; as in the case of strictly cyclic modules, they form a category.

<u>Prop^n 5.1</u> Let R be a semifir. Then $\mathcal{T}_R$ is a full abelian subcategory of $\mathcal{M}_R$. ([1] p.185)

Let $_R\mathcal{T}$ denote the corresponding category of left torsion modules. As before, there is a duality;

<u>Prop^n 5.2</u> $\mathcal{T}_R$ and $_R\mathcal{T}$ are dual categories.

<u>Cor^y</u> Suppose that both $_R\mathcal{T}$ and $\mathcal{T}_R$ satisfy ACC. Then they both satisfy DCC.

<u>Def^n</u> A semifir R is fully atomic if both $\mathcal{T}_R$ and $_R\mathcal{T}$ satisy ACC.

Note that a fir satisfies ACC_n for all n and hence is fully atomic.

<u>Prop^n 5.3</u> Let R be a fully atomic semifir and let M be a right torsion R-module. Then the set of $\mathcal{T}_R$-submodules of M forms a modular lattice of finite height.

Once the idea of a torsion module has been translated in terms of matrices, Prop^n 5.3 (and the Jordan-Holder Theorem for modular lattices) will provide a 'unique factorization' for matrices.

<u>Def^n</u> Let A be a n×n matrix over R. A is <u>full</u> if in any factorization $A = BC$ $(B \in {}^nR^m, C \in {}^mR^n)$, $m \geqslant n$.

<u>Prop^n 5.4</u> Let R be a semifir. Then a square matrix A is full iff the associated module $\mathrm{coker}\,\phi_A$ is a torsion module. ([1] p.199)

<u>Prop^n 5.5</u> Let R be a fully atomic semifir and let A be a full matrix over R. Then R has a factorization into (full) matrix atoms, and if $A = P_1P_2\ldots P_r$ and $A = Q_1Q_2\ldots Q_s$ are two factorizations of A into atoms then $r = s$ and there exists a

permutation σ of $1,\ldots,r$ such that P_i and $Q_{\sigma(i)}$ are stably associated $(i = 1,\ldots,r)$. (This follows immediately from 5.3 & 5.4.)

We now derive some equivalent conditions for stable association of matrices. The following definitions and results (plus proofs) may be found in [4].

Def^n Let R be any ring and let $A \in {}^mR^n$. A is left full if in any factorization $A = BC$ $(B \in {}^mR^q,\ C \in {}^qR^n)$ necessarily $q \geq m$; A is right full if in any such factorization $q \geq n$. A is left prime if in any factorization $A = PQ$ $(P \in R_m,\ Q \in {}^mR^n)$ P is right invertible. A is right prime if the analogous condition on the right holds.

Let $AC = BD$ be a relation between matrices over R. The relation is said to be right comaximal if $(A\ B)$ has a right inverse and left comaximal if $\begin{pmatrix} C \\ D \end{pmatrix}$ has a left inverse. It is comaximal if it is both left and right comaximal. The relation is left coprime if $(A\ B)$ is left prime, right coprime if $\begin{pmatrix} C \\ D \end{pmatrix}$ is right prime and coprime if it is both left and right coprime.

Prop^n 5.6 Let R be a semifir and A and B matrices over R of the same characteristic. Then the following are equivalent;

(i) A is stably associated to B

(ii) there exist invertible matrices U and V and identity matrices of suitable sizes such that

$$U\begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix} = \begin{pmatrix} B & 0 \\ 0 & I \end{pmatrix} V$$

(iii) there exists a comaximal relation $CA = BD$

(iv) there exists a coprime relation $CA = BD$.

Prop^n 5.7 Let R be a semifir and $AD = BC$ a relation between matrices over R in which $(A\ B)$ is left full and $\begin{pmatrix} D \\ C \end{pmatrix}$ is right full. Then we can cancel left and right square factors to get a comaximal relation i.e. there exist square matrices P and Q such that $A = PA'$, $B = PB'$, $D = D'Q$, $C = C'Q$ and $A'D' = B'C'$ is a comaximal relation.

§6. Eigenrings

Def^n Let R be a ring and J a right ideal of R. The (right) idealizer of J (in R), denoted $I_R(J)$ is the set $\{b \in R : bJ \subseteq J\}$.

It is easily seen that $I_R(J)$ is a ring and that J is a 2-sided ideal of $I_R(J)$. If J is a principal right ideal, say $J = aR$, then $I_R(J) = \{b \in R : ba \in aR\}$ so we write $I_R(a)$ instead of $I_R(J)$ and call this the idealizer of a.

Def^n Let R be a ring and J a right ideal of R. The (right) eigenring of J (in R), denoted $E_R(J)$ is $I_R(J)/J$.

Again if J is principal, say $J = aR$, we write $E_R(a)$ and call it the eigenring of a. There is an alternative formulation of the eigenring of an ideal;

Prop^n 6.1 Let R be a ring and J a right ideal of R. Then

$$E_R(J) \cong \mathrm{End}_R(R/J).$$

We may similarly define left idealizers and eigenrings; however we have the following result;

Prop^n 6.2 Let R be a ring and a a non-zerodivisor of R. Then the left and right eigenrings of a are isomorphic.

We shall be interested in two cases;

(i) where R is a 2-fir

(ii) where R is a matrix ring over a semifir.

In the first case the eigenring of an element is just the endomorphism ring of the associated strictly cyclic module. In the second case, suppose that $R = T_m$, where T is a semifir, and suppose that A is an element of R, full as a matrix over T. Then

$$E_R(A) = \mathrm{End}_{T_m}(T_m/AT_m) = \mathrm{End}_T({}^mT/A^mT)$$

so the eigenring of A is isomorphic to the ring of T-endomorphisms of the torsion T-module associated with A. In this case we shall write $E_T(A)$ instead of $E_R(A)$. We can apply Schur's Lemma in the category $\mathcal{C}_R$ or $\mathcal{T}_R$ to get the following result.

<u>Prop^n 6.3</u> Let R be a 2-fir (respectively semifir). Let A be an atom of R (respectively a full matrix atom over R). Then $E_R(A)$ is a skew field.

<u>Def^n</u> Let R be a k-algebra (k any commutative field). Then R is a <u>persistent</u> <u>2-fir</u> (respectively <u>semifir</u>) <u>over</u> <u>k</u> if both R and $R \otimes_k k(t)$ are 2-firs (respectively semifirs).

Free algebras are clearly persistent semifirs.

<u>Prop^n 6.4</u> Let R be a persistent 2-fir (respectively semifir). Let A be an element of R (respectively a full matrix over R). Then $E_R(A)$ is algebraic over k. [4]

Combining results 6.3 and 6.4 we get;

<u>Prop^n 6.5</u> Let R be a persistent 2-fir (respectively semifir) over an algebraically closed field k and let A be an atom of R (respectively a full matrix atom over R). Then $E_R(A) \cong k$.

In general if R is a k-algebra and a an element of R a is said to have a <u>scalar</u> <u>eigenring</u> if $E_R(a) \cong k$.

<u>Prop^n 6.6</u> Let R be a k-algebra and an atomic 2-fir and suppose that R satisfies DFL. Suppose moreover that every atom of R has a scalar eigenring; then every non-zero element of R has a commutative eigenring. ([1] p. 172)

If k is an algebraically closed field we can use this proposition (together with Prop^n 6.5) to deduce that every non-zero element of the free algebra $k\langle X\rangle$ has a commutative eigenring. In order to extend this to the case where k is not algebraically closed we need a result on the behaviour of eigenrings under ground field extensions.

Prop^n 6.7 Let R be a k-algebra and A a full matrix over R. Let E/k be a field extension and set $S = R \otimes_k E$. Then

$$E_S(A) = E_R(A) \otimes_k E$$

Cor^y Let k be any field. Then any non-zero element of the free algebra $k\langle X\rangle$ has a commutative eigenring.

There is one more result on eigenrings that we shall need later. Let $\mathcal{F}_R$ be some category of right R-modules. A right R-module $M \in \mathcal{F}_R$ is a distributive module if the lattice of $\mathcal{F}_R$-submodules of M forms a distributive lattice ; we shall be interested in the case where M is the strictly cyclic module associated with an element of a 2-fir R (and the category is the category of strictly cyclic R-modules).

Prop^n 6.8 Let M be a distributive module with both chain conditions and let $A_1, \ldots, A_n$ be the $\mathcal{F}_R$-simple modules occuring in a composition series for M (with their proper multiplicities). Then there is a homomorphism

$$\phi : \mathrm{End}(M) \longrightarrow \prod_{i=1}^{n} \mathrm{End}(A_i)$$

whose kernel is the Jacobson radical of End(M). Moreover $N = \ker\phi$ consists of all nilpotent endomorphisms of M and satisfies $N^n = 0$. ([1] p.150)

Chapter 2 Normal Forms

In this chapter we consider normal forms for matrices over $K_k\langle X\rangle$.

In §1 we define a lexicographical ordering of $K_k\langle X\rangle$; also the idea of left (and right) cofactors of elements or matrices. These two ideas are used in the next section.

In §2 we establish a normal form for full matrices over $K_k\langle X\rangle$ under stable association generalizing that given in [2]. A series of propositions leads up to the result (Th^{m} 2.1).

In §3 we establish a criterion for a matrix over a skew field to be cyclic (Th^{m} 3.1).

§1. Preliminaries

We recall from Chapter 1, §2 that there is a degree function d on $K_k\langle X\rangle$ given by $d(x) = 1$ for $x \in X$. We require a finer ordering than this in this chapter; we therefore introduce a lexicographical ordering as follows.

Def^n An element f of $K_k\langle X\rangle$ is pure (of degree r and type $(h(1),h(2),\ldots,h(r))$) if it is of the form

$$\sum_{j\in J} v_{1j}x_{h(1)}v_{2j}x_{h(2)}\cdots v_{rj}x_{h(r)}v_{r+1j}$$

where J is an indexing set, each $v_{ij} \in K$ and the $h(i)$ are integers (so $x_{h(i)} \in X$).

It is clear that any element of $K_k\langle X\rangle$ can be written uniquely as the sum of its pure components. We define an ordering on the set of pure elements as follows;

let f be of degree r and type $(h(1),h(2),\ldots,h(r))$

let g be of degree s and type $(k(1),k(2),\ldots,k(s))$

Then $f > g$ iff:

(i) $r > s$

or (ii) $r = s$, $h(i) = k(i)$ for $1 \leqslant i \leqslant j$ and $h(i+1) > k(i+1)$ for some $0 \leqslant j < r$.

Now for any element f of $K_k\langle X\rangle$ we define the pure-leading term of f, denoted f^t, to be the greatest pure component of f. $K_k\langle X\rangle$ can now be ordered by defining one element to be greater than another if its pure-leading term is greater. Let v be the order-preserving map from $K_k\langle X\rangle$ onto $\mathbb{N}$ induced by this ordering (thus $v(1) = 0$, $v(x_1) = 1$, etc.)

Clearly all the above may be extended to matrices over $K_k\langle X\rangle$; replace $K_k\langle X\rangle$ and K by $(K_k\langle X\rangle)_n$ and K_n respectively in the definitions.

In the particular case when $K = k$, so the ring is just the free algebra $k\langle X\rangle$, we say an element f is monic if the coefficient of its pure-leading term is 1.

The second idea we need is that of cofactors. Let u_i $(i \in I)$ be a k-basis of K. Any matrix A with entries in K can be written uniquely as $\sum_{i\in I} u_i A^i$, where the A^i are matrices with entries in k. A^i is called the right cofactor of u_i in A. Define[1]

$$A^* = (A^0 \; A^1 \; \ldots\ldots) \quad \text{and} \quad {}^*A = \begin{pmatrix} A^0 \\ A^1 \\ \vdots \end{pmatrix}$$

Now let A be any homogeneous matrix of degree ≥ 1 over $K_k\langle X\rangle$. Then A may be written uniquely as

$$\sum_{i,j} A^i_{-x_j}(x_j u_i)$$

where the $A^i_{-x_j}$ are matrices over $K_k\langle X\rangle$. $A^i_{-x_j}$ is called the left cofactor of $x_j u_i$ in A and we define

$$A^*_{-x_j} = (A^0_{-x_j} \; A^1_{-x_j} \; \ldots\ldots)$$

We make analogous definitions of the right cofactors of $u_i x_j$ in A.

We now prove two lemmas to be used in the proof of normal form in the next section.

Lemma 1.1 Let C be a matrix over K such that the rows of C are linearly independent over k. Then the rows of C^* are linearly independent (over k) and hence C^* has a right inverse.

Pf Suppose that the rows of C^* are linearly dependent. Then there exists $a \in {}^m k$ such that $aC = 0$. Hence $aC^i = 0$ for all $i \in I$ and so $aC = a(\sum_i C^i u_i) = 0$, contradicting the hypothesis.

[1] The notation implicitly assumes that $[K:k]$ is countable; the argument goes through in any case.

Def^n Let $A \in {}^pK^n$, $B \in {}^nK^p$, $x \in X$. Then AxB is in minimal form if the columns of A are linearly independent over k and the rows of B are linearly independent over k.

Lemma 1.2 Let $A \in {}^pK^n$, $B \in {}^nK^p$. Then there exists an $m \leq n$ and $C \in {}^pK^m$, $D \in {}^mK^p$ such that $AxB = CxD$ and CxD is in minimal form. Moreover, if CxD and ExF are in minimal form ($C \in {}^pK^m$, $D \in {}^mK^p$, $E \in {}^pK^r$, $F \in {}^rK^p$) and $CxD = ExF$ then $m = r$.

Pf Suppose that the columns of A are linearly dependent over k. Then there exists $J \in GL_n(k)$ such that $AJ = (A' \ \ 0)$. Write $J^{-1}B = \begin{pmatrix} B' \\ B'' \end{pmatrix}$. Then $AxB = A'xB'$. Clearly repeating this process on A and B will eventually yield the C,D required.

We observe that by Lemma 1.1, CxD is in minimal form iff ${}^*C$ and D^* have rank m. Now $CxD = ExF$. Taking left cofactors of xu_i we get $CD^i = EF^i$; now taking cofactors of u_j we get $C^jD^i = E^jF^i$. Hence $({}^*C)(D^*) = ({}^*E)(F^*)$. Since both CxD and ExF are in minimal form we have

$$m = \text{rank}({}^*CD^*) = \text{rank}({}^*EF^*) = r.$$

§2. Reduction to normal form

We start by recalling the normal form proved in [2] ; Let $A \in K_n$, $B \in K_m$ and suppose that $xI_n + A$ and $xI_m + B$ are stably associated over $K_k\langle x\rangle$. Then $m = n$ and A and B are conjugate over k. A matrix over $K_k\langle x\rangle$ is non-singular at ∞ if it is stably associated to a matrix of the form $xI_N + C$ ($C \in K_N$), so this result provides a normal form for matrices over $K_k\langle X\rangle$ non-singular at ∞. In this section we establish a (somewhat weaker) normal form for arbitrary full matrices over $K_k\langle X\rangle$, where $X = \{x_1,\ldots,x_d\}$ is a finite set of indeterminates.

Def^n A full matrix P over $K_k\langle X\rangle$ is in normal linear form if

$$P = C + \sum_{i=1}^{d} A_i x_i B_i$$

$$(C \in K_p,\ A_i \in {}^pK^{n_i}, B_i \in {}^{n_i}K^p)$$

satisfying the following conditions;

(i) the rows of $(A_1 \ \ldots \ A_d)$ are left linearly independent over K

(ii) the columns of $\begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_d \end{pmatrix}$ are right linearly independent over K

(iii) each $A_i x_i B_i$ is in minimal form.

We shall prove the following theorem;

Th^m 2.1 Let Q be a full matrix over $K_k\langle X\rangle$; then Q is stably associated to a matrix in normal linear form. Moreover if

$$Q_1 = C + \sum A_i x_i B_i \in (K_k\langle X\rangle)_p$$

$$Q_2 = D + \sum E_i x_i F_i \in (K_k\langle X\rangle)_q$$

are two matrices in normal linear form and $Q_1 \sim Q_2$ then $p = q$

and there exist $U,V \in GL_p(K)$ such that $Q_2 = UQ_1V^{-1}$.

As an immediate consequence of this theorem we have;

Cor^y Let $Q = C + \sum A_i x_i B_i$ ($C \in K_p$, $A_i \in {}^pK^{n_i}$; $B_i \in {}^{n_i}K^p$) be a matrix in normal linear form. The following are invariants;

(i) p = order of C

(ii) rank of C

(iii) n_i = number of columns of A_i.

We prove the theorem in three propositions.

Prop^n 2.2 Let Q be a full matrix over $K_k\langle X\rangle$. Then Q is stably associated to a matrix in normal linear form.

Pf For any elements a,b,c of a ring R we have that

$$(c + ab) \sim \begin{pmatrix} c+ab & 0 \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} c+ab & a \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} c & a \\ -b & 1 \end{pmatrix}$$

It is clear that by using this process (linearization by enlargement) sufficiently often we can find a matrix of the form $C + \sum A_i x_i B_i$ ($C \in K_q$, $A_i \in {}^qK^{m_i}$; $B_i \in {}^{m_i}K^q$) stably associated to Q. Let the rank of $(A_1 \,..\, A_d)$ over K be p. There exists $J \in GL_q(K)$ such that

$$J(A_1 \;\; A_2 \cdots A_d) = \begin{array}{c} \begin{pmatrix} A_1' & A_2' & \cdots & A_d' \\ 0 & 0 & \cdots & 0 \end{pmatrix} \end{array} \begin{array}{l} p \\ q-p \end{array}$$

Now let $C' = JC$ and partition each B_i as $(\overset{p}{B_i'} \;\; \overset{q-p}{B_i''})$. Then

$$\cdot\; Q \sim C' + \begin{array}{c} \begin{array}{cc} p & q-p \end{array} \\ \begin{pmatrix} \sum A_i' x_i B_i' & \sum A_i' x_i B_i'' \\ 0 & 0 \end{pmatrix} \end{array} \begin{array}{l} p \\ q-p \end{array}$$

Since Q is full the last $q-p$ rows of C' must have rank $q-p$ (over K), so by postmultiplying by a suitable invertible matrix over K, we have

$$Q \sim \begin{pmatrix} D_{11} + \sum E_i x_i F_i & D_{12} + \sum G_i x_i H_i \\ 0 & I_{q-p} \end{pmatrix}$$

$$\sim (D_{11} + \sum E_i x_i F_i) \qquad\qquad (D_{11} \in K_p)$$

and $\mathrm{rank}(E_1 \ E_2 \ \ldots \ E_d) = p$, so condition (i) of the definition is satisfied. Condition (ii) of the definition may be similarly enforced. Condition (iii) can be satisfied simply by writing each $E_i x_i F_i$ in minimal form (using Lemma 1.2).

<u>Lemma 2.3</u> Let $C + \sum A_i x_i B_i$ ($C \in K_p$, $A_i \in {}^pK^{n_i}$, $B_i \in {}^{n_i}K^p$) be a matrix in normal linear form. Then $\sum A_i x_i B_i$ is a left and right non-zerodivisor.

<u>Pf</u> Suppose the contrary, say

$$G(\sum A_i x_i B_i) = 0$$

Consider leading terms;

$$G^\ell(\sum A_i x_i B_i) = 0.$$

Now take left cofactors of $x_i u_j$;

$$G^\ell A_i B_i^{\ j} = 0$$

Hence $$G^\ell A_i B_i^* = 0$$

But $A_i x_i B_i$ is in minimal form and hence B_i^* has a right inverse; thus

$$G^\ell A_i = 0$$

and so $G^\ell(A_1 \ A_2 \ \ldots \ A_d) = 0$

But by condition (i) of the definition of normal linear form, $(A_1 \ A_2 \ \ldots \ A_d)$ has a right inverse. Hence $G^\ell = 0$, a contradiction unless $G = 0$. Thus $\sum A_i x_i B_i$ is a left non-zerodivisor. Similarly it is a right non-zerodivisor.

Prop^n 2.4 Let $Q_1 = C + \sum A_i x_i B_i$ and $Q_2 = F + \sum D_i x_i E_i$ be two matrices in normal linear form and suppose that $Q_1 \sim Q_2$. Then there exists a comaximal relation

$$UQ_1 = Q_2 V$$

in which U and V have entries in K.

Pf Since Q_1 and Q_2 are stably associated there are comaximal relations

$$UQ_1 = Q_2 V \qquad (1)$$

We show that in any such relation $\partial(U) = \partial(V)$. Suppose that $\partial(U) > \partial(V)$. Comparing leading terms in (1) we get

$$U^{\ell}(\sum A_i x_i B_i) = 0$$

By Lemma 2.3 this implies that $U^{\ell} = 0$ and hence $U = 0$, a contradiction since $\partial(U) > 0$. An analogous argument holds if $\partial(V) > \partial(U)$. Hence $\partial(U) = \partial(V)$.

Recall from §1 that v is the map from $K_k\langle X\rangle$ to $\mathbb{N}$ defined in terms of the lexicographic ordering of $K_k\langle X\rangle$. Let s be the minimum value assumed by v(U) in any comaximal relation (1). Suppose that the first x_i (reading from left to right) occurring in U^t, the pure leading term of U, is x_r. Let $v(U^t x_d) = N$ and consider the terms of v-value N,N-1,...,N-d+1 in (1):

$$U^t A_d x_d B_d = D_r x_r E_r V_1 \qquad (2.1)$$

$$U^t A_{d-1} x_{d-1} B_{d-1} = D_r x_r E_r V_2 \qquad (2.2)$$

$$\vdots \qquad\qquad \vdots$$

$$U^t A_1 x_1 B_1 = D_r x_r E_r V_d \qquad (2.d)$$

where the V_i are matrices occurring in V. Adding the d equations together we get

$$U^t(\sum A_i x_i B_i) = (D_r x_r E_r)(\sum V_i)$$

Since $\sum A_i x_i B_i$ is a non-zerodivisor, at least one of the V_i is non-zero. In fact the first non-zero V_i is the pure leading term of V, the second non-zero V_i is the second greatest pure component of V, etc. Moreover, for $i = 1,\dots,d$ and $s > r$,

$$D_s x_s E_s V_i = 0 \qquad (3)$$

for each of these expressions has v-value greater than N and the v-value of the leading term of the L.H.S. of (1) is $\leqslant N$.

Now take left cofactors of $x_j u_i$ in (2.d-j+1);

$$U^t A_j B_j^{\,i} = D_r x_r E_r (V_j)^i_{-x_j}$$

Hence;

$$U^t A_j B_j^* = D_r x_r E_r (V_j)^*_{-x_j} \qquad (4)$$

Now B_j^* has a right inverse, say M_j, so from (4);

$$U^t A_j = D_r x_r E_r (V_j)^*_{-x_j} M_j \qquad (5)$$

To simplify the notation write N_j for $(V_j)^*_{-x_j} M_j$. Combining the equations (5) for $j = 1,\dots,d$ we get;

$$U^t(A_1 \quad A_2 \ \dots \ A_d) = D_r x_r E_r (N_1 \quad N_2 \ \dots \ N_d) \qquad (6)$$

Now $(A_1 \quad A_2 \ \dots \ A_d)$ has a right inverse, say $\sum A_i G_i = 1$. Write $N = \sum N_i G_i$. Then from (6)

$$U^t = D_r x_r E_r N \qquad (7)$$

By applying to (3) the arguments we have just applied to (2.1)-(2.d) we also get

$$0 = D_s x_s E_s N \qquad (s > r) \qquad (8)$$

Now set $U' = U - Q_2 N$ and $V' = V - NQ_1$. Clearly

$$U'Q_1 = Q_2 V'$$

is a comaximal relation. Moreover

$$Q_2N = (D_1x_1E_1 + \dots + D_rx_rE_r)N + (D_{r+1}x_{r+1}E_{r+1} + \dots + D_dx_dE_d)N$$
$$+ \text{ terms of lower v-value}$$
$$= D_rx_rE_rN + 0 + \text{terms of lower v-value}$$
$$= U^t + \text{terms of lower v-value.}$$

Hence $U' = U - Q_2N$ has lower v-value than U, contradicting the choice of U. Thus we can choose U of v-value 0, i.e. with entries in K and it follows that V also has entries in K.

<u>Prop^n 2.5</u> Let $Q_1 = C + \sum A_ix_iB_i \in (K_k\langle X\rangle)_p$
and $Q_2 = F + \sum E_ix_iF_i \in (K_k\langle X\rangle)_q$

be two matrices in normal linear form and suppose that $Q_1 \sim Q_2$. Then $p = q$ and there exists $U,V \in GL_p(K)$ such that $UQ_1 = Q_2V$.

<u>Pf</u> By Prop^n 2.4 there is a comaximal relation

$$UQ_1 = Q_2V \qquad (1)$$

where U and V have entries in K. Hence there exist $P,T \in GL_q(K)$, $R,S \in GL_p(K)$ such that

$$PUR = \begin{array}{cc} \begin{array}{cc} m & p-m \end{array} & \\ \begin{pmatrix} I_m & 0 \\ 0 & 0 \end{pmatrix} & \begin{array}{l} m \\ q-m \end{array} \end{array} \quad \text{and} \quad SVT = \begin{array}{cc} \begin{array}{cc} n & p-n \end{array} & \\ \begin{pmatrix} I_n & 0 \\ 0 & 0 \end{pmatrix} & \begin{array}{l} n \\ q-n \end{array} \end{array}$$

The relation $PUR.R^{-1}Q_1T = PQ_2S^{-1}.SVT$ is still comaximal. Hence we may assume without loss of generality that the U and V in (1) are of the forms $\begin{pmatrix} I_m & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} I_n & 0 \\ 0 & 0 \end{pmatrix}$ respectively.

Assume that $m \geq n$ and let $s = p-m$, $t = q-m$. Partitioning Q_1 and Q_2 we can rewrite (1) as

$$\begin{pmatrix} I_n & 0 & 0 \\ 0 & I_{m-n} & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} X_{11} & X_{12} & X_{13} \\ X_{21} & X_{22} & X_{23} \\ X_{31} & X_{32} & X_{33} \end{pmatrix} = \begin{pmatrix} Y_{11} & Y_{12} & Y_{13} \\ Y_{21} & Y_{22} & Y_{23} \\ Y_{31} & Y_{32} & Y_{33} \end{pmatrix} \begin{pmatrix} I_n & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

so

$$\begin{pmatrix} X_{11} & X_{12} & X_{13} \\ X_{21} & X_{22} & X_{23} \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} Y_{11} & 0 & 0 \\ Y_{21} & 0 & 0 \\ Y_{31} & 0 & 0 \end{pmatrix}$$

Hence X_{12}, X_{13}, X_{22}, X_{23} and Y_{31} are all zero; (1) becomes

$$\begin{pmatrix} I_n & 0 & 0 \\ 0 & I_{m-n} & 0 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} X_{11} & 0 & 0 \\ X_{21} & 0 & 0 \\ X_{31} & X_{32} & X_{33} \end{pmatrix} = \begin{pmatrix} Y_{11} & Y_{12} & Y_{13} \\ Y_{21} & Y_{22} & Y_{23} \\ 0 & Y_{32} & Y_{33} \end{pmatrix}\begin{pmatrix} I_n & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

This is a comaximal relation; consider a relation of left comaximality.

$$\begin{pmatrix} L_{11} & L_{12} & L_{13} \\ L_{21} & L_{22} & L_{23} \\ L_{31} & L_{32} & L_{33} \end{pmatrix}\begin{pmatrix} X_{11} & 0 & 0 \\ X_{21} & 0 & 0 \\ X_{31} & X_{32} & X_{33} \end{pmatrix} + \begin{pmatrix} M_{11} & M_{12} & M_{13} \\ M_{21} & M_{22} & M_{23} \\ M_{31} & M_{32} & M_{33} \end{pmatrix}\begin{pmatrix} I_n & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = I_p$$

Consider the bottom right-hand corner of this equation;

$$L_{33}X_{33} = I_s$$

Since $K_k\langle X\rangle$ is weakly finite, this implies that

$$X_{33}L_{33} = I_s \qquad (2)$$

For any matrix G over $K_k\langle X\rangle$ let $G^{(1)}$ denote the homogeneous component of G of degree 1. Since X_{33} is of degree ≤ 1 (as a submatrix of Q_1), by taking leading terms in (2) we obtain

$$X_{33}^{(1)}L_{33}^{\ell} = 0$$

Now
$$\left(\sum A_i x_i B_i\right)\begin{pmatrix} 0 \\ 0 \\ L_{33}^{\ell} \end{pmatrix} = \left(Q_1^{(1)}\right)\begin{pmatrix} 0 \\ 0 \\ L_{33}^{\ell} \end{pmatrix}$$

$$= \begin{pmatrix} X_{11}^{(1)} & 0 & 0 \\ X_{21}^{(1)} & 0 & 0 \\ X_{31}^{(1)} & X_{32}^{(1)} & X_{33}^{(1)} \end{pmatrix}\begin{pmatrix} 0 \\ 0 \\ L_{33}^{\ell} \end{pmatrix}$$

$$= 0$$

But $\sum A_i x_i B_i$ is a non-zerodivisor and so $L_{33}^{\ell} = 0$, a contradiction unless $s = 0$. Thus $s = 0$ and so

$$X = \begin{pmatrix} X_{11} & 0 \\ X_{21} & 0 \end{pmatrix}$$

Since X is full we now must have $m-n = 0$ and so $p = m = n$.

Then
$$Q_1 = Q_2 \begin{pmatrix} I_m & 0 \\ 0 & 0 \end{pmatrix}$$

and since both Q_1 and Q_2 are full $q-m = 0$. Hence $q = m = n = p$, $U = V = I_n$ and the result is proved.

This completes the proof of the theorem. We note that in the special case that the matrices concerned are non-singular at zero (that is, the result of specializing each x_i to zero is an invertible matrix over K) we can strengthen this normal form a little, We insist (in addition to conditions (i) - (iii) already given) that C, the constant term, be the identity matrix. It then follows immediately that any two stably associated matrices in this form are conjugate over K.

§3. Cyclicity of a matrix

Let k be a commutative field, let $A \in k_n$ and let $V = k^n$. V is a right $k[x]$-module under the action $vx = vA$ and the matrix A is said to be cyclic if V is a cyclic module i.e. there exists $v \in V$ such that $V = vk[x]$. It can be shown that A is cyclic if and only if $xI_n - A$ is stably associated (over $k[x]$) to an element of $k[x]$.

Now let K be a skew field with centre k and $A \in K_n$. By analogy with the commutative case we define A to be cyclic if $xI_n - A$ is stably associated over $K_k\langle x\rangle$ to an element of $K_k\langle x\rangle$. In this section we derive a criterion for a square matrix over a skew field to be cyclic. By the result mentioned at the beginning of §2, $xI_n - A$ and $xI_n - B$ are stably associated iff A is conjugate over k to B; hence we are looking for a condition on the k-conjugacy class of A. This is provided by Th^m 3.1.

Th^m 3.1 Let K be a skew field with centre k. Then a matrix $A \in K_n$ is cyclic iff A is conjugate over k to a matrix with non-zero entries on the sub-diagonal and zeros beneath the subdiagonal.

Pf ($\Rightarrow$) Suppose that $xI_n - A \sim p \in K_k\langle x\rangle$ Then there exist comaximal relations

$$(xI_n - A)U = Vp \qquad (U, V \in {}^n(K_k\langle x\rangle)) \qquad (1)$$

We show that we may choose such a relation with V of degree 0. Suppose the contrary and let ∂V assume its minimum value in any such relation (1). Compare leading terms in (1);

$$xU^{\ell} = V^{\ell}p \tag{2}$$

Since all the terms in (2) are homogeneous, (2) implies that V^{ℓ} is a right multiple of x, say $V^{\ell} = xS$. Hence $U^{\ell} = Sp$. Now define

$$U' = U - Sp \qquad V' = V - (xI \quad A)S$$

Then $\qquad (xI_n - A)U' = V'p$

is a comaximal relation and $\partial V' < \partial V$, contradicting our choice of V. Hence we may take $\partial V = 0$ i.e. $V \in K^n$. Again consider leading terms of (1)

$$xU^{\ell} = Vp \tag{3}$$

Let $V = (a_1\ a_2 \ldots a_n)^T$. Since (1) is comaximal at least one of the a_i is non-zero, say $a_j \neq 0$. Then from (3) we see that $a_j p$ is a right multiple of x, hence $p = a_j^{-1}xr$ (say), and now $a_i p = a_i a_j^{-1}xr$ is a right multiple of x. Hence $a_i a_j^{-1} \in k$ for all i, and so by adjusting p by a suitable element of K we may assume without loss of generality that $V \in k^n$.

Since $V \in k^n$ (and is non-zero) there exists $J \in GL_n(k)$ such that $JV = (1\ \ 0\ \ 0 \ldots 0)^T$. Set $A' = JAJ^{-1}$, $U' = JU$. Then (1) becomes

$$(xI_n - A')U' = \begin{pmatrix} p \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{4}$$

Write $U' = (m_1\ \ m_2\ \ \ldots\ \ m_n)^T$. It is easily seen from (4) that $\partial m_1 > \partial m_i$ $(i = 2,3,..,n)$. Suppose that σ is a permutation of $\{2,3,\ldots,n\}$ such that $\partial m_{\sigma(2)} \geqslant \partial m_{\sigma(3)} \geqslant \ldots \geqslant \partial m_{\sigma(n)}$. Let J' be the permutation matrix representing σ and set

$$A'' = J'^{-1}A'J' \qquad U'' = J'U'$$

Then (4) still holds with A' and U' replaced by A'' and U'' respectively and the elements of U'' are arranged in descending order of degree. We note that none of the elements of U'' can be zero, for suppose that the last $n-m+1$ were zero. Let Z be the matrix obtained from A'' by deleting the last $n-m+1$ rows and columns and H the matrix obtained from U'' by deleting the last $n-m+1$ elements. Then

$$(xI_m - Z)H = \begin{pmatrix} p \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

and hence $xI_m - Z \sim p \sim xI_n - A$, a contradiction since $m \neq n$. Thus none of the elements of U'' are zero.

We shall show that A'' is conjugate over k to a matrix of the form described in the statement of the theorem. The idea is to successively reduce the 1^{st}, 2^{nd}, ..., n^{th} rows to the required form. We use induction. Let $P(r)$ denote the statements;

(i) there exists a matrix $B_r = (b^r_{ij}) \in K_n$, conjugate over k to A'' such that $b^r_{ji} = 0$ $(i < j-1)$ and $b^r_{j,j-1} \neq 0$ for all $j \leq r$. (i.e. the first r rows of the matrix B_r are in the required form).

(ii) there exist $U_r = (u^r_1 \ u^r_2 \ \ldots \ u^r_n)^T \in (K_k\langle x\rangle)^n$ such that $\partial u^r_1 > \partial u^r_2 > \ldots > \partial u^r_r \geq \partial u^r_{r+1} \geq \partial u^r_{r+2} \geq \ldots \geq \partial u^r_n$ and

$$(xI_n - B_r)U_r = \begin{pmatrix} p \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad (5)$$

$P(1)$ is satisfied by taking $B_1 = A''$ and $U_1 = U''$. Suppose that $P(r)$ is established; consider the $(r+1)^{th}$ row of (5);

$$-b^r_{r+1,1}u^r_1 - \dots - b^r_{r+1,r}u^r_r + (x - b^r_{r+1,r+1})u^r_{r+1}$$
$$- b^r_{r+1,r+2}u^r_{r+2} - \dots - b^r_{r+1,n}u^r_n = 0 \qquad (6)$$

If $b^r_{r+1,1} \neq 0$ then $-b^r_{r+1,1}u^r_1$ is the leading term of the LHS of (6) (because of the arrangement of the u^r_i in order of descending degree) and hence $u^r_1 = 0$. Hence $b^r_{r+1,1} = 0$. Similarly $b^r_{r+1,i} = 0$ for $i < r-1$.

Now we want to reduce the $(r+1,r-1)$ entry to 0. By hypothesis $b^r_{r,r-1} \neq 0$. Let

$$K = I_n - b^r_{r+1,r-1}(b^r_{r,r-1})^{-1}N_{r+1,r}$$

where N_{ij} denotes the matrix with a 1 in the (i,j) place and 0s elsewhere. Now let $B_{r+1} = KB_rK^{-1}$, $U_{r+1} = KU_r$. We note that B_{r+1} agrees with B_r on the top left-hand $r \times r-1$ submatrix of B_r and also on the first $r-2$ elements of the $(r+1)^{th}$ row. Moreover $b^{r+1}_{r+1,r-1} = 0$. Since U_{r+1} still satisfies the hypothesis (ii) of $P(r)$ all that remains to prove is that $b^{r+1}_{r+1,r} \neq 0$ and that $\partial u^{r+1}_{r+1} < \partial u^{r+1}_r$.

Consider what (6) becomes with the new naming (and remembering that $b^{r+1}_{r+1,i} = 0$ for $i < r-1$);

$$-b^{r+1}_{r+1,r}u^{r+1}_r + (x - b^{r+1}_{r+1,r+1})u^{r+1}_{r+1} - \dots - b^{r+1}_{r+1,n}u^{r+1}_n = 0 \quad (7)$$

If $\partial u^{r+1}_{r+1} = \partial u^{r+1}_r$ then the leading term of the LHS of (7) is xu^{r+1}_{r+1} and hence $u^{r+1}_{r+1} = 0$. Similarly if $b^{r+1}_{r+1,r} = 0$. Thus $\partial u^{r+1}_r > \partial u^{r+1}_{r+1}$ and $b^{r+1}_{r+1,r} \neq 0$, so $P(r+1)$ is established.

Thus $P(n)$ is true and so the forward implication of the theorem is proved.

($\Leftarrow$). This is just a straightforward calculation.

We consider some particular cases;

(i) $K = k$ is commutative. We clearly may reduce all the entries on the subdiagonal to 1 and then reduce all the entries on or above the diagonal (excluding the last column) to 0. We then have A in the form

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & b_0 \\ 1 & 0 & \cdots & 0 & b_1 \\ 0 & 1 & 0 \cdots & 0 & b_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdots & 0 & 1 & b_{n-1} \end{pmatrix} \qquad (b_i \in k)$$

This matrix is of course the companion matrix of the polynomial $f(x) = x^n - \sum_{i=0}^{n-1} b_i x^i$, and $xI_n - A \sim f$.

(ii) $n = 2$. Here the only condition for a matrix to be cyclic is that the bottom left hand corner of some matrix in the conjugacy class be non-zero; it is easily seen that this holds unless A is scalar i.e. $A = gI_2$ for some $g \in K$.

Chapter 3 Factorizations and Eigenrings

This chapter deals with the factorizations and eigenrings of elements and matrices in free algebras.

In §1 we consider the following situation; let R be a k-algebra, E/k a Galois extension with Galois group G and let $S = R \otimes_k E$. Let J be a principal right ideal of S generated by a non-zerodivisor and suppose that J is invariant under the action of G. Does J necessarily have an invariant generator ? This holds if $H^1(G, U(S))$ is trivial and we show that this condition is satisfied if R is a matrix ring over a fir (Prop^n 1.3). We prove an analogous result for purely inseparable extensions and derivations (Prop^n 1.4).

In §2 we determine what types of factorizations of matrix atoms over free algebras occur when the ground field is extended. If the extension is purely inseparable then the factorization is rigid (Prop^n 2.1) and if the extension is Galois then the factorization is fully reducible (Prop^n 2.4).

In §3 we consider eigenrings of atoms in free algebras; we show that each atom has a unique 'splitting field', given by the normal closure of the eigenring (Th^m 3.3).

Some examples of the factorizations described in §2 are constructed in §4.

In §5 we consider the eigenrings of matrix atoms over free algebras. We show that we can construct arbitrary division algebras over a commutative field k as the eigenring of a matrix atom of $k\langle X\rangle$ (Th^m 5.5).

§1. Invariant generators of invariant ideals

In considering the factorization of elements of free algebras under ground field extensions we shall come across the following question; do principal right ideals of $E\langle X\rangle$ invariant under the action of Gal(E/k) have an invariant generator? We also find the same question for matrices.

We answer the question in more generality. Recall the definition of the first cohomology group. Let G be a group and U a group (not necessarily abelian) on which G acts. A map $G \to U$ given by $g \mapsto u_g$ is a crossed homomorphism if it satisfies the following identity;

$$u_{gh} = u_h u_g^{\ h}$$

Two crossed homomorphism $g \mapsto u_g$ and $g \mapsto v_g$ are equivalent if there exists $c \in U$ such that

$$u_g = cv_g c^{-g} \qquad \text{(for all } g \in G)$$

The set obtained by taking the set of crossed homomorphisms and factoring out by this equivalence relation is the first cohomology set, denoted $H^1(G,U)$. $H^1(G,U)$ is trivial if it has only one element, namely the equivalence class of the trivial crossed homomorphism $G \to \{1\}$.

Now let R be a k-algebra and E/k a Galois extension with Galois group G. Let $S = R \otimes_k E$. We can regard G as acting on S (fixing R). Call a subset I of S G-invariant if $I^g \subseteq I$ for all $g \in G$; the G-invariant elements of S are just those that lie in R.

Prop^n 1.1 Let k,E,G,R and S be as above and suppose that $H^1(G,U(S))$ is trivial. Then any G-invariant principal right ideal of S generated by a non-zerodivisor is generated by an element of R.

Pf Let $I = fS$ be G-invariant (f a non-zerodivisor). For each $g \in G$, $f^g \in fS$, say $f^g = fu_g$. Consider f^{gh};

$$fu_{gh} = f^{gh} = (f^g)^h = (fu_g)^h = f^h u_g{}^h = fu_h u_g{}^h \qquad (1)$$

Since f is a non-zerodivisor we deduce from (1) that

$$u_{gh} = u_h u_g{}^h \qquad (2)$$

Taking $h = g^{-1}$ in (2) we see that $u_g \in U(S)$; thus $g \mapsto u_g$ is a crossed homomorphism of G into U(S). Since $H^1(G,U(S))$ is trivial this crossed homomorphism must be equivalent to the identity i.e. there exist $v \in U(S)$ such that $u_g = vv^{-g}$ (here v^{-g} denotes $(v^{-1})^g$).

Now let $f' = fv$. $fS = f'S$ and

$$(f')^g = (fv)^g = f^g v^g = fu_g v^g = fv = f' \qquad \text{for all } g \in G$$

so $f' \in R$.

The problem thus reduces to that of establishing that the first cohomology set is trivial. In the particular case where R = k the result is well-known;

Prop^n 1.2 Let E/k be a finite Galois extension with Galois group G. Then $H^1(G,U(E))$ is trivial.

(See e.g.[8] p.151 , where it is also proved that $H^1(G,GL_n(E))$ is trivial.)

Using this result we prove a more general result, including the case of invertible matrices over a free algebra.

Th^m 1.3 Let E/k be a Galois extension with Galois group G. Let R be a k-algebra and let $S = R\otimes_k E$. Then if R is a fir $H^1(G,GL_n(S))$ is trivial.

Pf Let $g\mapsto U_g$ be a crossed homomorphism of G into $GL_n(S)$. Let $F = S^n$. F is a left S-module (and hence also a left R-module) under the natural action.

Let T be the skew group ring on E over G (i.e. $T = E[G:eg = ge^g]$). F is a right T-module under the action

$$se = s(eI_n) \qquad (s\in F, e\in E)$$
$$sg = s^g U_g \qquad (s\in F, g\in G)$$

Now let F_1 be the elements of F fixed by all the elements of G. Since R is a fir and F_1 is a submodule of the free R-module F, F_1 is a free left R-module. Let $s_i (i\in I)$ be a left R-basis for F_1. We show that it is also a left S-basis for F.

(i) The set $s_i(i\in I)$ is left independent over S. Let g_i $(i = 1,2,\dots,m)$ be a list of all the elements of G and let a_i $(i = 1,2,\dots,m)$ be a k-basis for E. We note that the matrix C defined by $c_{ij} = a_j^{g_i}$ is invertible (this follows from Dedekind's Lemma)

Now suppose that there is a relation of S-dependence $\sum_i t_i s_i = 0$ $(t_i\in S)$. We may write $t_i = \sum_j a_j t_{ji}$ $(t_{ji}\in R)$. We then have

$$\sum_j (a_j(\sum_i t_{ji}s_i)) = 0$$

If we act on this by some $g\in G$ we get

$$\sum_j (a_j^g(\sum_i t_{ji}s_i)) = 0 \qquad (1)$$

Write t for the vector $(\sum t_{1i}s_i, \sum t_{2i}s_i, \dots, \sum t_{mi}s_i)^T$. Then from (1) we have that

$$Ct = 0$$

and hence $t = 0$. Thus $\sum_i t_{ji}s_i = 0$ for each i, But the s_i are left R-independent and so all the $t_{ji} = 0$. Thus the s_i are left S-dependent.

(ii) The set s_i $(i \in I)$ spans F. Let

$$H = \{s \in F : sg \in sE \text{ for all } g \in G\}$$

We show firstly that any element of H is a left E-multiple of an element of F_1 and secondly that any element of F is a sum of elements of H, which establishes the desired result.

(1) Let $s \in H$, say $sg = sb_g$ $(b_g \in E)$ for each $g \in G$. It is now easily checked that $g \mapsto b_g$ is a crossed homomorphism of G into E . Since by Prop^n 1.2 $H^1(G,E^*)$ is trivial there exists $d \in E$ such that $b_g = dd^{-g}$. Then for any $h \in G$,

$$(ds)h = (sd)h = s(dh) = s(hd^h) = sb_hd^h = sd = ds$$

so ds F_1 and hence s is a left E-multiple of an element of F_1.

(2) Let $f_i = \sum_{g \in G} ga_i^g \in T$ $(i = 1,2,\ldots,m)$. Since C is an invertible matrix there exist $z_i \in E$ such that $\sum_i f_iz_i = 1$. Now suppose that s is any element of F. Set $s_i' = sf_iz_i$. Then

$$s = s1 = s(\sum_i f_iz_i) = \sum_i sf_iz_i = \sum_i s_i'$$

For any $h \in G$ we have

$$\begin{aligned} s_i'h = sf_iz_ih = sf_ihz_i^h &= s(\sum_g ga_i^g hz_i^h) = s(\sum_g gha_i^{gh}z_i^h) \\ &= s((\sum_g gha_i^{gh})z_i^h) = s(f_iz_i^h) = s_i'(z_i^{-1}z_i^h). \end{aligned}$$

Thus each $s_i' \in H$ and s is the sum of the s_i'.

We have shown that the $s_i (i \in I)$ form an S-basis for F. Hence $|I| = n$. Let B be the matrix whose rows are the s_i. Then B is invertible and

$$B = Bg = B^gU_g \quad \text{for all } g \in G$$

so $U_g = B^{-g}B$. Thus every crossed homomorphism of G into $GL_n(S)$ is equivalent to the identity and $H^1(G, GL_n(S))$ is trivial.

<u>Cor^y</u> Let P be a full matrix over $S = E\langle X\rangle$ and suppose that the ideal PS_n is invariant under Gal(E/k). Then $PS_n = P'S_n$ for some $P' \in (k\langle X\rangle)_n$.

We also need an analogous result for derivations. We treat the simplest case. Let E/k be a simple purely inseparable extension of exponent 1 i.e. $E = k(a)$ where $a^p \in k$ (p = char k). Let d be the derivation on E defined by $a^d = 1$; d has field of constants k. Let R be a fir and a k-algebra and let $S = R \otimes_k E$. d may be extended to a derivation of S_n over R_n (by putting $R^d = 0$ and $(b_{ij})^d = (b_{ij}{}^d)$).

<u>Prop^n 1.4</u> Let P be a full matrix over S such that $P^d \in PS_n$. Then there exists $U \in GL_n(S)$ such that $PU \in R_n$.

<u>Pf</u> Let $P^d = PM$. Let $T = E[t : te = et + e^d,\ t^p = 0]$. We can define a left action of T on the free right S-module $F \cong {}^nS$ by

$$ts = s^d + Ms \qquad (s \in F)$$

$$es = se \qquad (s \in F,\ e \in E)$$

This makes F into a left T-module. We also make F into a right R-module under the obvious restriction from S.

Let $$F_1 = \{s \in F : ts = 0\}$$

F_1 is an R-submodule of the free right R-module F and R is a fir; hence F_1 is a free right R-module. Let $s_i (i \in I)$ be a right R-basis for F_1. We show that it is also an S-basis for F.

(i) The set $s_i (i \in I)$ is right independent over S. Suppose there is a relation of dependence $\sum_i s_i m_i = 0$ $(m_i \in S)$. Since E is spanned over k by $1, a, \ldots, a^{p-1}$ we may write $m_i = \sum_{j=1}^{p-1} a^j m_{ij}$ $(m_{ij} \in R)$ and the relation of dependence becomes

$$\sum a^j(\sum s_i m_{ij}) = 0$$

Premultiplying by t gives

$$ja^{j-1}(\sum s_i m_{ij}) = 0$$

(since $ts_i = 0$) and continuing like this we get

$$\begin{pmatrix} 1 & a & \cdots & a^{p-1} \\ 0 & 1 & & (p-1)a^{p-2} \\ & & 2! \ddots & \vdots \\ 0 & & 0 & (p-1)! \end{pmatrix} \begin{pmatrix} s_i m_{i1} \\ s_i m_{i2} \\ \vdots \\ s_i m_{ip} \end{pmatrix} = 0$$

But clearly the left-hand matrix is invertible. Hence each $\sum s_i m_{ij}$ is 0 and since the s_i are R-independent, all the m_{ij} must be 0 i.e. $m_i = 0$ for all $i \in I$. Thus the s_i are linearly independent over S.

(ii) The s_i span F. Since the matrix $C = (c_{ij})$ defined by $c_{ij} = (a^j)^{d^i} = {}^jC_i\ a^{j-i}$ is invertible we can find $b_o, b_1, \ldots, b_{p-1}$ such that

$$C \begin{pmatrix} b_o \\ b_1 \\ \vdots \\ b_{p-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

It can now be checked that (in T)

$$\sum_i a^i t^{p-1} b_i = 1$$

Let $s \in F$ and define $m_i = t^{p-1} b_i s$. We see that;

(1) $tm_i = t^p b_i s = 0$, so $m_i \in F_1$

(2) $s = \sum_i a^i m_i = \sum m_i a^i$, so s is a right combination (over E) of the m_i.

Thus the s_i also span F, and hence $|I| = n$.

Let U be the matrix whose columns are the s_i. $U \in GL_n(S)$ and

$$\begin{aligned} tU &= 0 \\ &= U^d + MU \end{aligned}$$

Hence

$$\begin{aligned} (PU)^d &= P^dU + PU^d \\ &= PMU + PU^d \\ &= P(MU + U^d) \\ &= 0. \end{aligned}$$

§2. Nature of factorizations under ground field extensions

We deal first with the purely inseparable case.

Th^{m} 2.1 Let $R = k\langle X\rangle$, let E/k be a purely inseparable extension and let $S = E\langle X\rangle$. Let P be a matrix atom of R_m. Then P has an atomic factorization in S_m of the form $P = P_1\ldots P_n$ where $P_1 \sim P_2 \sim \ldots \sim P_n$. If $m = 1$ (so P is an element of R) then this factorization is rigid.

Befor proving this theorem we state and prove a proposition and a particular case of the theorem.

Prop^{n} 2.2 Let $S = E\langle X\rangle$ (where E is any commutative field) and let $f_1, f_2, \ldots, f_n$ be atoms of S with $f_1 \sim f_2 \sim \ldots \sim f_n$. Then the product $f_1 f_2 \ldots f_n$ is rigid.

Pf Suppose that $f = g_1 g_2 \ldots g_r$ is a different atomic factorization of f in S. Since S is a UFD, $r = n$ and each $g_i \sim f_1$. Now suppose that $g_1 S = f_1 S$. Cancelling on the right in the relation

$$f_1 . f_2 f_3 \ldots f_n = g_1 . g_2 g_3 \ldots g_n$$

we get a coprime (and hence comaximal) relation

$$f_1 t = g_1 s$$

and now $t \sim g_1 \sim f_1 \sim s$, a contradiction (by Prop^{n} 1.4.3).

Hence $f_1 S \neq g_1 S$. Continuing inductively we can show that the two factorizations $f = f_1 f_2 \ldots f_n$ and $f = g_1 g_2 \ldots g_r$ are equivalent. Thus $L(fS,S)$ is a chain and the product $f = f_1 f_2 \ldots f_n$ is rigid.

Prop^{n} 2.3 Hypotheses and conclusions as in Th^{m} 2.1, except assume that the extension E/k is a simple purely inseparable extension of exponent 1.

Pf Let k be of characteristic p. E is of the form $k(a)$ where $a^p \in k$. There is a derivation d on E (with field of constants k) given by $a^d = 1$. This may be extended to a derivation of S_m over R_m by setting $(b_{ij})^d = (b_{ij}{}^d)$ and $R^d = 0$.

Now suppose that P has a factorization (in S_m)

$$P = P_1 P_2 \dots P_r G \tag{1}$$

where the P_i are atoms of S_m with $P_1 \sim P_2 \sim \dots \sim P_r$ and G has no factorization with a left atomic factor stably associated to P_1. If G is invertible the result is established, so assume that G is a non-unit. We derive a contradiction. Since $P \in R_m$, $P^d = 0$; hence applying d to (1) gives

$$0 = (P_1 \dots P_r)^d G + (P_1 \dots P_r) G^d$$

$$-(P_1 \dots P_r) G^d = (P_1 \dots P_r)^d G \tag{2}$$

Since P is an atom of R_m and $P_1 \dots P_r$ is a proper left factor of P, $P_1 \dots P_r \notin R_m$ and hence $(P_1 \dots P_r)^d \neq 0$. Thus (2) provides a non-zero common right multiple of $(P_1 \dots P_r)$ and $(P_1 \dots P_r)^d$. We find common right and left factors in (2);

$$G^d = MQ,\ G = M'Q,\ -P_1 \dots P_r = FN,\ (P_1 \dots P_r)^d = FN'$$

Note that N is not invertible. (For suppose that N was invertible. Then $(P_1 \dots P_r)^d$ is a right multiple of $(P_1 \dots P_r)$ and by Prop^n 1.4 there exists $U \in GL_m(S)$ such that $P_1 \dots P_r U \in R_m$, contradicting the atomicity of P.) Cancelling the right and left factors in (2) gives the coprime (and hence comaximal) relation

$$N.M = N'.M'$$

Thus $M' \sim N$ and N as a right factor of $P_1 \dots P_r$ is the product of atoms stably associated to P_1. Hence G has a left atomic factor stably associated to P_1, contradicting our hypothesis.

It follows that P has a factorization of the form

$$P = P_1 \dots P_m$$

where the P_i are pairwise stably associated atoms of S. If P is an element of R then by Prop^n 2.2 the factorization is rigid.

<u>Pf of Th^m</u> There is a sequence of fields

$$k = E_o \subseteq E_1 \subseteq E_2 \subseteq \dots \subseteq E_m = E$$

such that E_{i+1}/E_i is a simple purely inseparable extension of exponent 1 ($i = 0,1,\dots,m-1$). We prove by induction on i that all the atomic factors of P in E_i are stably associated. The case $i = 0$ is trivial.

Suppose that P has an atomic factorization $P = P_1 P_2 \dots P_q$ in $E_j\langle X\rangle$ with $P_1 \sim P_2 \sim \dots \sim P_q$. Now P_1 is an atom of $E_j\langle X\rangle$ and E_{j+1}/E_j is a simple purely inseparable extension of exponent 1. By Prop^n 2.3 P_1 has a factorization in $E_{j+1}\langle X\rangle$ of the form $P_1 = G_1 \dots G_p$ with the G_i stably associated atoms. Now P_1 and P_r $(2 \leqslant r \leqslant q)$ are stably associated as elements of $E_j\langle X\rangle$, hence also as elements of $E_{j+1}\langle X\rangle$. Thus all the atomic factors of P_r in $E_{j+1}\langle X\rangle$ are stably associated to G_1 and so the factorization of P in $E_{j+1}\langle X\rangle$ is of the form $P = G_1 G_2 \dots G_N$ with $G_1 \sim G_2 \sim \dots \sim G_N$. If $n = 1$, so P is an element of R then by Prop^n 2.2 this factorization is rigid.

Now we deal with the Galois case.

<u>Prop^n 2.4</u> Let $R = k\langle X\rangle$, let E/k be a Galois extension with Galois group G and let $S = E\langle X\rangle$. Let P be a matrix atom in R_m. Then the factorization of P in S_m is completely reducible; it is

$$ {}^{m}S/P^{m}S = \bigoplus_{g\in T} {}^{m}S/Q_1^{g}\,{}^{m}S $$

where T is some subset of G and Q_1 an atom of S_m.

Pf G induces a group of automorphisms of S_m with fixed ring R_m. Since $P \in R_m$, G fixes P and so induces a group of lattice automorphisms of $L(PS_m, S_m)$, the lattice of principal right ideals of S_m containing PS_m (equivalently, the lattice of m-generator torsion modules containing ${}^{m}S/P^{m}S$). Let Q_1 be an atomic left factor of P in S_m and consider the ideal

$$ I = \bigcap_{g\in G} Q_1^{g} S_m $$

I is a principal right ideal of S_m, say $I = JS_m$ and clearly I is invariant under G. By the corollary to Prop^n 1.3 I has an invariant generator, say $I = KS_m$ $(K \in R_m)$. But then K is a left factor of P and P is an atom of R_m; hence $KS_m = PS_m$.

Taking an irredundant intersection of the $Q_1^{g} S_m$ over some subset T of G we get the desired result.

Cor^y Let $R = k\langle X\rangle$, let E/k be a Galois extension with Galois group G and let $S = E\langle X\rangle$. Let f be an atom of R. Let L be the factor lattice of f in S and let P be the corresponding partially ordered set. Then P is the unordered set of (say) t elements, so $L = 2^t$. G has a natural action on P and this action is transitive.

§3. The splitting field

We start with a useful result relating the eigenrings of atoms to the eigenrings of their factors in extended rings.

Prop^n 3.1 Let $R = k\langle X\rangle$, let E/k be a field extension and let $S = E\langle X\rangle$. Let f be an atom of R and suppose that f has an atomic factorization $f = f_1f_2\ldots f_n$ in S. Then $E_R(f)$ embeds (as a ring) in $E_S(f_1)$. In particular if f_1 is an absolute atom then $E_R(f)$ embeds in E.

Pf By Prop^n 1.6.7, $E_S(f) = E_R(f)\otimes_k E$, so there is an embedding

$$a: E_R(f) \longrightarrow E_S(f)$$

By Prop^n 1.6.8, there is a map

$$b: E_S(f) \longrightarrow \prod_i E_S(f_i)$$

There is also the projection map

$$c: \prod_i E_S(f_i) \longrightarrow E_S(f_1)$$

Combining these maps we get a (non-zero) map cba: $E_R(f) \longrightarrow E_S(f_1)$ Since f is an atom, $E_R(f)$ is a field and hence this map is an embedding.

If f_1 is an absolute atom then $E_S(f_1) \cong E$ and the last statement of the proposition follows.

We thus have that $E_R(f)$ embeds in any field over which f has an absolutely atomic factor. We now want to show that f has an absolutely atomic factor over $E_R(f)$ and factorizes completely over the normal closure of $E_R(f)$. This will prove the existence of unique 'splitting fields'. We deal first with the purely inseparable case and then with the general case.

Def^n An atom of $k\langle X\rangle$ is purely inseparable if it factorizes into the product of absolute atoms over some purely inseparable extension of k.

Prop^n 3.2 Let f be a purely inseparable atom of $R = k\langle X\rangle$. Then $E_R(f)$ is a purely inseparable extension of k over which f splits into absolute atoms.

Pf By hypothesis f splits into absolute atoms over some purely inseparable extension of k. By Prop^n 3.1, $E_R(f)$ embeds in this field and hence is itself a purely inseparable extension of k.

Write $F = E_R(f)$, $S = F\langle X\rangle$, and $T = E_S(f)$. By Prop^n 1.6.7, $T = E_R(f)\otimes_k F = F\otimes_k F$.

By Th^m 2.1, the atomic factorization of f in S is of the form $f = f_1\ldots f_n$, where $f_1 \sim f_2 \sim \ldots \sim f_n$. We shall prove that f_1 has a scalar eigenring. Since $f_1 \sim f_n$ there is a comaximal relation

$$af_1 = f_n a' \qquad (1)$$

Define a: $I_S(f_1) \longrightarrow I_S(f)$ by $c \longmapsto f_1\ldots f_{n-1}ac$. This is not a ring homomorphism but it is an E-space homomorphism. a induces a map b: $I_S(f_1) \longrightarrow E_S(f)$. Then

$$\begin{aligned}\ker(b) &= \{c \in I_S(f_1) : f_1\ldots f_{n-1}ac \in f_1\ldots f_n S\}\\ &= \{c \in I_S(f_1) : ac \in f_n S\}\\ &= f_1 S\end{aligned}$$

(for since (1) is comaximal, $af_1 = f_n a'$ is a LCRM of a and f_n). Thus b induces an (E-space) embedding c: $E_S(f_1) \hookrightarrow E_S(f) = T$.

Note that each element of T is either a unit or a zero-divisor (see e.g. [6] p.197). Let $s \in I_S(f)$ and let $t = \bar{s}$ be the image of s in T. There is a relation $sf = fs'$, which is right comaximal iff t is invertible. Clearly if $s \in f_1 S$ this relation is not right comaximal. Conversely, if the relation is not right comaximal then s and f have a common left factor; since f has the rigid factorization $f = f_1\ldots f_n$, s must have f_1 as a left factor.

Thus s is a non-unit iff $s \in f_1S$. Now let

$$J = \{t \in T : ta = 0 \text{ for all non-units } a\}$$

J is a minimal right ideal of T and isomorphic to F (as T-module). We claim that $Im(c) \subseteq J$. By (2) it suffices to show that any element of Im(c) is annihilated by f_1.

Let $m \in Im(c)$; $m = f_1 \dots f_{n-1}ac$ for some $c \in I_S(f_1)$. Hence

$$\begin{aligned} \overline{mf_1} &= \overline{f_1 \dots f_{n-1}acf_1} \\ &= \overline{f_1 \dots f_{n-1}af_1c'} \\ &= \overline{f_1 \dots f_{n-1}f_na'c'} \\ &= 0. \end{aligned}$$

Thus $Im(c) \subseteq J$. Comparing k-dimensions now yields

$$\begin{aligned} |E_S(f_1):k| &= |Im(c):k| \\ &\leqslant |J:k| \\ &\leqslant |F:k| \end{aligned}$$

But $F \subseteq E_S(f_1)$; hence $F \cong E_S(f_1)$, and F has a scalar eigenring.

Now suppose that f_1 is not an absolute atom. Since f is purely inseparable, f_1 factorizes into absolute atoms over some purely inseparable extension G of F. By Th^m 2.1 the factorization of f_1 over G is of the form $f_1 = g_1g_2 \dots g_m$, where $g_1 \sim g_2 \sim \dots \sim g_m$. By hypothesis, $m > 1$. Now let $cg_1 = g_mc'$ be a comaximal relation. Then $g_1 \dots g_{m-1}c$ is a non-trivial element of the eigenring of f_1 in $G\langle X\rangle$. But f_1 has a scalar eigenring over F, hence also over G

Thus f_1 (and so also $f_2, \dots, f_n$) are absolute atoms.

<u>Th^m 3.3</u> Let f be an atom of $R = k\langle X\rangle$. Then f has at least one absolutely atomic factor over $E_R(f)$ and f factorizes into the product of absolute atoms over the normal closure of $E_R(f)$.

<u>Pf</u> Let E be a minimal Galois extension of k over which f factorizes

into purely inseparable atoms, say $f = f_1 \ldots f_r$ in $E\langle X\rangle$. Let $S = E\langle X\rangle$, let G be $\mathrm{Gal}(E/k)$, let L be the factor lattice of f in S and let P be the corresponding partially ordered set. Define

$$M = \{g \in G \,:\, f_1{}^g = f_1\}$$

By the corollary to Prop^n 2.4 G acts transitively on P (a set of r elements) and hence M is a subgroup of G of index r. Let

$$M' = \{e \in E \,:\, e^g = e \quad \text{for all } g \in M\}$$

M' is a separable extension of k and $|M':k| = r$. Let $T = M'\langle X\rangle$; note that $f_1 \in T$. We show that $E_R(f) \cong E_T(f_1)$; since by Prop^n 3.1 $E_R(f) \hookrightarrow E_T(f_1)$ it suffices to show that $E_R(f)$ and $E_T(f_1)$ have the same dimension as k-spaces.

Again using the corollary to Prop^n 2.4 we have that f is fully reducible over S; $S/fS \cong \bigoplus_{g\in B} S/f_1{}^g S$, where B is a subset of G with r elements (in fact, B could be taken to be a set of coset representatives of M in G). Clearly f_1 and $f_1{}^g$ have isomorphic eigenrings; hence

$$\begin{aligned} E_S(f) &\cong \prod_{g\in B} E_S(f_1{}^g) \\ &\cong (E_S(f_1))^r \end{aligned}$$

so

$$|E_S(f):E| = r|E_S(f_1):E|.$$

It follows that

$$\begin{aligned} |E_R(f):k| &= |E_S(f):E| \\ &= r\,|E_S(f_1):E| \\ &= r|E_R(f_1):M'| \\ &= |E_T(f_1):k| \end{aligned}$$

Thus $E_R(f) \cong E_T(f_1)$. Since f_1 is a purely inseparable atom of T it splits into absolute atoms over $E_T(f_1)$ (Prop^n 3.2). Thus f has at least one absolutely atomic factor over $E_R(f)$.

Now let K be the normal closure of $E_R(f)$. K contains E and since K is normal every element of Gal(E/k) extends to an element of Aut(K). In $K\langle X\rangle$ f_1 has the factorization

$$f_1 = g_1 \ldots g_m$$

where the g_i are absolute atoms. Hence f_1^g has the factorization

$$f_1^g = g_1^g \ldots g_m^g \qquad (1)$$

where g denotes the extension of g from Gal(E/k) to Aut(K) and the g_j^g are absolute atoms (because the g_j are).

In $E\langle X\rangle$ f has the factorization

$$f = f_1 \ldots f_r$$

and (from the Cor^y to Prop^n 2.4) each f_j is stably associated to f_1^g for some $g \in G$. From (1) we deduce that each f_j factorizes into absolute atoms over K.

Thus f factorizes into absolute atoms in $K\langle X\rangle$.

§4. Examples

In this section we construct some examples of the factorizations described in §2.

Prop^n 4.1 Let $f_i = x^{n-i}yx^{i-1} + a_i x + 1$ $(1 \leq i \leq n$; n a fixed integer) be elements of $k(a_1,\ldots,a_n)\langle x,y\rangle$ and let $f = f_1 \ldots f_n$. Then f is symmetric in the a_i.

Pf Let $h_i = x^{n-i}yx^{i-1} + 1$ and let $h = x^n yx^{-1} + 1$. Then

$$\begin{aligned} f_i &= h_i + a_i x \\ &= x^{-i}hx^i + a_i x \end{aligned}$$

Let J be the set of all functions from $\{1,\ldots,n\}$ to $\{+,-\}$ and define $t_i^{+} = h_i$, $t_i^{-} = a_i x$ $(i = 1,\ldots,n)$. Then

$$\begin{aligned} f &= \prod_{i=1}^{n} f_i \\ &= \prod_{i=1}^{n} (x^{-i}hx^i + a_i x) \\ &= \sum_{j\in J} t_1^{j(1)} \ldots t_n^{j(n)} \\ &= \sum_{r=0}^{n} \sum_{\substack{j\in J;\\ |j^{-1}(+)|=r}} t_1^{j(1)} \ldots t_n^{j(n)} \end{aligned}$$

Now define $s_i^{+} = 1$, $s_i^{-} = a_i$. Then if $|j^{-1}(+)| = r$,

$$t_1^{j(1)} \ldots t_n^{j(n)} = (x^{-1}h)^r x^n s_1^{j(1)} \ldots s_n^{j(n)}$$

Thus

$$f = \sum_{r=0}^{n} (x^{-1}h)^r x^n \Big(\sum_{\substack{j\in J;\\ |j^{-1}(+)|=r}} s_1^{j(1)} \ldots s_n^{j(n)} \Big)$$

and each term in brackets is the coefficient of z^r in the expansion of $\prod_{i=1}^{n} (z + a_i)$ and hence symmetric in the a_i. Thus f is symmetric in the a_i.

Prop^n 4.2 Let k be a field and g an irreducible polynomial of k[t]. Let E be the splitting field of g. Assume that E is either separable (so Galois) or (simple) purely inseparable, and let $a_1, a_2, \ldots, a_n$ be the roots of f in E. Define f_i and f as in Prop^n 4.1. Then;

(i) f_i is an absolute atom of $E\langle X\rangle$

(ii) f is an atom of $k\langle X\rangle$.

<u>Pf</u> That f_i is an absolute atom may be easily seen by considering degrees in y. Now let $R = k\langle X\rangle$ and $S = E\langle X\rangle$. To prove (ii) we consider the two cases separately.

<u>Case 1</u> E/k Galois. Let $G = \mathrm{Gal}(E/k)$. Then G acts transitively on $a_1, \ldots, a_n$ and hence $x^{n-1}y + a_i x + 1$ is a left atomic factor of f for $i = 1,2,..,n$. However they are pairwise not stably associated; since S satisfies DFL this imples that

$$\bigcap_{i=1}^{n} (x^{n-1}y + a_i x + 1)S$$

is generated by an element of length at least n. But f is of length n and thus

$$fS = \bigcap_{i=1}^{n} (x^{n-1}y + a_i x + 1)S$$

Moreover, these n atoms exhaust all the possible left atomic factors of f in S (again because S satisfies DFL and f is of length n). Now suppose that g is a left factor of f in R. Then $g \in (x^{n-1}y + a_j x + 1)S$ for some j. Now $g^\alpha = g$ for each $\alpha \in G$; so $g \in (x^{n-1}y + a_i x + 1)S$ for each i. Hence $g \in fS$. Thus f is an atom of R.

<u>Case 2</u> E/k purely inseparable. Then $a_i = a$ (say) for $i = 1,\ldots,n$, and so all the f_i are stably associated; a comaximal relation relating f_i and f_{i-1} is

$$x(x^{n-i}yx^{i-1} + ax + 1) = (x^{n-i+1}yx^{i-2} + ax + 1)x.$$

Since all the factors of f are similar the factorization is rigid; thus if g is a left factor of f in R, $g = f_1 \ldots f_j$ for some $1 \leq j \leq n$. Now specialize y to 0; we get

$$(ax + 1)^j \in k[x]$$

Thus $a^j \in k$ and so $j = 0$ or n i.e. g is either a unit or equivalent to f. Thus f is again an atom of R.

Particular instances of this construction are;

(i) $k = Q$, $f(t) = t^2 + 1$, $E = Q(i)$

$$(xy + ix + 1)(yx - ix + 1) = xy^2x + x^2 + xy + yx + 1.$$

(ii) $k = Q$, $f(t) = t^3 - 2$ with roots $a, a\omega, a\omega^2$, $E = Q(a,\omega)$

$$(x^2y + ax + 1)(xyx + a\omega x + 1)(yx^2 + a\omega^2 x + 1) =$$
$$x^2yxyxyx^2 + x^2yxyx + x^2y^2x^2 + xyxyx^2 + 2x^3 + x^2y + xyx + yx^2 + 1.$$

(iii) F a field of characteristic 3, $k = F(z)$, $f(t) = t^3 - z$ with root say s (so $s^3 = z$) and $E = k(s)$

$$(x^2y + sx + 1)(xyx + sx + 1)(yx^2 + sx + 1) =$$
$$x^2yxyxyx^2 + x^2yxyx + x^2y^2x^2 + xyxyx^2 + zx^3 + x^2y + xyx + yx^2 + 1.$$

In order to construct some more examples of factorizations we use the idea of <u>continuant polynomials</u>; these are polynomials $p_0, p_1, \ldots, p_n, \ldots$ in the non-commuting indeterminates $t_1, t_2, \ldots, t_n, \ldots$ defined inductively by

$$p_0 = 1,\ p_1(t_1) = t_1 \text{ and}$$
$$p_n(t_1,\ldots,t_n) = p_{n-1}(t_1,t_2,\ldots,t_{n-1})t_n + p_{n-2}(t_1,\ldots,t_{n-2}).$$

In any ring with the 2-term weak algorithm (in particular, in free algebras) it is possible to analyse comaximal relations in terms of continuant polynomials (see [1]). However, all we require here is the rather obvious result in the opposite direction;

<u>Prop^n 4.4</u> Let $t_1, \ldots, t_n$ be elements of $k\langle X\rangle$. Then

$p_n(t_1,\dots,t_n)\cdot p_{n-1}(t_{n-1},\dots,t_1) = p_{n-1}(t_1,\dots,t_{n-1})\cdot p_n(t_n,\dots,t_1)$

is a comaximal relation.

Pf This is easily proved by induction.

We may now construct some more examples.

Prop^n 4.4 Let $X = \{t_1,\dots,t_n\}$ and let $R = \mathbb{Q}\langle X\rangle$. Let p_n denote $p_n(t_1,\dots,t_n)$ and p'_n denote $p_n(t_n,\dots,t_1)$. Then

(i) $f = p_np'_n + p_{n-1}p'_{n-1}$ is an atom of $\mathbb{Q}\langle X\rangle$

(ii) over $\mathbb{Q}(i)\langle X\rangle$, f has the absolutely atomic factorization

$$\begin{aligned} f &= (p_n + ip_{n-1})(p'_n - ip'_{n-1}) \\ &= (p_n - ip_{n-1})(p'_n + ip'_{n-1}) \end{aligned}$$

Pf We first prove by induction on n that $p_n \pm ip_{n-1}$ is an absolute atom. The case n = 1 is trivial. Write $f_n = p_n \pm ip_{n-1}$. Then

$$f_n = p_{n-1}t_n + p_{n-2} \pm ip_{n-1}.$$

Suppose that $f_n = gh$. The degree of f_n in t_n is 1 and so g and h must be of degrees 0 and 1 respectively in t_n. Write $h = h_o + h_1$, where h_i is homogeneous of degree i in t_n. Then

$$gh_o = p_{n-2} \pm ip_{n-1}.$$

By inductive hypothesis either g or h_o is a unit. If h_o is a unit we may take it to be 1 and then

$$\begin{aligned} g &= p_{n-2} \pm ip_{n-1} \\ gh_1 &= p_{n-1}t_n \end{aligned}$$

This is clearly impossible; hence g is a unit and f_n is an absolute atom.

That
$$\begin{aligned} f &= (p_n + ip_{n-1})(p'_n - ip'_{n-1}) \\ &= (p_n - ip_{n-1})(p'_n + ip'_{n-1}) \end{aligned}$$

follows immediately from Prop^n 3.3 above.

Thus in $Q(i)\langle X\rangle$ f has a factor lattice of length 2. Since the lattice is distributive there are exactly two possible left atomic factors of f, namely $(p_n + ip_{n-1})$ and $(p_n - ip_{n-1})$. But neither of these atoms is stably associated to an element of $Q\langle X\rangle$. (For suppose that $p_n + ip_{n-1} \sim g \in Q\langle X\rangle$. Define $a: Q(i)\langle X\rangle \to Q(i)[z]$ by sending $t_1,\dots,t_{n-1}$ to 1 and t_n to z. Then $a(p_n + ip_{n-1})$ is of the form $Bz + C + Di$, where B,C and D are positive integers; and this must be stably associated to a(g), an element of $Q[z]$. This is clearly impossible.)

Thus f has no proper atomic left factor in $Q\langle X\rangle$ and so f is an atom of $Q\langle X\rangle$.

A particular example of this type of factorization is

$$(xyz + ixy + x + z + i)(zyx - iyx + x + z - i) =$$
$$xyz^2yx + xyzx + xzyx + xyz^2 + z^2yx + x^2 + xz + zx + z^2 + 1.$$

§5. Eigenrings of matrices over free algebras

We start by recalling from §6 of Chapter 1 some general results on eigenrings of matrices. Let R be a persistent semifir over a field k and let A be a full matrix over R. Then

(i) $E_R(A)$ is algebraic over k (1.6.4)

(ii) if A is an atom then $E_R(A)$ is a skew field (1.6.3)

(iii) if A is an absolute atom then $E_R(A) \cong k$ (an immediate consequence of 1.6.5 and 1.6.7).

Of course $k\langle X\rangle$ is a persistent semifir and so these results apply. However in this case we can strengthen (i) (in fact using a different method of proof from that in [4]).

<u>Prop^n 1.1</u> Let A be a full matrix over $R = k\langle X\rangle$. Then $E_R(A)$ is finite-dimensional over k.

<u>Pf</u> We use notation and methods from Chapter 2. First we note that if two matrices are stably associated then their associated torsion modules are isomorphic and hence their eigenrings are also isomorphic. Thus there is no loss in generality in taking A in normal linear form; say

$$A = A_o + \Sigma x_i A_i \qquad (A_o, A_i \in k_n)$$

Now let $P \in I_R(A)$, say $PA = AQ$. We claim that there exists an $M \in R_n$ such that $P - AM$ lies in k_n. Suppose the contrary and let $N \in R_n$ be such that $T = P - AN$ has degree as small as possible. Write $S = Q - NA$. We have $TA = AS$. Comparing leading terms we get;

$$T^{\ell}(\Sigma x_i A_i) = (\Sigma x_i A_i)\, S^{\ell}$$

By the methods of Chapter 2 it follows that T^{ℓ} is a right multiple of $(\Sigma x_i A_i)$, say $T = (\Sigma x_i A_i)W$. By Lemma 2.2.3 $(\Sigma x_i A_i)$ is a non-zerodivisor, so the degree of W is one less than that of T. Set $T' = T - AW$. Then the degree of T' is less than that of T, contradicting the hypothesis.

Thus for each $P \in I_R(A)$ there exists $M \in R_n$ such that $P - AM \in k_n$, say $P - AM = f(M)$. The map $f: I_R(A) \to k_n$ is well-defined, for suppose that both $P - AM$ and $P - AN$ lie in k_n. Then

$$\begin{aligned} A(M - N) &= (P - AN) - (P - AM) \\ &\in k_n. \end{aligned}$$

Comparing terms of highest degree we get

$$(\Sigma x_i A_i)(M - N)^{\ell} = 0$$

and since $(\Sigma x_i A_i)$ is a non-zerodivisor, $(M - N)^{\ell} = 0$ so $M = N$.

It now follows easily that f is a homomorphism with kernel AR_n; hence f induces an embedding $E_R(A) \hookrightarrow k_n$.

<u>Cor^y</u> Let A be a matrix atom over $R = k\langle X\rangle$. Then $E_R(A)$ is a skew field finite-dimensional over k.

If we restrict attention to 1x1 matrices i.e. elements then we have seen that all eigenrings are commutative (Cor[y] to 1.6.7); this result turns on the fact that every factor lattice is distributive. In the general (matrix) case this condition does not hold and it is easy to produce matrices with non-commutative eigenrings - an example is the matrix $\mathrm{diag}(x,x) \in (k[x])_2$ which has eigenring k_2. It is not so evident that matrix atoms can have non-commutative eigenrings, but in fact one can produce arbitrary finite-dimensional skew fields as eigenrings of matrix atoms; the next few pages are devoted to establishing this result.

Prop^n 5.2 Let k be any field, let $X = \{x_{ij} : 1 \leq i,j \leq r\}$ be a set of indeterminates and let $R = k\langle X\rangle$. Let $Q = (x_{ij}) \in R_r$. Then Q is an (absolute) matrix atom.

In order to prove this obvious-looking result we use the following lemma.

Lemma 5.3 Let k be a field, $X = \{x_1,\ldots,x_m\}$ a set of indeterminates. Let $R = k\langle X\rangle$, let $n \leq m$ and define $I = \sum_{i=1}^{n} x_i R$. Then I is a maximal proper n-generator right ideal of R.

Pf Recall that every right ideal J of R is free of unique rank, this rank being denoted by p(J). Let

$$S = \{J \trianglelefteq R : I \subsetneq J \subsetneq R,\ p(J) \leq n\}$$

Suppose that S is non-empty. Choose $J \in S$ of minimal rank, say $p(J) = r$ ($\leq n$). Now choose free generators of J, $y_1,\ldots,y_r$ so as to;

(i) minimize $\max(\partial(y_j))$

(ii) given (i), to minimize the number of i such that $\partial(y_i) = \max(\partial(y_j))$.

Suppose that $\max(\partial(y_j)) > 1$, say (without loss of generality) that $\partial(y_r) > 1$. Now $I \subset J$, so for $j = 1,\ldots,n$

$$x_j = \sum_i y_i a_{ij} \qquad (a_{ij} \quad R)$$

If each $a_{ir} = 0$ then $\sum_{i=1}^{r-1} y_i R \supseteq I$, so by assumption on minimality of p(J) $\sum_{i=1}^{r-1} y_i R = \sum_{i=1}^{n} x_i R$, which is a contradiction (compare ranks). Thus some $a_{ir} \neq 0$, say $a_{jr} \neq 0$. Then

$$\begin{aligned}\partial\left(\sum_i y_i a_{ji}\right) &= \partial(x_j)\\ &= 1\end{aligned}$$

so the set $\{y_1,\ldots,y_r\}$ is right dependent. By the weak algorithm (see Ch 1, §2), y_r is right dependent on $y_1, y_2, \ldots, y_{r-1}$, say $\partial(y_r - \sum_{i=1}^{r-1} y_i b_i) < \partial(y_r)$. But now $y_1, \ldots, y_{r-1}, y_r - \sum_i y_i b_i$ is a generating set of J and it contradicts condition (i) or (ii). Thus $\max(\partial(y_j)) = 1$ i.e. each y_j is of degree 1 or less.

It is now clear that we can choose the generators $y_1, y_2, \ldots, y_r$ of J such that $y_1 = x_1$, $y_2 = x_2, \ldots$ and since $n \geq r$ this means that $J = I$; thus S is the empty set and the result is established.

<u>Pf of Prop^n 5.2</u> Suppose Q has the factorization $Q = AB$ $(A, B \in R_r)$ We show that either A or B is invertible. Consider the first row of the factorization;

$$(x_{11}\ x_{12}\ \ldots\ x_{1r}) = (a_{11}\ a_{12}\ \ldots\ a_{1r})\ B$$

Thus $(\sum a_{1i}R)$ is a n-generator right ideal of R containing $(\sum x_{1i}R)$. By the preceding lemma, $(\sum a_{1i}R) = (\sum x_{1i}R)$ or R.

<u>Case 1</u> $(\sum a_{1i}R) = (\sum x_{1i}R)$. Then there exists $J \in GL_r(R)$ s.t.

$$AJ = \begin{pmatrix} x_{11}\ x_{12}\ \ldots\ x_{1r} \\ * \end{pmatrix}$$

Considering the factorization $Q = AJ.J^{-1}B$ we see that $J^{-1}B = I_r$, so B is invertible.

<u>Case 2</u> $(\sum a_{1i}R) = R$. Then there exists $J \in GL_r(R)$ s.t.

$$\begin{aligned} Q &= AJ.J^{-1}B \\ &= \left(\begin{array}{c|c} 1 & 0 \ \ldots\ 0 \\ \hline c_{21} & \\ c_{31} & A' \\ \vdots & \\ c_{r1} & \end{array}\right) . \left(\begin{array}{c|c} x_{11} & x_{12}\ \ldots\ x_{1r} \\ \hline d_{21} & \\ d_{31} & B' \\ \vdots & \\ d_{r1} & \end{array}\right) \end{aligned}$$

where A' and B' lie in R_{r-1}. Define new variables by

$$y_{1j} = x_{1j} \qquad (r \geq j \geq 1)$$

$$y_{ij} = x_{ij} - c_{i1}x_{1j} \qquad (i>1,\ j \geq 1)$$

The y_{ij} form a set of r^2 elements generating $k\langle X\rangle$; since $|X| = r^2$, they form a free generating set and so the map $x_{ij} \to y_{ij}$ is an automorphism of R. It follows that this change of variable preserves atomicity and invertibility of matrices. Let $Q' = (y_{ij})$. Then

$$Q' = \begin{pmatrix} 1 & & & & \\ -c_{11} & 1 & & & \\ -c_{21} & & 1 & & \\ \vdots & & & \ddots & \\ -c_{r1} & & & & 1 \end{pmatrix} \cdot Q$$

$$= \left(\begin{array}{c|ccc} 1 & 0 & 0 \ldots & 0 \\ \hline 0 & & & \\ \vdots & & A'' & \\ 0 & & & \end{array}\right) \left(\begin{array}{c|ccc} y_{11} & y_{12} & \cdots & y_{1r} \\ \hline d_{21} & & & \\ \vdots & & B'' & \\ d_{r1} & & & \end{array}\right) \qquad (1)$$

where A'' and B'' are A' and B' rewritten in the new variables and the d_{r1}'s are some elements of R. Consider the bottom right-hand $r-1 \times r-1$ submatrix of Q in the above factorization; we get

$$\begin{pmatrix} y_{22} & y_{23} & \cdots & y_{2r} \\ y_{32} & y_{33} & \cdots & y_{3r} \\ \vdots & & & \\ y_{r2} & \cdots & \cdots & y_{rr} \end{pmatrix} = A''\, B''$$

We may assume inductively that the result holds for $r-1 \times r-1$ matrices; hence either A'' or B'' is invertible.

If A'' is invertible, so is A.

If B'' is invertible then

$$A'' = \begin{pmatrix} y_{22} & \cdots & y_{2r} \\ \vdots & & \\ y_{r2} & \cdots & y_{rr} \end{pmatrix} . (B'')^{-1}$$

Now consider the first column of (1);

$$\begin{pmatrix} y_{21} \\ \vdots \\ y_{r1} \end{pmatrix} = \begin{pmatrix} y_{22}. & \cdots & y_{2r} \\ \vdots & & \\ y_{r2} & & y_{rr} \end{pmatrix} . W$$

for some $W \in {}^{r-1}R$. But this is clearly impossible ($y_{21} \notin \sum_{i>1} y_{2i}R$) Thus either A or B is invertible and hence Q is an atom.

Cor^y Let k be a field, $B_1, B_2, \dots, B_n$ ($n = r^2$) a k-basis for k_r and let $Y = \{y_1, \dots, y_n\}$ and $R = k\langle Y\rangle$. Then $Q = \sum_i y_i B_i$ is a matrix atom.

Pf An invertible change of variable does not affect atomicity; and we may clearly make such a change of variable $y_k \mapsto z_{ij}$ to make Q into (z_{ij}). The result now follows by Prop^n 5.2.

We need one more result, on the splitting of extensions, before we can construct the eigenrings.

Prop^n 5.4 Let $R = k\langle X\rangle$, let E/k be a commutative field extension and let $S = R \otimes_k E$. Let

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0 \qquad (1)$$

be a s.e.s. of R-modules and suppose that the induced s.e.s.

$$0 \longrightarrow A\otimes E \xrightarrow{f} B\otimes E \xrightarrow{g} C\otimes E \longrightarrow 0 \qquad (2)$$

of S-modules splits. Then the original s.e.s. of R-modules splits.

Pf Let $h: C\otimes E \longrightarrow B\otimes E$ be the splitting map for (2). For any $c \in C$, $(c\otimes 1)h = \sum_i b_i \otimes e_i$ (where $\{e_i\}$ is some fixed basis for E over k). Define $j: C \rightarrow B$ by $cj = b_1$. We show that $jg = 1$. Now $hg = 1$, so

$$c\otimes 1 = (c\otimes 1)hg = (\sum b_i \otimes e_i)g = \sum_i (b_i g)\otimes e_i$$

(this last equality because g is induced up from g). But $\{e_i\}$

is a basis for E/k; hence $c = b_1 g = c(jg)$. Thus $jg = 1$ and hence j is an R-homomorphism splitting (1).

Th^{m} 5.5 Let D be a skew field of dimension $n = r^2$ over its centre k and let E be a maximal commutative subfield of D (which we may take to be a separable extension of k). Note that $D \hookrightarrow k_n$. Let $A_1, A_2, \ldots, A_n$ be a k-basis of the image of D in k_n and set

$$P = \sum_i x_i A_i \in (k\langle X\rangle)_n.$$

Write $R = k\langle X\rangle$, $S = E\langle X\rangle$. Then

(i) P is an atom of R_n which splits into the product of r stably associated absolute atoms in S

(ii) the eigenring of P (in R_n) is D^{op}.

Pf We have that $|E:k| = r$ and $D \otimes_k E = E_r$. Since the A_i form a k-basis for D they form an E-basis for E_r (in E_n). By the Skolem-Noether Theorem (see e.g. [7] p.222) any two embeddings of E_r in E_n are conjugate; hence there exists $U \in GL_n(R)$ such that the A_i^U form an E-basis for the copy of E_r consisting of matrices of the form

$$\begin{pmatrix} C & & & \\ & C & & \\ & & \ddots & \\ & & & C \end{pmatrix} = C \otimes I_r \qquad (C \in E_r)$$

Let $A_i^U = B_i \otimes I_r$. In S_n P is stably associated to $\sum x_i A_i^U$, and it is clear that $\sum x_i A_i^U$ decomposes into r factors, each stably associated to $Q = \sum x_i B_i$. Hence we have a decomposition

$$({}^nS)/P({}^nS) \cong \bigoplus ({}^nS)/Q_i({}^nS) \qquad (\text{each } Q_i \sim Q).$$

Hence $$E_S(P) \cong (E_S(Q))^r.$$

But by the corollary following Prop^{n} 5.2, Q is an absolute atom and so $E_S(Q) \cong E$. Thus $E_S(P) \cong E_r$.

Now consider $E_R(P)$. It clearly contains those matrices in k_n centralizing each A_i, so $E_R(P) \supseteq D^{op}$. But

$$|E_R(P):k| = |E_S(P):E| = r^2 = n = |D^{op}:k|$$

so $E_R(P) \cong D^{op}$.

It only remains to verify that P is an atom of R. Let M be the torsion module associated with P and suppose that N is a torsion R-submodule. Since $End_R(M)$ is a skew field ($\cong D^{op}$) , the s.e.s.

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

cannot be split. By Prop^n 5.4 it follows that the s.e.s.

$$0 \longrightarrow N\otimes E \longrightarrow M\otimes E \longrightarrow M/N\otimes E \longrightarrow 0$$

is also not split. But $M\otimes E$ is a fully reducible torsion module and N a torsion S-submodule, so the sequence must split. ※ . Thus M is a simple torsion module and P is an atom of R.

References

[1] P.M. Cohn. Free rings and their relations. No 2, LMS monographs, Academic Press (London and New York 1971).

[2] P.M. Cohn. The Cayley-Hamilton theorem in skew fields. Houston J. Maths, Vol 2, No 1 (1976).

[3] P.M. Cohn. Skew field constructions. LMS lecture note series 27, Cambridge University Press (Cambridge 1977).

[4] P.M. Cohn. The universal field of fractions of a semifir, Part 1. To appear Proc. LMS.

[5] G. Grätzer. General lattice theory. Birkhauser Verlag (Basel and Stuttgart 1978).

[6] N. Jacobson. Lectures in Abstract Algebra III. Van Nostrand. (New York and London 1964).

[7] N. Jacobson. Basic Algebra II. W.H. Freeman & Co. (San Francisco 1980).

[8] J.P. Serre. Local Fields. Springer Verlag. (New York 1979).