REPRESENTATIONS OF MATROIDS

by

Norman Elliott Fenton

A thesis presented in support of
an application for the degree of
Doctor of Philosophy at the
University of Sheffield.

Department of Pure Mathematics,
The University of Sheffield,
October, 1981.

CONTENTS

INTRODUCTION

The concept of matroids was originally introduced by Whitney and Van der Waerden in the 1930's to generalise the notion of linear dependence in a vector space; certain axioms satisfied by this relation were observed to be satisfied by other types of 'dependence' relations, such as algebraic dependence and 'cycle' dependence in a graph. Consequently a matroid was defined to be a set with an abstract dependence relation satisfying these axioms. One of the most natural questions to ask is whether every such 'matroid' is representable in the obvious sense in a vector space. The answer is of course no (otherwise matroid theory would be equivalent to linear algebra) although in the early years of the subject examples of non-representable matroids were not easily obtainable. In this thesis we continue the work of Ingleton (in [20]) and Vámos (in [35,36]) on the representation problem, buiding up to an algebraic treatment in the important last chapter.

Chapter one is essentially preliminary material and is subdivided into four sections which, broadly speaking, reflect the subject content of the rest of the thesis :-

1) Algebra in which the basic set notation and algebraic conventions are listed. Since the main body of the thesis is in matroid theory rather than algebra, we have listed here without proof as many as possible of the algebraic definitions and theorems which we will be using to avoid cluttering up the text later on. However, because of the specialised nature of some of the algebraic machinery (notably in §5) some has had to be deferred until the relevant stage in the thesis. Standard texts which adequately cover all the necessary algebra here are [2,8,14,42].

2) Projective geometry. This is a constantly recurring theme throughout and this preliminary account prepares the reader for the more substantial material which appears in §2 and in particular in §4. For a fuller account

we refer to [3,24,25].

3) Graph Theory. We shall assume a familiarity with the basic notions of graph theory but list here some particularly relevant definitions and results. A good account of the subject may be found in [17].

4) Matroid Theory. Being a relatively new development in mathematics, matroid theory has even fewer universally accepted definitions and notation than other more established branches of the subject, and consequently it is a prerequisite to lay these down from the outset. In doing this it should be noted that for my own purposes it has been inconvenient to follow exactly the notation of any one standard work, although [37] is the closest approximation for definitions and conventions. The texts [1,10,15,34,37] adequately cover most results listed here and are a continual source of reference throughout the rest of this work.

In chapter two we make a detailed study of the notion of projective equivalence of matrices. Although labourious and technical in places, the work here is of fundamental importance for this thesis since projectively equivalent matrices represent the same isomorphism class of matroids. We show by construction (Theorem (2.8)) the existence of a 'canonical'form with respect to the relation of projective equivalence. This is achieved by introducing the notion of s-projective equivalence and the atomic entries of a matrix. Once the atomic entries of a matrix are known, the proof of (2.8) provides an algorithm for determining the projective canonical form. Using the projective canonical form we provide a new proof of the 'second fundamental theorem of projective geometry', and proofs of the uniqueness of representability of binary and ternary matroids (Theorems (2.13) and (2.18)). In [12], Brylawski and Lucas have also studied this problem (from a different angle) and we describe the connection between the two different approaches (Theorem (2.19) being the important 'link'), although it must be stressed that the work here was achieved without the aid of [12]. We conclude the chapter by describing the 'step diagonal form' of a matrix (definition (2.24)) and show in (2.25) that every matrix is permutation equivalent to a matrix in step diagonal form. The relevance of this result is indicated by proposition (2.26) which has important implications for later chapters.

In chapter three we study a class of matroids (which I call 'atomic matroids') arising naturally from the work in §2. In Theorem (3.6) we show that atomic matroids are precisely binary fundamental transversal matroids (described in [6,9]). In (3.7) we introduce a class of graphs called A-graphs, and prove that atomic matroids are precisely the cycle matroids of A-graphs (Theorem (3.12)), thus providing a complete graphical characterization of binary fundamental transversal matroids.

In chapter four we return to the main theme of the thesis; we are primarily interested here in the representations of matroids defined by dependence of points from a projective space. We describe a method for constructing matroids which are in an important sense 'uniquely representable' (Theorem (4.10)) and this leads to a procedure for constructing matroids with certain predetermined characteristic sets.(Examples (4.14)).

The notion of generalised projective equivalence is introduced (definition (4.15)) and we show that from both an algebraic and geometric viewpoint (Theorems (4.21),(4.23)) this notion is essentially the same as projective equivalence. In Theorem (4.17) we prove that any two representations of a full projective geometry (over an arbitrary field) are generally projectively equivalent, thus generalising a result in [12] which states that full projective geometries over finite prime fields are uniquely representable.

The chapter concludes with a section on the representation of uniform matroids; the significant problem is to determine the smallest field over which a uniform matroid is representable, and we show (proposition (4.26)) that this is essentialy equivalent to determining the maximum value k for which k-arcs exist in a certain projective space. The latter problem has been studied extensively by geometers, and we show how considerable simplifications of the proofs of some of their important results ((4.27)-(4.31)) can be achieved by using (4.26) together with straightforward matroid arguments.

In chapter five, which forms a substantial proportion of the thesis, we reduce the whole problem of matroid representation to an algebraic problem. The main result of Vámos in [35] (given here as Theorem (5.5)) leads fairly naturally to the construction of a ring A_M (which I have called the Vámos ring) associated with each matroid M. This ring is a polynomial type ring based on a generic matrix X of indeterminates, and is non-zero precisely when M is representable (Proposition (5.7)). Theorems (5.8) and (5.15) show that A_M is a 'universal object' with respect to representations of M, and there is a natural correspondence (although not a bijection) between the prime ideals of A_M and the representations of M (Corollary (5.9)). Consequently by using only some well known results from commutative ring theory we are able to deduce results about representability which were previously very difficult to prove (for example (5.11) and (5.13)). Although the ring A_M has some very nice properties, it is based on too many indeterminates to be explicitly described easily even for the simplest matroids M. Consequently by a two stage process of simplification which corresponds to reducing the matrix X first to column echelon form and then to projective canonical form, we are able to define new rings R_M, V_M with successively fewer indeterminates, such that both rings retain all the important properties of A_M. At the same time we are able to determine the exact algebraic relationship between the three rings (Theorems (5.22) and (5.26)) so that we are justified in restricting our attention to the simplest of the rings V_M. The most remarkable by-product of this simplification is theorem (5.24); that the natural correspondence between the prime ideals of V_M and the representations of M in projective canonical form is actually a bijection. Thus the representation problem is reduced to the study of the prime ideal structure of V_M and on this we can bring the full weight and sophisticated machinery of commutative algebra to bear. We are thus able to determine explicitly (in (5.28)) the ring V_M for many important classes of matroids, the most satisfing of these results being that V_M is equal to the ring of integers if and only if M is regular. We also provide a partial solution to the problem of determining which rings can arise as Vámos rings of matroids (5.28.7)).

In theorems (5.19),(5.29),(5.21), we determine the effect on V_M of performing matroid operations on M, and the chapter concludes by exhibiting a relationship (Theorem(5.29)) between the Vámos ring and White's bracket ring (described in [38,39,40,41]).

Apart from chapter one, all results appearing in the text which are not attributed to any author or which have no reference provided, are to the best of my knowledge new.

ACKNOWLEDGEMENTS

I am indebted to my supervisor Peter Vámos for his very generous assistance with this thesis, and also to the Science Research Council for their financial support.

I would also like to thank the referee of my article entitled 'Characterization of atomic matroids' (submitted to the Quarterly Journal of Mathematics, Oxford) whose comments I believe have greatly improved the contents of chapter three, and J.W.P. Hirschfeld, who provided me with the historical background to the problem of finding maximal k-arcs (in chapter four).

In addition to those above I would also like to thank a number of people whose interest and help have influenced the contents of this thesis ; these are Victor Bryant, Haya Freedman, David Jordan, Hazel Perfect, Rodney Sharp, and Andy Wiseman.

REPRESENTATIONS OF MATROIDS

by

Norman Elliott Fenton

SUMMARY

Chapter one is preliminary material subdivided into the four main sections which reflect the subject content of the thesis, 1) algebra, 2) projective geometry, 3) graphs, 4) matroid theory.

In chapter two we make a detailed study of the notion of projective equivalence of matrices, showing by construction the existence of a canonical form with respect to this relation. The relevance of this is that projectively equivalent matrices represent the same isomorphism class of matroids.

In chapter three we study a class of matroids which arises naturally from the work of the previous chapter, showing that these are precisely binary fundamental transversal matroids. We provide a complete gaphical characterization of these matroids.

In chapter four we are interested in the representations of matroids defined by dependence of points from a projective space. We establish the uniqueness of representability of certain matroids including all full projective geometries. The representation of uniform matroids is also tackled from a geometrical viewpoint.

In chapter five we show that we can associate a ring with each matroid M in such a way that this ring is a universal object with respect to representations of M. There is a natural bijection between the prime ideals of this ring and the projective equivalence classes of representations of M.

§1 PRELIMINARIES

1. Algebra

The usual set theoretic notation is adopted throughout. The symbol $\subset$ denotes containment but not necessarily strict containment. The empty set is denoted by ϕ ; the expression $X\backslash Y$ denotes the set difference of X and Y, and the cardinality of a set X is denoted by $|X|$.

Unless otherwise stated all rings are commutative with identity and by a ring homomorphism we shall mean a homomorphism which preserves the identity. A ring isomorphism is a homomorphism which is both injective (one -to-one) and surjective (onto). An automorphism of a ring A is an isomorphism of A onto itself. The ring of integers is denoted by $\mathbb{Z}$, and the ring of rational numbers is denoted by $\mathbb{Q}$.

The only rings to be considered which are not assumed to be commutative are division rings ; a division ring is a ring in which every non-zero element has a multiplicative inverse. A (non-zero) division ring which is also commutative is a field. A ring without zero-divisors is an integral domain ; every integral domain possesses a quotient field which is unique up to isomorphism. An ideal $\underline{a}$ of A is prime if for any $x,y \in A$, $xy \in \underline{a}$ implies $x \in \underline{a}$ or $y \in \underline{a}$. The collection of prime ideals of A is denoted by Spec A. An ideal of A is maximal if it is not properly contained in any other ideal of A. For any ideal $\underline{a}$, the quotient ring $A/\underline{a}$ is an integral domain if and only if $\underline{a} \in$ Spec A, and is a field if and only if $\underline{a}$ is a maximal ideal. Every maximal ideal is prime and every ring A ($\neq 0$) contains at least one maximal ideal. The ring A is Noetherian if every ideal is finitely generated.

Let A,B be rings. Then B is said to be an A-algebra if there is a homomorphism $f: A \to B$ for which B is an A-module with respect to 'multiplication' defined by

$$ab = f(a)b \qquad \text{for } a \in A,\ b \in B$$

In particular, every ring is a $\mathbb{Z}$-algebra (via the mapping $n \to n.1$) and if

A contains a field F as a subring, then A is an F-algebra (via the inclusion mapping). These are the only examples of algebras we shall need .

For any two rings A,B, by a product (C,γ,ψ) of A,B (over $\mathbb{Z}$) we mean a ring C and homomorphisms $\gamma:A \to C$, $\psi:B \to C$, such that C is generated by $\{\gamma(A), \psi(B)\}$. In particular the tensor product of A and B (over $\mathbb{Z}$), which always exists, is denoted by $A \otimes_{\mathbb{Z}} B$ and is characterized by the following

(1.1)Proposition (Universal mapping property of tensor products).

T.F.A.E. (the following are equivalent)

i) The product (C,γ,ψ) of A and B (over $\mathbb{Z}$) is a tensor product of A and B.

ii)Given any two homomorphisms g and h of A and B respectively into a ring D, there exists a homomorphism $f:C \to D$ such that $f=g\gamma^{-1}$ on $\gamma(A)$ and $f=h\psi^{-1}$ on $\psi(B)$.

Analagous results hold when $A \otimes_R B$ is the tensor product over R of two R-algebras A,B.

For any ring A and abelian group G, the group ring of G over A is denoted by A(G). If H is the free abelian group on t generators $x_1,\ldots,x_t$ (so that H consists of all elements of the form $x_1^{n_1}\ldots x_t^{n_t}$ where the $n_i \in \mathbb{Z}$), the group ring A(H) is usually denoted by $A\langle x_1,\ldots,x_t\rangle$.

For any integer $q=p^t$ where p is a positive prime and t is a positive integer, there is (up to isomorphism) a unique field of q elements; this field is denoted by GF(q). Conversely every finite field is isomorphic to some GF(q).

(1.2)Proposition: The field GF(q) possesses non-identity automorphisms if and only if q is non-prime.

For any field F the prime subfield of F is the smallest subfield contained in F. Up to isomorphism the prime subfield is always either $\mathbb{Q}$ or GF(p) for some prime p. The characteristic of F, denoted char(F) ,is defined to be zero if the prime subfield of F is $\mathbb{Q}$, and p if the prime subfield of F is GF(p).

For any fields E,F, the field E is called an extension of F (written E/F) if $E \supset F$. If $\alpha_1, \ldots, \alpha_n \in E$ we write $F(\alpha_1, \ldots, \alpha_n)$ for the subfield of E generated by $\alpha_1, \ldots, \alpha_n$ over F. An element $\alpha \in E$ is algebraic over F if $f(\alpha)=0$ for some non-zero polynomial $f(X) \in F[X]$. If α is not algebraic over F, α is transcendental over F. The extension E/F is an algebraic extension if every element in E is algebraic over F, and is a transcendental extension otherwise.

Given any field extension E/F, let $\alpha_1, \ldots, \alpha_n, \beta \in E$. Then β is algebraically dependent on $\alpha_1, \ldots, \alpha_n$ over F if β is algebraic over $F(\alpha_1, \ldots, \alpha_n)$. If $X \subset E$, the elements of X are said to be algebraically independent over F if each finite subset of X consists of elements which are algebraically independent over F. Such a set X is called a transcendence set (over F); a transcendence set X in E is called a transcendence basis of E/F if it is maximal, that is, if X is not a proper subset of another transcendence set.

(1.3) Proposition Transcendence bases for E/F always exist, and any two have the same cardinality. Moreover a transcendence set X is a transcendence basis of E/F if and only if E/F(X) is an algebraic extension.

The common cardinality of the various transcendence bases of E/F is called the transcendence degree of E/F, written tr.d (E/F).

(1.4) Proposition Suppose $F \subset E \subset K$ are successive field extensions. Then

$$\text{tr.d}\,(K/F) = \text{tr.d}\,(K/E) + \text{tr.d}\,(E/F)$$

A field is algebraically closed if it possesses no proper algebraic extensions. If K/F is an algebraic extension, then K is said to be the algebraic closure of F if i) K/F is algebraic, and ii) K is algebraically closed.

(1.5) Theorem If F is a field then there exists an algebraic closure of F, and any two algebraic closures of F are isomorphic fields.

The following well known theorem can be found in [38] p.107

(1.6)Theorem Let K be an algebraically closed field and let E/F be an algebraic extension. If $\sigma: F \to K$ is a monomorphism (injective homomorphism), then σ can be extended to a monomorphism $\sigma': E \to K$.

(1.7)Corollary Suppose F_1, F_2 are fields with the same algebraic closure K. If $\sigma: F_1 \to F_2$ is an isomorphism then there is an automorphism σ' of K which extends σ.

Proof Take E=K and $F=F_1$ in (1.6). Certainly then σ is a monomorphism of F_1 into K which can be extended to a monomorphism $\sigma': K \to K$. But σ' must be surjective (and hence an automorphism) for otherwise $\sigma'(K)$ is an algebraic closure of F_2 strictly contained in K and this is impossible since $K/\sigma'(K)$ is then a proper algebraic extension.

A basic knowledge of linear algebra will be assumed. A vector will mean a row vector and will be denoted by $\underline{v}$. The transpose of a matrix A will be denoted by A^T. The $(r\times r)$ identity matrix is denoted by I_r, and a diagonal matrix $\begin{bmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_r \end{bmatrix}$ is denoted by $\mathrm{diag}(a_1,\ldots,a_r)$.

2. Projective Geometry

A projective space (or projective geometry) is a system consisting of a set $\mathcal{P}$ of points together with certain subsets $\mathcal{L}$ of $\mathcal{P}$ called lines such that $(\mathcal{P},\mathcal{L})$ satisfies the following axioms:-

(i) any two distinct points are on exactly one line

(ii) if x,y,z,w are four distinct points, no three of which are collinear (on the same line) and if xy (the unique line containing x and y) intersects zw then xz intersects yw.

(iii) each line contains at least three points.

A subset $\Pi \subset \mathcal{P}$ is called a subspace if for any two distinct points of Π it contains the whole line determined by them. It follows from (ii) that subspaces can also be introduced inductively using the concept of dimension (which in the event of possible confusion will be specified as projective dimension) :- A point is a subspace of dimension 0, a line is a subspace of dimension 1. If Π is a subspace of dimension d and if the point $x \notin \Pi$, then Π together with all the lines joining x to points of Π is a subspace of dimension $d+1$. If for some integer n, $\mathcal{P}$ has dimension n, we say that the projective space $(\mathcal{P},\mathcal{L})$ has dimension n, otherwise $(\mathcal{P},\mathcal{L})$ is called an infinite dimensional projective space. If $(\mathcal{P},\mathcal{L})$ has dimension $n \geq 1$, a hyperplane of $(\mathcal{P},\mathcal{L})$ is an $(n-1)$-dimensional subspace of $(\mathcal{P},\mathcal{L})$. Projective spaces of dimension 2 are usually called projective planes; we shall be generally only considering projective spaces of finite dimension $n \geq 2$. For any subspace Π of a projective space we define rank Π = dimension $\Pi + 1$

(1.8) Definition Suppose $\Gamma = (\mathcal{P},\mathcal{L})$ is a projective space of dimension n. A simplex in Γ is a set of $n+2$ points, no $n+1$ of which are contained in a hyperplane of Γ. When $n=2$, a simplex of Γ is called a quadrangle.

(1.9) Definition Suppose $\Gamma = (\mathcal{P},\mathcal{L})$, $\Gamma' = (\mathcal{P}',\mathcal{L}')$ are two projective spaces. A projectivity (or isomorphism) from Γ to Γ' is a one-to-one, order preserving mapping of the partially ordered set of all subspaces of Γ upon the partially ordered set of all subspaces of Γ'.

Given a collection of points $x_1,\ldots,x_m$ in a projective space it is easily seen that there is a unique smallest subspace containing $\{x_1,\ldots,x_m\}$, called the subspace spanned by $x_1,\ldots,x_m$ and denoted by $\langle x_1,\ldots,x_m\rangle$. The set of points $x_1,\ldots,x_m$ is said to be dependent if for some $1 \leq i \leq m$, $x_i \in \langle x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_m\rangle$. A set of points which is not dependent is said to be independent.

The projective geometry PG(m,F)

Suppose F is a field and F^m the collection of ordered m-tuples of F, so that F^m is a vector space over F of (vector space) dimension m. Let $\mathcal{P}$ be the collection of one-dimensional subspaces of F^m and let $\mathcal{L}$ be the collection of two-dimensional subspaces (planes) of F^m. The full projective geometry of rank m (or (projective) dimension m-1) is $(\mathcal{P},\mathcal{L})$ where a 'point' P is on the 'line' ℓ if and only if $P \subset \ell$ in F^m. Thus the 'points' of PG(m,F) have the form $P=F\underline{v}$ where $0 \neq \underline{v} \in F^m$, and we shall call $\underline{v}$ a coordinate vector of P ; if $|F| = q < \infty$, there are q-1 distinct coordinate vectors of P, but it is easily seen (in all cases) that there is a unique coordinate vector whose first non-zero coordinate is equal to 1, and we shall call this the natural coordinate vector of P. If we identify the points of PG(m,F) with their natural coordinate vectors in F^m then for k=0,1,...,m-1 the subspaces of PG(m,F) of (projective) dimension k (or rank k+1) correspond precisely to the (k+1)-dimensional subspaces of F^m.

In PG(m,F) the notion of dependence corresponds corresponds to linear dependence over F if again we identify points with their coordinate vectors. For most of our purposes F will be finite, hence a field of $q=p^t$ elements for some prime p and integer $t \geq 1$. In this case PG(m,F), alternatively denoted PG(m,q), is a finite projective geometry with $q^{m-1}+\ldots+q+1$ points. The projective plane PG(3,2) (of 7 elements) is the smallest non-trivial example of a projective space and is called the Fano plane. It should be noted that some authors write PG(m-1,F) for our PG(m,F). Also the full projective geometry PG(m,D) is defined in an analagous way when D is a division ring.

The following classical result may be found in [3] p.302

(1.10) Theorem Any projective geometry of rank $m \geq 4$ is isomorphic to PG(m,D) for some division ring D ; a projective plane is isomorphic to PG(3,D) for some division ring D if and only if the plane is Desarguesian (see [24],p.140 for definition).

By Wedderburn's theorem (see for example [14]) every finite division ring is a field, hence by (1.10) we deduce that every finite projective geometry of rank $m \geq 4$ is isomorphic to $PG(m,F)$ for some field F, and that every finite Desarguesian plane is isomorphic to $PG(3,F)$ for some field F.

(1.11)Definition Let V,W be vector spaces over fields F,K respectively. A semi-linear transformation of V upon W is a pair $\sigma = (\sigma', \sigma'')$ consisting of an isomorphism σ' of the additive group of V upon the additive group of W, and a field isomorphism of F upon K subject to

$$\sigma'(\alpha \underline{v}) = \sigma''(\alpha)\sigma'(\underline{v}) \quad \text{for each} \quad \alpha \in F, \ \underline{v} \in V$$

If $F=K$ and $\sigma'' = id_F$, then σ is a linear transformation. When we are considering a vector space V of dimension m over F we shall usually take $V=F^m$.

(1.12)Proposition Suppose $\sigma = (\sigma', \sigma'')$ is a semi-linear transformation of F^m upon K^m. Then σ induces a projectivity between $PG(m,F)$ and $PG(m,K)$.

Proof Suppose S is a subspace of $PG(m,F)$ of rank k for some $0 \leq k \leq m-1$, so that (by the above mentioned convention) S corresponds to a k-dimensional subspace of the vector space F^m. The set $\sigma(S)$ of all elements $\sigma'(s)$ with $s \in S$ is clearly a subspace of K^m. Hence the mapping of the subspace S of $PG(m,F)$ upon the subspace $\sigma(S)$ of $PG(m,K)$ is the desired projectivity.

The converse to the above result for projective geometries of rank $m \geq 4$ is the following 'first fundamental theorem of projective geometry'.

(1.13)Theorem For $m \geq 3$ any projectivity of $PG(m,F)$ upon $PG(m,K)$ is induced by a semi-linear transformation of F^m upon K^m.

Proof See [3], p 44-48

A projectivity of $PG(m,F)$ upon itself is called an auto-projectivity of

PG(m,F). By (1.13) any auto-projectivity is induced by a semi-linear transformation of F^m. Consequently we have:-

(1.14) Definition An auto-projectivity which is induced by a linear transformation is called a collineation.

(1.15) Theorem ('Second Fundamental Theorem of Projective Geometry') In PG(m,D) (where D is a division ring, $m \geq 2$) there is one and only one collineation mapping any given simplex onto another given simplex if and only if D is a field.

Proof See [3] pp.66-68.

3. Graphs

All graphs considered will be finite, that is, if G(V,E) (or more simply G) is a graph then the vertex set V and the edge set E are both finite. The notions of loop, parallel edge, simple graph, subgraph, isomorphism, homeomorphism, tree, forest, connected component, path, cycle, contraction, deletion are all defined as in [17]. With these definitions we have the following well known result:-

(1.16) Proposition If the graph G(V,E) has k connected components then any spanning forest for G has exactly $|V| - k$ edges.

If the vertex set of a graph can be partitioned into two sets V_1, V_2 in such a way that every edge of the graph joins a vertex of V_1 to a vertex of V_2 then the graph is said to be bipartite. A complete graph is a simple graph in which an edge joins each pair of vertices. The complete graph on n vertices is denoted by K_n. If a bipartite graph has the property that every vertex of V_1 is joined to every vertex of V_2 and it is simple then it is called a complete bipartite graph and is denoted by $K_{m,n}$ where $m = |V_1|$ and $n = |V_2|$. The graph obtained from the cycle of length k on replacement of each edge by a pair of parallel edges is denoted by C_k^2 .

The graph obtained from G by subdividing an edge e into two edges is called the series extension of G at e. The graph obtained by adding an edge parallel to e is called the parallel extension of G at e. A series-parallel network is a graph which can be obtained from a single edge (which may be a loop) by a finite sequence of series and parallel extensions.

4. Matroid Theory

(1.17) Definition A matroid $M(E)$ (or simply M) consists of a finite set E, together with a non-empty collection ξ of subsets of E, called the independent sets, which satisfy the following two axioms :-

1) If $A \in \xi$ and $B \subset A$, then $B \in \xi$.
2) If $A, B \in \xi$ with $|A| = |B| + 1$, then there exists an $x \in A \backslash B$ such that $B \cup \{x\} \in \xi$.

(1.18) Proposition Suppose A, B are independent in M with $|B| < |A|$. Then there exists $C \subset A \backslash B$ such that $|B \cup C| = |A|$ and $B \cup C$ is independent.

(1.19) Definition Two matroids M_1 and M_2 on E_1 and E_2 respectively are isomorphic if there is a bijection $\psi : E_1 \to E_2$ which preserves independence.

(1.20) Examples

1) The most natural example of a matroid is a finite set of vectors together with the collection of its linearly independent subsets. The central theme of this thesis concerns matroids which are isomorphic to matroids arising in this way. (We shall presently give an alternative definition of these so-called 'linearly representable' matroids). Closely related to this example is :-

2) Any finite set of points of a full projective geometry $PG(m,D)$ together with the collection of its independent subsets. In particular, for the finite field $GF(q)$, $PG(m,q)$ itself may be viewed as a matroid on $q^{m-1} + \dots + q + 1$ elements. The Fano plane $PG(3,2)$ is usually called the Fano matroid when viewed in this way and is denoted by F_7.

3) Let $G = G(V,E)$ be a graph. Let $X \in \xi$ if and only if X does not contain a cycle of G (for $X \subset E$). Then ξ is the collection of independent sets of a matroid on E, called the cycle matroid of G, denoted by $M(G)$. An arbitrary matroid M is graphic if there is a graph G for which M is isomorphic to $M(G)$.

4) Suppose F,K are fields with $F \subset K$. Let E be a finite subset of K and let $X \in \xi$ if and only if $X \subset E$ and the elements of X are algebraically independent over F. Then ξ is the collection of independent sets of a matroid on E.

5) Let E be a set of cardinality n, and let ξ be the collection of subsets of cardinality $\leq r$ (where $r \leq n$). Then ξ is the collection of independent subsets of a matroid on E called the Uniform matroid (of rank r, size n) and is denoted by $U_{r,n}$.

6) If $\mathcal{A}$ is a family of finite subsets of a set E then the collection partial transversals of $\mathcal{A}$ (see, e.g. [1] p.279) is the set of independent sets of a matroid on E. An arbirary matroid M on E is called a transversal matroid if there exists some family

$\mathcal{A} = \{X_1,\ldots,X_t\}$ say of subsets of E such that $\xi(M)$ is the family of partial transversals of $\mathcal{A}$. This matroid is denoted by $M[X_1,\ldots,X_t]$ and we call $\mathcal{A}$ a presentation of M. In this case, if $E = \{e_1,\ldots,e_n\}$, then the matrix induced by the presentation is the $(n\times t)$ zero-one matrix whose $(i,j)^{th}$ entry is equal to 1 if $e_i \in X_j$.

For a matroid M on E the notions of basis, circuit and rank are defined in a manner entirely analagous to the same concepts in vector spaces; thus a basis of M is a maximal independent subset, a circuit is a minimal dependent set, and the rank of a set $A \subset E$ is the cardinality of a maximal independent subset of A (and is denoted by $\rho(A)$). The rank of the matroid M is the rank of E, i.e. the common cardinality of any basis of M, so that for example the uniform matroid $U_{r,n}$ has rank r. In the case of a graphical matroid M(G), the circuits of M(G) are precisely the cycles of G, and the bases are precisely the spanning forests. Consequently, by (1.16), we now have :-

(1.21) Proposition If the graph G=G(V,E) has k connected components, then the cycle matroid M(G) has rank $|V| - k$.

Any one of the concepts of bases, circuits or rank could have been used (instead of independent sets) to axiomatize matroids, for example we have :-

(1.22) (Basis axioms) A non-empty collection $\mathcal{B}$ of subsets of E is the set of bases of a matroid on E if and only if it satisfies

Whenever $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \backslash B_2$, there is a $y \in B_2 \backslash B_1$ such that $(B_1 \cup \{y\}) \backslash \{x\} \in \mathcal{B}$.

(1.23) (Circuit Axioms) A collection of subsets $\mathcal{C}$ of E is the set of circuits of a matroid on E if and only if it satisfies:-

1) If $C \in \mathcal{C}$ then no proper subset of C is in $\mathcal{C}$.

2) If C_1, C_2 are distinct members of $\mathcal{C}$ and if $x \in C_1 \cap C_2$ then there is a $C_3 \in \mathcal{C}$ such that $C_3 \subset (C_1 \cup C_2) \backslash \{x\}$.

A loop of M(E) is an element $x \in E$ such that $\{x\}$ is a dependent set. Two elements $x, y \in E$ are said to be parallel if neither are loops and $\{x,y\}$ is a dependent set. We shall also say that x is a parallel element if for some $y \in E$, x,y are parallel. A coloop is an element which is contained in every basis of M. In the case of a graphical matroid, loops and parallels correspond precisely to the graph-theoretical notions. As for graphs a simple matroid is then a matroid without loops or parallels. Associated with every matroid M(E) is a canonical simple matroid $M_0(E_0)$, the underlying simple matroid of M(E), which may be constructed as follows:-

(1.24) Let $E' = \{e \in E;\ e \text{ not a loop}\}$. For each $e \in E'$ let $[e]$ denote the equivalence class of elements parallel to e (with the convention that $[e] = \{e\}$ if e is not a parallel). Let $\bar{e}$ be a unique representative of $[e]$. Write $E_0 = \{\bar{e};\ e \in E'\}$, then M_0 is the matroid on E_0 for which a subset $\bar{A} \subset E_0$ is independent in M_0 if and only if A is independent in M.

(1.25) Corollary For a finite field F, PG(m,F) (viewed as a matroid as in (1.20.1)) is the underlying simple matroid of F^m (viewed as a matroid as in (1.20.1)).

For any suset $E' \subset E$ the matroid M induces two matroids on E' which correspond in the natural way to subgraphs of a graph obtained by deletion and contraction of edges. The restriction of M to E', written $M|_{E'}$ is the matroid on E' whose independent sets are precisely those subets of E' which are independent in M. In a graph this corresponds to 'deleting' the edges $E\backslash E'$. We shall write $M\backslash E'$ for $M|_{E\backslash E'}$ and say that $M\backslash E'$ is the matroid formed from M by deleting the set E'. The contraction of M to E', written $M_{\otimes E'}$ is the matroid on E' in which a subset $A \subset E'$ is independent if and only if $A \cup B$ is independent in M for some basis B of $M\backslash E'$. In a graph this corresponds to 'contracting away' the edges $E\backslash E'$. We shall write M/E' for the matroid $M_{\otimes E\backslash E'}$ and say that M/E' is the matroid formed from M by contracting away from E'.

The dual matroid of M, denoted M^* is the matroid on E whose collection of bases is the set $\{E\backslash B;\ B \text{ is a basis of } M\}$. For example the dual of $U_{r,n}$ is precisely $U_{n-r,n}$. It is clear that $(M^*)^* = M$. A set $A \subset E$ is a cobasis (cocircuit) if A is a basis (circuit) in M. Restriction, contraction and dual are related by the following well known result (see, e.g. [10] p.38, or [37] p.63):-

(1.26) Proposition For any subset $E' \subset E$, $M/E' = (M^*\backslash E')^*$

If $E' \subset E$ a matroid M' on E' is called a minor of M if M' is obtained from M by any combination of restrictions and contractions. Suppose now that $M_1, \ldots, M_t$ are matroids respectively on the (pairwise disjoint) sets $E_1, \ldots, E_t$. Write $E = \cup E_i$. The direct sum of the matroids M_i $(i=1,\ldots,t)$, written $M_1 \oplus \ldots \oplus M_t$ is the matroid on E whose collection of bases is the set

$$\{B_i : B_i \text{ is a basis of } M_i \text{ for } i=1,\ldots,t\}$$

For any two elements $x, y \in E$, x is connected to y if $x=y$ or there is a circuit of M which contains both x and y. This is an equivalence relation on E whose equivalence classes are called the connected components of M. If there is one connected component then then M is connected. Clearly, loops and coloops are connected components of M. It must be noted that the definition of connectivity does not correspond to connectivity in a graph, but we do have the following important result(see [17] p.27)

(1.27) Theorem Suppose G is a connected graph without loops and having at least 3 vertices. T.F.A.E.

(i) $M(G)$ is a connected matroid

(ii) G is a 2-connected graph

For our purposes the following (easily proved) characterization of the connected components of M will be particularly useful.

(1.28) Suppose M has connected components $E_1, \ldots, E_t$.

$$\text{Then } M = M_{|E_1} \oplus \cdots \oplus M_{|E_t}$$

The remaining definitions and results in this section are crucial for the understanding of this thesis. In particular it should be noted that where I am using rows of a matrix some authors are using columns.

(1.29) Definition The matroid M is said to be (linearly) representable over a field F (or simply F-representable) if there is a one-to-one correspondence between the elements of E and the rows of a matrix A over F such that dependence in M corresponds to linear dependence (over F) of rows of A. The matrix A is said to be a representation of M over F (or an F-representation). If M is representable over at least one field, we say that M is a (linearly) representable matroid.

It is not difficult to see that the above definition is equivalent to the definition suggested in (1.20.1). Henceforth we shall always assume that M has size n and rank r, in which case it is easily seen that we may always assume that a representation matrix A of M is an $(n \times r)$ matrix.

Suppose now that A is an arbitrary $(n \times r)$ matrix over a field F whose rows are indexed by the n elements of E. For each $X \subset E$, let $A(X)$ denote the $(|X| \times r)$ submatrix of A consisting of those rows indexed by X. Then the following result (which is easily proved using (1.18)) provides us with a workable criteria for determining whether A is an F-representation of M, a result which will be used extensively and without further comment throughout this work:-

(1.30) Proposition For an $(n \times r)$ matrix A over F, T.F.A.E.

(i) A is an F-representation of M.

(ii) For every r-subset $X \subset E$, X is a basis of M if and only if $\det A(X) \neq 0$.

Let us assume henceforth that $E = \{e_1, \dots, e_n\}$ and that $B = \{e_1, \dots, e_n\}$ is a basis of M .

(1.31) Proposition For a field F, M is F-representable if and only if there is an F-representation matrix of the form

$$A := \begin{array}{c} e_1 \\ \vdots \\ e_r \\ e_{r+1} \\ \vdots \\ e_n \end{array} \left[\begin{array}{c} I_r \\ \hline A_1 \end{array} \right] \qquad (1.31.1)$$

Proof Since the first r elements of E are independent, the first r rows of any F-representation matrix A' are linearly independent over F. But then the column echelon form of A' is a matrix of the form

(1.31.1) having the same corresponding linearly independent sets of rows as A', whence A is also an F-representation of M.

In [37]p.143 it is shown that if A is an F-representation of M of the form $A = \left[\frac{I_r}{A_1}\right]$ then the matrix $A' = \left[\frac{I_{n-r}}{A_1^T}\right]$ is an F-representation of M^* with respect to the ordering $e_{r+1},\ldots,e_n,e_1,\ldots,e_r$. Since $M = (M^*)^*$, we can thus deduce from (1.30):-

(1.32) Proposition The matroid M is F-representable if and only if M^* is F-representable.

If M is F-representable by the matrix A and if $E' \subset E$ then clearly the matrix $A(E')$ is an F-representation of $M|_{E'}$. consequently by (1.26) and (1.32) we may deduce:-

(1.33) Proposition If M is F-representable then every minor of M is F-representable.

The next two results are proved in chapter 7 of [1]

(1.34) Proposition The matroid $M(E)$ is F-representable if and only if the underlying simple matroid $M_0(E_0)$ is F-representable.

(1.35) Proposition Suppose $M = M_1 \oplus \cdots \oplus M_t$ where M_i is defined on E_i, with $B_i = B \cap E_i$ (a basis for M_i) and $|B_i| = r_i$ for $i=1,\ldots,t$. Then if $A_i = \begin{array}{c} B_i \{ \\ E \backslash B_i \{ \end{array} \left[\frac{I_{r_i}}{A_i'}\right]$ is an F-representation of M_i for $i=1,\ldots,t$, the matrix

$$A = \left[\begin{array}{ccc} & I_r & \\ \hline A'_1 & & 0 \\ & \ddots & \\ 0 & & A'_t \end{array}\right]$$

is an F-representation of M (with respect to the obvious ordering of E).

(1.36) Corollary The matroid M is F-representable if and only if each of its connected components is F-representable.

Proof Sufficiency follows from (1.28) and (1.35) whereas necessity follows from (1.33)

A matroid is said to be binary if it is representable over GF(2), ternary if it is representable over GF(3) and regular if it is representable over every field. The next two results show that binary and ternary matroids may be characterized by 'exclusion of certain minors.' The first result is due to Tutte, and is proved in [37] pp. 167-169, while the second is credited to Reid with proofs in [4], [30].

(1.37) Theorem A matroid is binary if and only if it does not contain $U_{2,4}$ as a minor.

(1.38) Theorem A matroid is ternary if and only if it does not contain any of the matroids $U_{2,5}$, F_7 or their duals.

A matrix N over $\mathbb{Z}$ is called unimodular if every square submatrix has determinant (over $\mathbb{Q}$) equal to 0,1 or -1. A matroid is called unimodular if it possesses a unimodular representation matrix (over $\mathbb{Q}$). The following theorem summarises the various characterizations of regular matroids and can be deduced from results of Tutte, [34], and Aigner, [1] pp. 344-346, and (1.37), (1.38).

(1.39) Theorem For a matroid M, T.F.A.E

1) M is regular

2) M is unimodular

3) M is binary and does not contain as a minor either F_7 or F_7^*.

4) M is binary and ternary

5) M is binary and F-representable for a field F with char $F \neq 2$

The characteristic set $c(M)$ of a matroid M consist of those integers n for which M is representable over a field of characteristic n. Thus $c(M) \subset P \cup \{0\}$ where P denotes the set of positive primes, and M is representable if and only if $C(M) \neq \phi$.

Suppose now that B is a basis of M. It follows easily from (1.23) that for each $e \in E \backslash B$ there is a unique circuit contained in $B \cup \{e\}$. This circuit is called the fundamental circuit of $B \cup \{e\}$ in M, and is denoted by $C_M(B,e)$ or more simply $C(B,e)$ if there is no ambiguity. For the following important definition we shall assume that $E = \{e_1,\ldots,e_n\}$ and that $B = \{e_1,\ldots,e_r\}$.

(1.40) Definition The B-basic circuit incidence matrix (B-basic c.i. matrix) $A_B=[a_{ij}]$ is the $((n-r)\times r)$ zero-one matrix with columns indexed by B and rows indexed by $E\backslash B$ where $a_{ij}=1$ if $e_j \in C(B,e_i)$.

The matrix A_B is obviously dependent on the ordering of E; a permutation of B corresponds to a permutation of the columns of A_B and a permutation of $E\backslash B$ corresponds to a permutation of the rows.

(1.41) Proposition Suppose A_B is given as above, and $B^* = E\backslash B$. Then A_B^T is the B^*-basic c.i.matrix of M^* with respect to the ordering $e_{r+1},\ldots,e_n,e_1,\ldots,e_r$.

Proof If $e_j \in C_M(B,e_i)$ $(1 \leq j \leq r,\ r+1 \leq i \leq n)$ then $(B\backslash\{e_j\}) \cup \{e_i\}$ must be a basis of M. Write $B' = (B\backslash\{e_j\}) \cup \{e_i\}$, then $E\backslash B'$ is a basis of M^* . But $E\backslash B' = B^*\backslash\{e_i\}) \cup \{e_j\}$ and since this set is independent in M^*, we must have $e_i \in C_{M^*}(B^*,e_j)$. The converse follows by duality.

(1.42) Suppose $A = [I_r \mid A']^T$ is a (column echelon) F-representation of M. Then the matrices A' and A_B have their non-zero entries in the same corresponding positions.

Proof Write $A_B=[a_{ij}]$, $A'=[b_{ij}]$ with the same indexing as above. For each i, j write $X_{ij} = (B\backslash\{e_j\}) \cup \{e_i\}$. Then

$$\det N(X_{ij}) = \pm b_{ij} \qquad (1.42.1)$$

If $a_{ij}=0$ then $e_j \notin C(B,e_i)$, whence $C(B,e_i) \subset (B\backslash\{e_j\}) \cup \{e_i\} = X_{ij}$. But then X_{ij} is a dependent set in M, so by (1.42.1) $b_{ij}=0$. If conversely $b_{ij}= 0$ then by (1.42.1), X_{ij} contains a circuit of M. Since $C \subset B \cup \{e_i\}$, we must have $C = C(B,e_i)$ by uniqueness of the latter. Thus $C(B,e_i) \subset X_{ij}$ so that $e_j \in C(B,e_i)$ whence $a_{ij}= 0$.

(1.43) Corollary If M is binary, the matrix $[I_r \mid A_B]^T$ is a representation of M over GF(2).

(1.44) Definition Let A be a matrix with rows R and columns C. Then A is block reducible if there exist proper subsets $R' \subset R$ and $C' \subset C$ such that all non-zero entries of A are contained in either the submatrices $R' \times C'$ or $(R\backslash R') \times (C\backslash C')$. Similarly the matrix A has k blocks if the rows and columns can be partitioned into k blocks $R_1,\ldots,R_k$ and $C_1,\ldots,C_k$ respectively such that all non-zero entries of A are contained in the submatrices $R_i \times C_i$ for $i=1,\ldots,k$ and each submatrix is block irreducible. Also by convention we shall always assume a block irreducible matrix has no zero row or column.

(1.45) Proposition If M has B-basic c.i.matrix $A_B=[a_{ij}]$. Then

1) r_i is a zero row of A_B if and only if e_i is a loop.

2) c_j is a zero column of A_B if and only if e_j is a coloop.

3) $\{r_{i_1},\ldots,r_{i_s}\} \times \{c_{j_1},\ldots,c_{j_t}\}$ forms a block of A_B if and only if $\{e_{j_1},\ldots,e_{j_t},e_{i_1},\ldots,e_{i_s}\}$ is a connected component of M.

4) For $r+1\leq i\leq n$ and $1\leq j\leq r$, e_i,e_j are parallel if and only if $a_{ij}=1$.

Proof For 1),2),3), see [12].

4) The elements e_i,e_j are parallel if and only if $\{e_i,e_j\}$ is a circuit. But then $C(B,e_i) = \{e_i,e_j\}$,so the result follows.

(1.46) Corollary Suppose A_B has r' zero rows, c' zero columns and k blocks. Then M has $r'+c'+k$ connected components, and for some suitable ordering of B, $E\backslash B$,

$$A_B = \begin{array}{c} \\ \\ r' \end{array}\!\!\left[\begin{array}{ccc|c} A_1 & & 0 & 0 \\ & \ddots & & \\ 0 & & A_k & 0 \\ \hline & 0 & & 0 \end{array}\right]^{\;c'}$$

where the A_i's are the blocks corresponding (as in (1.45.3)) to the k (non-trivial) components of M. Moreover if these k connected components are $E_1,\ldots,E_k$ respectively and if $B_i = B\cap E_i$ $(i=1,\ldots,k)$, then A_i is the B_i-basic c.i.matrix for $M|_{E_i}$.

§2 PROJECTIVE EQUIVALENCE OF MATRICES

Unless otherwise stated all matrices considered will be over a fixed field F, although the next definition is also valid for matrices over a division ring.

(2.1)Definition Let M, N be $(n\times m)$ matrices. Then M is projectively equivalent to N if there exists an $(m\times m)$ non-singular matrix C and an $(n\times n)$ non-singular diagonal matrix D such that $DMC = N$. In the case where C is also diagonal we shall say that M is strongly projectively equivalent to N (s-projectively equivalent).

It is clear that projective equivalence is an equivalence relation on the class of $(n\times m)$ matrices (over F). It is also easily seen that if M,N are projectively equivalent then any set of rows of M is linearly dependent over F if and only if the same corresponding set of rows of N is linearly dependent over F. It now follows by definition (1.29) that projectively equivalent matrices represent the same isomorphism class of matroids, and herein lies its importance to this work.

As its name suggests, another (more classical) motivation for the study of projective equivalence is in projective geometry:-

(2.2)Proposition Let M,N be $(n\times m)$ matrices without zero rows, so that the n rows of M,N respectively are the coordinate vectors of n points, say $P_1,\dots,P_n$ and $Q_1,\dots,Q_n$ in PG(m,F). Then M,N are projectively equivalent if and only if there is a collineation of PG(m,F) in which P_i is mapped to Q_i for $i=1,\dots,n$.

Proof If M,N are projectively equivalent then $DMC = N$ for some non-singular diagonal matrix D and non-singular matrix C. Since $\lambda P = P$ for each point P in PG(m,F) and $0 \neq \lambda \in F$ the rows of DM also are the coordinate vectors of $P_1,\dots,P_n$. Being non-singular, C represents a linear transformation of F^m whose induced auto-projectivity of $PG(m,F)$ is thus (by (1.12)) the required collineation. Conversely suppose that there is a linear transformation of F^m, represented by an $(m\times m)$ non-singular matrix C say, inducing the specified collineation. Then for for each $i=1,\dots,n$ if $\underline{v}_i$ is any coordinate vector of P_i and $\underline{w}_i$ any coordinte vector of Q_i it follows from the definition in §1 that $F(\underline{v}_iC) = F\underline{w}_i$. In particular this is true when $\underline{v}_i,\underline{w}_i$ are the i^{th} rows of M,N respectively. But then for $i=1,\dots,n$ there exist $0 \neq \lambda_i \in F$ for which $\lambda_i(\underline{v}_iC) = \underline{w}_i$. Writing $D = \mathrm{Diag}(\lambda_1,\dots,\lambda_n)$ it follows that D is non-singular and $DMC = N$.

Let us consider some other familiar equivalence relations defined on matrices :-

i) If M,N $(n\times m)$ matrices, write $M \overset{1}{\sim} N$ if and only if there exists an $(n\times n)$ non-singular matrix B and an $(m\times m)$ non-singular matrix C for which $BMC = N$.

ii) If M,N $(n\times n)$ matrices, write $M \overset{2}{\sim} N$ if and only if there exists an $(n\times n)$ non-singular matrix C for which $C^{-1}MC = N$ (<u>similarity</u>)

iii) If M,N $(n\times m)$ matrices, write $M \overset{3}{\sim} N$ if and only if there exists an $(m\times m)$ non-singular matrix C for which $MC = N$ (<u>column equivalence</u>)

In each of these cases we ask the question: ' is there a canonical form of matrix with respect to the given equivalence relation, i.e. is there some special simple type of matrix for which we can say that every matrix within the given class is equivalent to a unique matrix of this type ?' The answer in each of the above cases is affirmative and well known. The canonical form of i) for a matrix of rank r is precisely

$$\left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right]$$

The canonical form of ii) is the <u>rational canonical form</u>, which in the case when F is algebraically closed becomes the simpler <u>Jordan Canonical</u>

form. The canonical form of iii) is none other than the column echelon form. We shall show by construction that a canonical form exists for projective equivalence (we shall henceforth call this the 'projective canonical form').

First we observe that projective equivalence, like the equivalences above, is rank preserving. Accordingly we may restrict our attention to matrices having the same rank r, and so we define $\mathcal{C}$ to be the class of all $(n\times m)$ matrices of rank r (over F). It should be noted that equivalence iii) above is closely related to projective equivalence; clearly column equivalence implies projective equivalence, hence every matrix is projectively equivalent to a matrix in column echelon form. Consequently we begin in earnest by taking a closer look at the column echelon form.

Let $A \in \mathcal{C}$ and suppose the rows of A are indexed by $\{1,\ldots,n\}$. Since A has rank r there is at least one r-subset $J \subset \{1,\ldots,n\}$ for which $A(J)$ (defined in §1) has rank r. Let J_1 be the first such subset in the natural lexicographic order. Then it is easily seen that A is in column echelon form (which in this case we shall call J_1-column echelon form) if and only if $A(J_1) = [I_r | 0]$, and in this case we must have $A = [A' | 0]$ for some $(n\times r)$ matrix A'. Suppose now that $J_2 = \{1,\ldots,n\}\backslash J_1$ and that A is in J_1-column echelon form, then the only 'part' of A not already determined by J_1 is the $(n-r)\times r$ submatrix $A'(J_2)$. We shall call $A'(J_2)$ the non-identity submatrix of A.

With this notation we have:-

(2.3) Proposition Suppose $A,B \in \mathcal{C}$ are in J_1-column echelon form, with respective non-identity submatrices $A' = [a_{ts}]$ and $B' = [b_{ts}]$ $(1 \leq t \leq n-r,\ 1 \leq s \leq r)$. T.F.A.E.

i) A,B are projectively equivalent.

ii) A',B' are s-projectively equivalent

iii) There are non-zero elements $\mu_1,\ldots,\mu_r$, $\delta_1,\ldots,\delta_{n-r}$ of F for which $\delta_t a_{ts}\mu_s = b_{ts}$ for each t,s.

<u>Proof</u> (ii)$\Leftrightarrow$(iii) is clear so it suffices to prove (i)$\Leftrightarrow$(iii).

<u>(i)$\Rightarrow$(iii)</u> Let $D = \mathrm{Diag}(\lambda_1,\ldots,\lambda_n)$, $C = [c_{ij}]$ be non-singular matrices for which $DAC = B$. Then in particular we have

$$DAC(J_1) = B(J_1) = [I_r | 0] \qquad (2.3.1)$$

Suppose that $J_1 = \{i_1,\ldots,i_r\}$ and $J_2 = \{j_1,\ldots,j_{n-r}\}$. Then for each $t=1,\ldots,r$ the i_t^{th} row of DA is $(0,\ldots,0,\lambda_{i_t},0,\ldots,0)$. Hence the i_t^{th} row of DAC is $(\lambda_{i_1}c_{t1},\ldots,\lambda_{i_t}c_{tm})$, and so $DAC(J_1) = [\lambda_{i_t}c_{ts}]$ $(1\leq t\leq r,\ 1\leq s\leq m)$. By (2.3.1) this means that

$$C = \left[\begin{array}{c|c} \begin{matrix}\lambda_{i_1}^{-1} & & 0\\ & \ddots & \\ 0 & & \lambda_{i_r}^{-1}\end{matrix} & 0 \\ \hline \multicolumn{2}{c}{C'} \end{array}\right]$$

Now write $\mu_1=\lambda_{i_1}^{-1}$,..., $\mu_r=\lambda_{i_r}^{-1}$ $\delta_1=\lambda_{j_1}$,..., $\delta_{n-r}=\lambda_{j_{n-r}}$

Then $\mu_1,\ldots,\mu_r$, $\delta_1,\ldots,\delta_{n-r}$ are the required elements of F.

<u>(iii)$\Rightarrow$(i)</u> Suppose that $\mu_1,\ldots,\mu_r$, $\delta_1,\ldots,\delta_{n-r}$ satisfy the given relations and that J_1, J_2 are as above.

Write $\lambda_{i_1}=\mu_1^{-1}$,..., $\lambda_{i_r}=\mu_1^{-1}$ $\lambda_{j_1}=\delta_1$,..., $\lambda_{j_{n-r}} = \delta_{n-r}$

Then if $D = \mathrm{Diag}(\lambda_1,\ldots,\lambda_n)$ and $C = \mathrm{Diag}(\mu_1,\ldots,\mu_r,1,1,\ldots,1)$, we have $DAC = B$ (so in fact we have shown A,B are s-projectively equivalent in this case).

(2.4)<u>Remark</u> In our search for the projective canonical form it now suffices (by (2.3) and the comments prior to it) to find a canonical form with respect to s-projective equivalence; for suppose such a canonical form exists - call it the <u>strong canonical form</u> (s.c.f), so that every matrix B is s-projectively equivalent to a unique matrix in s.c.f (called the <u>associated s.c.f. of B</u>). Then every matrix is projectively equivalent to a unique matrix in column echelon form whose non-identity submatrix is in s.c.f. Thus for any matrix A the associated projective canonical form of A would be precisely the associated column echelon form of A in which the non-identity submatrix B say, is replaced by the s.c.f. of B.

Since by (2.3) s-projectively equivalent matrices have their non-zero entries in the same corresponding positions, our search for an s.c.f. will be restricted to finding certain privileged non-zero entries which would become equal to 1. What are these privileged entries ? They certainly cannot comprise all the non-zero entries, since for example

$$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \quad \text{is not s-projectively equivalent to} \quad \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} .$$

On the other hand it is easy to see that any matrix is s-projectively equivalent to a matrix in which every <u>leading entry</u> (first non-zero entry in a row or column) is equal to 1, so we would certainly expect our 'privileged' entries to include all leading entries. However these will not in general be sufficient to give a canonical form since, e.g.

$$\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix} \quad \text{is s-projectively equivalent to} \quad \begin{bmatrix} 0 & 1 \\ 1 & 3 \end{bmatrix} \qquad (2.4.1)$$

and these matrices are not equal even though their leading entries are all equal to 1. So in truth we will have to search somewhere between these two extremes to find the 'privileged' entries. In order to do so we introduce some new notions.

Suppose that $A = [a_{ij}]$ is an arbirary matrix. We shall be concerned with sequences of non-zero entries of A in which the position (i,j) of the non-zero entry a_{ij} concerns us rather than the specific value a_{ij}. Consequently we shall frequently use the notation (i,j) to replace the cumbersome a_{ij} and also describe a_{ij}, $a_{i'j'}$ as distinct if $(i,j) \neq (i',j')$.

(2.5) <u>Definition</u> A <u>chain</u> in A is a sequence of distinct non-zero entries of A such that consecutive terms are either in the same row or the same column, with a strict alternation between the two. Thus a chain from (i,j) to (i',j') can be any one of the following four types of sequences of non-zero entries of A :-

$$\left.\begin{array}{ll}
\text{(I)} & (i,j),\ (i_1,j),\ (i_1,j_1),\ldots,\ (i_{p+1},j_p),\ (i_{p+1},j'),\ (i',j') \\
\text{(II)} & (i,j),\ (i,j_1),\ (i_1,j_1),\ldots,\ (i_p,j_p),\ (i_p,j'),\ (i',j') \\
\text{(III)} & (i,j),\ (i_1,j),\ (i_1,j_1),\ldots,\ (i_p,j_p),\ (i',j_p),\ (i',j') \\
\text{(IV)} & (i,j),\ (i,j_1),\ (i_1,j_1),\ldots,\ (i_p,j_{p+1}),\ (i',j_{p+1}),(i',j')
\end{array}\right\}\ p\geq 1$$

(Also by convention, if $j=j'$ the trivial chain $(i,j),(i',j')$ will be considered to be a chain of type (II), and if $i=i'$ it will be considered to be a chain of type (IV)).

For any such chain we also say that a_{ij} is connected to $a_{i'j'}$ by the given chain C. The length of C is simply the number of terms in C and is denoted by $\ell(C)$. A chain of type (I) or (III) in which $i_1,\ldots,i_{p+1} < i$ will be called a u-chain. The key to finding our privileged entries for the canonical form is in the following:-

(2.6) Definition A non-zero entry a_{ij} of A is non-atomic if for some $1\leq j'<j$ there is a u-chain of type (I) connecting a_{ij} to, $a_{i,j'}$. Otherwise a_{ij} is atomic. An atomic chain in A is a chain in which each term is atomic.

(2.7) Example

1) Every leading entry of a matrix is atomic.

2) In the matrix

$$A = \begin{bmatrix} 0 & a_{12} & a_{13} & 0 \\ a_{21} & 0 & a_{23} & 0 \\ 0 & a_{32} & 0 & a_{34} \\ a_{41} & 0 & 0 & a_{44} \end{bmatrix}$$ (where all the marked a_{ij}'s are non-zero)

the entry a_{23} is atomic even though it is not a leading entry (the same is true of the (2,2) entry of the matrices in (2.4.1)). The entry a_{44} is non-atomic by virtue of the u-chain

$$(4,4),(3,4),(3,2),(1,2),(1,3),(2,3),(2,1),(4,1).$$

3) Suppose A' is the submatrix of A consisting of the first t rows of A

(where $1 \leqslant t \leqslant$ no. of rows of A). Then for each $a_{ij} \in A'$, a_{ij} is atomic in A' if and only if a_{ij} is atomic in A. The corresponding statement for columns is not true, since for example if

$$A = \begin{bmatrix} 0 & a_{12} & a_{13} \\ a_{21} & 0 & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \qquad \text{and} \qquad A' = \begin{bmatrix} 0 & a_{12} \\ a_{21} & 0 \\ a_{31} & a_{32} \end{bmatrix}$$

then a_{32} is atomic in A' but non-atomic in A because of the u-chain

$$(3,2),(1,2),(1,3),(2,3),(2,1),(3,1)$$

4) If $A = [a_{ij}]$, $B = [b_{ij}]$ are s-projectively equivalent matrices then a_{ij} is atomic if and only if b_{ij} is atomic, since by (2.3) both matrices have their non-zero entries in the same corresponding positions.

(2.8) Theorem <u>Every matrix is s-projectively equivalent to a unique matrix in which every atomic entry is equal to 1.</u>

Thus the privileged entries we were looking for in our search for the s.c.f. are precisely the atomic entries. Before proving (2.8) we shall need a lemma:-

(2.9) Lemma <u>Any two atomic entries of A are connected by at most one atomic chain.</u>

Proof Assume the contrary. Then we can consider all '4-tuples' $\Pi = (a, a', C, C')$ where a, a' are atomic entries of A connected by <u>distinct</u> atomic chains C, C'. Of all such 4-tuples choose one, say $\Pi_0 = ((i,j),(i',j'), C_1, C_2)$ for which $\ell(C_1) + \ell(C_2)$ is <u>minimal</u>. The chains C_1, C_2 may be any of the four different types. We will prove the lemma by showing that each possible permutation leads to a contradiction. First suppose that both chains begin by moving along column j (so that they are a permutation of types I and III), say

$$C_1 = (i,j),(i_1,j),\ldots,(i',j') \qquad \text{and} \qquad C_2 = (i,j),(i_1',j),\ldots,(i',j')$$

Then let C_1' be the chain formed from C_1 by deleting the first term (i,j) only. Let C_2' be the chain formed from C_2 by replacing the first term (i,j) by the term (i_1,j) or simply deleting (i,j) if $i_1' = i_1$. It is clear that the 4-tuple $((i_1,j),(i',j'), C_1', C_2')$ contradicts the choice of Π_0. We may arrive at similar contradictions when a) both chains begin by moving along row i (permutation of types II and IV), b) both chains end by moving along column j' (permutation of types I and II) or c) both chains end by moving along row i' (permutation of III and IV). This leaves us with only two possibilities:–

case d) one of C_1,C_2 is type I and the other is type IV, or

case e) one of C_1,C_2 is type II and the other is type III

We will show only that d) is impossible since the argument against e) is almost identical. Without loss of generality assume that

$$C_1 = (i,j),(i_1,j),(i_1,j_1),\ldots,(i_{p+1},j_p),(i_{p+1},j'),(i',j')$$
$$C_2 = (i,j),(i,j_1'),(i_1',j_1'),\ldots,(i_q',j_{q+1}'),(i',j_{q+1}'),(i',j')$$

First we will show that

$$i,i_1,\ldots,i_{p+1},\ i',\ i_1',\ldots,i_q' \quad \text{are all distinct} \qquad (2.9.1)$$

Certainly the row indeces $i,i_1,\ldots,i_{p+1},i'$ occuring in C_1 are all distinct, for otherwise we would have $i_s = i_t$ for some $0\leq s<t\leq p+2$ (taking $i_0=i$, $i_{p+2}=i'$) and then we could 'shorten' C_1 to the chain
$C_1' = (i,j),(i_1,j),\ldots,(i_s,j_{s-1}),(i_t,j_t),(i_{t+1},j_{t+1}),\ldots,(i',j')$
(where $j_0=j$, $j_{-1}=j'$) in which case $((i,j),(i',j'), C_1', C_2)$ contradicts the choice of Π_0. By a similar argument all the row indeces $i,i_1',\ldots,i_q',i'$ occuring in C_2 are distinct. So to establish (2.9.1) it suffices to show that $\{i_1,\ldots,i_{p+1}\} \cap \{i_1',\ldots,i_q'\} = \phi$. Suppose not. Then $i_s=i_t'$ for some $1\leq s\leq p+1$ and $1\leq t\leq q$ and so we have the chains

$$D_1 = (i_s,j_{s-1}),(i_s,j_s),\ldots,(i_{p+1},j'),(i',j')$$
$$D_2 = (i_s,j_{s-1}),(i_t',j_{t+1}'),\ldots,(i',j_{q+1}'),(i',j')$$

in which case $((i_s,j_{s-1}),(i',j'), D_1, D_2)$ contradicts the choice of Π_0, thus proving (2.9.1).

Thus the set $\mathcal{J}$ of row indeces (listed in (2.9.1)) has a unique maximal element which is either i_s for some $0\leq s\leq p+2$ or i'_t for some $1\leq t\leq q$. Assume first it is i_s. Then we may 'link' the chains C_1, C_2 to form

$$(i_s,j_s),(i_{s+1},j_s),\ldots,(i',j'),(i',j'_{q+1}),\ldots,$$

$$,\ldots,(i,j'_1),(i,j),(i_1,j),(i_1,j_1),\ldots,(i_{s-1},j_{s-1}),(i_s,j_{s-1}) .$$

By definition of i_s, the above chain is a u-chain from (i_s,j_s) to (i_s,j_{s-1}) which contradicts the fact that both these entries are atomic. A similar contradiction involving (i'_t,j'_{t+1}) and (i'_t,j'_t) is deduced if i'_t is the maximal element in $\mathcal{J}$.

<u>Proof of Theorem</u> (2.8)

Let $A = [a_{ij}]$ be an arbitrary $(n\times m)$ matrix. There are two things to prove:-

(2.8.1) that A is s-projectively equivalent to a matrix in which every atomic entry is equal to 1, and

(2.8.2) if A,B are $(n\times m)$ matrices in which each atomic entry is equal to 1, and which are s-projectively equivalent, then A=B.

By (2.3), to prove (2.8.1) we must find non-zero elements $\delta_1,\ldots,\delta_n$, $\mu_1,\ldots,\mu_m$ of F for which

$$\delta_i a_{ij}\mu_j = 1 \quad \text{whenever } a_{ij} \text{ is atomic} \qquad (2.8.3)$$

for then $[\delta_i a_{ij}\mu_j]$ is the required matrix. We prove (2.8.3) by induction on n . If n=1 then $A = [a_{11},\ldots,a_{1m}]$ and the atomic entries are precisely the non-zero entries. So take $\delta_1 = 1$ and

$$\mu_j = \begin{cases} 1 & \text{if } a_{1j} = 0 \\ a_{1j}^{-1} & \text{if } a_{1j} \neq 0 \end{cases} \qquad (j=1,\ldots,m)$$

Next assume that $n>1$ and that the result holds for matrices of less than n rows. In particular the result holds for the submatrix of A consisting of the first n-1 rows. Then (by (2.7.3)) there is at least one set of non-zero elements $\delta_1,\ldots,\delta_{n-1}$, $\mu_1,\ldots,\mu_m$ of F, satisfying

$$\delta_i a_{ij}\mu_j = 1 \quad \text{whenever } a_{ij} \text{ is atomic in A and } 1\leq i\leq n-1 \qquad (2.8.4)$$

Of all the sets of elements of F which satisfy (2.8.4) choose one, say $S = \{\delta_1,\ldots,\delta_{n-1},\mu_1,\ldots,\mu_m\}$ for which $X(S)$ is maximal where $X(S)$ is the set of atomic entries a_{nj} in the last row of A for which $a_{nj}\,\mu_j = 1$. If $X(S)$ contains every atomic entry in the last row of A then (2.8.3) is clearly satisfied by the elements $\delta_1,\ldots,\delta_{n-1}$, $\delta_n=1$, $\mu_1,\ldots,\mu_m$. So assume this is not the case and seek a contradiction. Let (n,j_0) be an atomic entry in the last row for which $(n,j_0) \notin X(S)$. We are going to construct a new set S' satisfying (2.8.4) for which $X(S')$ strictly contains $X(S)$. First define

$$\mu'_{j_0} = a^{-1}_{n,j_0} \tag{2.8.5}$$

Now replace μ_{j_0} in S by μ'_{j_0}. The resulting set S_0 clearly satisfies $X(S) \subset X(S_0)$, but if there is another atomic entry (i_1,j_0) in the j_0^{th} column then we do <u>not</u> necessarily have $\delta_{i_1} a_{i_1,j_0} \mu'_{j_0} = 1$. So what we must do is consider the set of all possible atomic u-chains from (n,j_0); for every row index i and every column index j appearing in such a chain we will define δ'_i, μ'_j respectively to replace δ_i, μ_j in S. Suppose then that

$$C = (n,j_0),(i_1,j_0),(i_1,j_1),\ldots,(i_{p+1},j_p),(i_{p+1},j_{p+1})$$

is such an atomic u-chain (where the appearance of the last term is dependent on whether C is type I or III). Each even-numbered term (i_s,j_{s-1}) (for $s=1,\ldots,p+1$) in C will determine δ'_{i_t} and each odd-numbered term (i_t,j_t) (for $t=0,\ldots,p+1$, with $i_0=n$) will determine μ'_{j_t} according to the following inductive procedure:-

By (2.8.5) the first term (n,j_0) determines $\mu'_{j_0} = a^{-1}_{n,j_0}$

If (i_s,j_{s-1}) is a subsequent even-numbered term, with $\mu'_{j_{s-1}}$ already determined, write

$$\delta'_{i_s} = (a_{i_s j_{s-1}}\,\mu'_{j_{s-1}})^{-1} \tag{2.8.6}$$

If (i_t,j_t) is a subsequent odd-numbered term, with δ'_{i_t} already determined, write

$$\mu'_{i_t} = (\delta'_{i_t} a_{i_t j_t})^{-1} \tag{2.8.7}$$

We have to check that there is no ambiguity about the choices of the δ''s and the μ''s ; suppose that row i appears as an index in two different atomic u-chains from (n,j_0). Then considering only the first part of these chains (up to the first occurence of i) we get two subchains C_1, C_2 say from (n,j_0) to (i,j') and (i,j'') respectively. If these chains are identical then of course the above procedure will lead to the same choice of δ'_i in each case. If they are distinct, then we can add the term (i,j') to C_2, obtaining two distinct atomic chains from (n,j_0) to (i,j') which contradicts (2.9).

Thus each row i can be 'reached' by an atomic u-chain from (n,j_0) in at most one way, and in the case when it can be reached μ'_i is uniquely determined according to (2.8.6). If row i cannot be reached in this way simply take $\delta'_i = \delta_i$. For similar reasons each column j can be reached in at most one way, in which case μ'_j is uniquely determined according to (2.8.7), and if column j cannot be reached we simply take $\mu'_j = \mu_j$.

The new set $S' = \{\delta'_1, \ldots, \delta'_{n-1}, \mu'_1, \ldots, \mu'_m\}$ now satisfies (2.8.2). Moreover if $a_{nj} \in X(S)$ then clearly column j cannot be reached by an atomic u-chain from (n,j_0) for otherwise we could construct an atomic u-chain from (n,j_0) to (n,j) which contradicts the fact that both these entries are atomic. Thus $\mu'_j = \mu_j$ and $a_{nj}\mu'_j = a_{nj}\mu_j = 1$. Thus $X(S) \subset X(S')$ and strict inequality now follows from the choice of a_{n,j_0} together with (2.8.5). This contradicts the choice of S.

To prove (2.8.2), suppose $A = [a_{ij}]$, $B = [b_{ij}]$ are s-projectively equivalent matrices in which each atomic entry is equal to 1. By (2.7.4) a_{ij} is atomic if and only if b_{ij} is atomic and in this case $a_{ij} = b_{ij} = 1$. Also there are non-zero elements $\delta_1, \ldots, \delta_n, \mu_1, \ldots, \mu_m$ of F for which

$$\delta_i a_{ij} \mu_j = b_{ij} \qquad (1 \leq i \leq n,\ 1 \leq j \leq m) \tag{2.8.8}$$

We have to show that $a_{ij} = b_{ij}$ for each i,j and we do this by induction on n. If n=1 then every non-zero entry of A,B is atomic, hence equal to 1. So assume n>1 and that the result holds for matrices of less than n rows. In particular, by (2.7.3) we may assume that $a_{ij} = b_{ij}$ whenever $1 \leq i \leq n-1$. By (2.8.8) we deduce that

$$\delta_i \mu_j = 1 \quad \text{whenever} \quad a_{ij} \neq 0 \quad \text{and } 1 \leq i \leq n-1 \qquad (2.8.9).$$

It now suffices to show that $\delta_n \mu_j = 1$ whenever $a_{nj} \neq 0$. Assume not; let (n,j_0) be the first non-zero entry in the last row for which $\delta_n \mu_{j_0} \neq 1$. Then certainly (n,j_0) is non-atomic (by(2.8.8)), hence there is a chain

$$(n,j_0),(i_1,j_0),(i_1,j_1),\ldots,(i_p,j),(n,j)$$
$$\text{where} \quad j < j_0 \quad \text{and} \quad i_1,\ldots,i_p < n$$

But then, by (2.8.9),

$$\delta_{i_1} \mu_{j_0} = \delta_{i_1} \mu_{j_1} = \delta_{i_2} \mu_{j_1} = \ldots = \delta_{i_p} \mu_j = 1$$

Thus $\mu_{j_0} = \mu_{j_1} = \ldots = \mu_j$, whence $\delta_n \mu_{j_0} = \delta_n \mu_j = 1$, by choice of (n,j_0). This contradiction completes the proof of the theorem.

(2.10) Definition An arbitrary matrix A is in projective canonical form (p.c.f.) if A is in column echelon form and every atomic entry of the non-identity submatrix of A is equal to 1.

(2.11) Corollary Every matrix A is projectively equivalent to a unique matrix in p.c.f. (called the associated p.c.f. of A)

Proof Follows immediately from remark (2.4) and theorem (2.8)

(2.12) Remark

1) The method described in the proof of (2.8) of considering all possible atomic u-chains from atomic entries in the last row of a matrix

A provides an algorithm for finding the associated s.c.f. of A (once the atomic entries of A are known). Consider, for example the matrix A of (2.7.2). The entry a_{41} is the only atomic entry in the last row, and the atomic u-chain (4,1),(2,1),(2,3),(1,3),(1,2),(3,2),(3,4) determines (according to the formulae (2.8.6),(2.8.7))

$$\mu_1 = a_{41}^{-1}, \quad \delta_2 = a_{21}^{-1}a_{41}, \quad \mu_3 = a_{23}^{-1}a_{21}\,a_{41}^{-1}, \quad \delta_1 = a_{13}^{-1}a_{41},$$
$$\mu_2 = a_{12}^{-1}a_{13}\,a_{41}^{-1}, \quad \delta_3 = a_{32}^{-1}a_{12}\,a_{13}^{-1}a_{41}, \quad \mu_4 = a_{34}^{-1}a_{32}a_{12}^{-1}a_{13}a_{41}^{-1}$$

Taking $\delta_4 = 1$ (as in the proof) the s.c.f. of A is thus the matrix $A' = \mathrm{Diag}(\delta_1,\delta_2,\delta_3,\delta_4)\ A\ \mathrm{Diag}(\mu_1,\mu_2,\mu_3,\mu_4)$, that is

$$A' = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & \lambda \end{bmatrix} \qquad (\text{where } \lambda = a_{44}a_{34}^{-1}\,a_{32}a_{12}^{-1}\,a_{13}a_{41}^{-1}).$$

Thus if, for example $B = \left[\frac{I_4}{A}\right]$ then the associated p.c.f. of B is the matrix $\left[\frac{I_4}{A'}\right]$.

2) Throughout the proof of (2.8) the only elements of the field F which are used are those in the subfield of F generated by the entries of the matrix A. Consequently the s.c.f is independent of F in the sense that F could be any field which contains all the entries of A. Thus if two matrices A,B (over F) are not (s-)projectively equivalent over F then they are not (s-)projectively equivalent over any field containing F.

3) As has already been observed, projective (and s-projective) equivalence are well defined for matrices over an arbitrary division ring. In fact the commutativity of F is not used in the proof of (2.8.1), so we may deduce that any matrix A over a division ring D is s-projectively equivalent to a matrix in which every atomic entry is equal to 1 (s.c.f). However in the proof of (2.8.2), the deduction of (2.8.9) from (2.8.8) is dependent on the commutativity of F, so in general we

cannot achieve uniqueness. Indeed if a,b are any two non-commuting elements of D (so that $bab^{-1} = a$) then

$$\begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & a \end{bmatrix} \begin{bmatrix} b^{-1} & 0 \\ 0 & b^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & bab^{-1} \end{bmatrix}$$

Consequently, the matrices $\begin{bmatrix} 1 & 1 \\ 1 & a \end{bmatrix}$, and $\begin{bmatrix} 1 & 1 \\ 1 & bab^{-1} \end{bmatrix}$ are <u>distinct</u>, s-projectively equivalent matrices (over D) which <u>are</u> both in s.c.f. For similar reasons (which we study in detail in §4) it is quite possible that two matrices over a field F may be non-projectively equivalent (over F) but projectively equivalent over some division ring containing F.

4) Suppose the matrix A has no zero entries in the first row. In this case the associated s.c.f. of A is particularly easily described; the only atomic entries are the leading entries, so the associated s.c.f. is a matrix of the form

$$B = \left[\begin{array}{c} 1 \quad 1 \ \dots \ 1 \\ \hline B' \end{array}\right]$$

where the leading entry of each row of B' is equal to 1.

<u>Applications of the projective canonical form</u>

First we present a new proof of (1.15), the 'second fundamental theorem of projective geometry' :-

<u>Proof of (1.15)</u> Suppose first that D is a field and $m \geq 2$. As in (2.2), any simplex in PG(m,D) is associated with an $(m+1)\times m$ matrix over D. By definitions (1.8) and (2.10) any such matrix has projective canonical form

$$\left[\begin{array}{c} I_m \\ \hline 1 \quad 1 \ \dots \ 1 \end{array}\right] \qquad (2.15.1)$$

and consequently, by (2.2) and (2.11) there is always at least one collineation mapping any given simplex onto another simplex. To show that there is only one such collineation it suffices to prove that the identity map is the only collineation which leaves invariant every point of the simplex given by (2.15.1). Let γ be such a collineation and $P \in PG(m,D)$. Suppose that the natural coordinate vectors of P, $\gamma(P)$ are respectively $(a_1,\dots,a_m)$ and $(b_1,\dots,b_m)$. By (2.2)

$$\left[\begin{array}{cccc} & I_m & & \\ \hline 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_m \end{array}\right] , \quad \left[\begin{array}{cccc} & I_m & & \\ \hline 1 & 1 & \dots & 1 \\ b_1 & b_2 & & b_m \end{array}\right]$$

are projectively equivalent matrices. Now since the first non-zero entry in each of $(a_1,\dots,a_m)$, $(b_1,\dots,b_m)$ is equal to 1, it follows from (2.12.4) that both these matrices are in p.c.f., hence by (2.11), $(a_1,\dots,a_m) = (b_1,\dots,b_m)$ so that $P = \gamma(P)$ and γ is the identity.

Conversely suppose that D is not a field, in which case there are two non-commuting elements $a,b \in D$. Then the (distinct) matrices

$$A = \left[\begin{array}{cccc} & I_m & & \\ \hline 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & a \end{array}\right] , \quad B = \left[\begin{array}{cccc} & I_m & & \\ \hline 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & bab^{-1} \end{array}\right]$$

are projectively equivalent over D since $(b\, I_{m+2})\, A\, (b^{-1}\, I_m) = B$. Since the first $m+1$ rows respectively of A,B represent the same simplex in $PG(m,D)$, it follows from (2.2) that there is a collineation other than the identity mapping one simplex onto itself.

The main application of the p.c.f. is in the study of matroid representations. Suppose that M is a matroid of rank r on the set $E = \{e_1,\dots,e_n\}$ where $B = \{e_1,\dots,e_r\}$ is a basis of M. Then if M is F-representable it follows from the above work that the associated p.c.f. for any representation has the form $\left[\frac{I_r}{A}\right]$ where every atomic entry of A is equal to 1. For example, we can immediately deduce from (1.43) and (2.11) that every representation of M over GF(2) is projectively equivalent to the matrix $[I_r \mid A_B]^T$ where A_B is the B-basic c.i.matrix of M. We next use the p.c.f. to present new proofs of results concerning certain uniqueness of representability of binary and ternary matroids. The first of these is

(2.13) Theorem Suppose M is binary. Then there is a matrix A in p.c.f. all of whose non-zero entries are equal to ± 1, such that any representation of M over any field F has A as its associated p.c.f.

Before proving this important theorem we shall need a definition and two lemmas:-

(2.14) Definition For any $m \geq 2$, an $(m \times m)$ block irreducible matrix A is a circuit matrix if every row and every column of A has exactly two non-zero entries.

(2.15) Lemma Let A be an $(m \times m)$ circuit matrix all of whose non-zero entries are equal to ± 1 except possibly one which is equal to a say. Then (up to sign), $\det A = 1 \pm a$

Proof Since A is block irreducible, it is easily seen that A has exactly two non-vanishing permutation products - one of which is equal to ± 1, the other of which is equal to $\pm a$.

(2.16) Lemma Suppose A is an $(m \times m)$ circuit matrix (over F) for which the matrix $A' = [I_m \mid A]^T$ is an F-representation for some binary matroid $M'(E')$ of $2m$ elements. Then the set of m elements of E' corresponding to the rows of A form a circuit in M', so $\det A = 0$.

Proof Let A_1 be the $(m \times m)$ matrix over GF(2) whose non-zero entries appear in the same positions as those of A. Then clearly by definition (2.17) the m rows of A_1 form a circuit in $(GF(2))^m$. But by (1.43) $[I_m|A_1]^T$ is a representation of M' over GF(2) so the result follows.

Proof of (2.13) Let $A=[a_{ij}]$ be an F-representation in p.c.f. We have to show that every entry of A is equal to ± 1, where the sign is uniquely determined by the matroid M (i.e. is not dependent on the particular representation). We proceed by induction on n. The cases n=1,2 (and n=r) are trivial so assume that $n>r>1$ and that the result holds for binary matroids of fewer than n elements. Now

$$A = \left[\frac{I_r}{A_1}\right] \qquad \text{where} \quad A_1 = \begin{array}{c} \\ e_n \end{array}\left[\frac{A_1'}{-\underline{v}-}\right], \text{say.}$$

and all atomic entries of A_1 are equal to 1. With respect to the obvious ordering, $\left[\frac{I_r}{A_1'}\right]$ is an F-representation of the matroid $M\backslash\{e_n\}$ which, by (2.7.3) is in p.c.f. By (1.33) $M\backslash\{e_n\}$ is binary so by the inductive hypothesis every non-zero entry of A_1' is equal to ± 1 with the sign uniquely determined by the matroid $M\backslash\{e_n\}$ (and a fortiori, by M). Thus we have to show that every non-zero entry of $\underline{v}$ (the last row of A) is equal to ± 1 where the sign is uniquely determined by the previous rows.

If every entry of $\underline{v}$ is atomic in A_1 we are done since then all the non-zero entries are equal to 1. If not we proceed to:-

stage I There is at least one u-chain from a non-atomic entry in the last row to an atomic entry in the last row. Choose one C say, of minimal length among all such chains. Then C has the form

$$C = (n,j),(i_1,j),(i_1,j_1),\ldots,(i_{m-1},j_{m-2}),(i_{m-1},j'),(n,j')$$

where $m\geq 2$, $i_1,\ldots,i_{m-1} < n$ and (n,j') is atomic.

Let $I = \{n,i_1,\ldots,i_{m-1}\}$, $J = \{j,j_1,\ldots,j_{m-1},j'\}$. The choice of C ensures that the elements of I, J respectively are all distinct.

Moreover if N is the $(m\times m)$ submatrix of A_1 whose rows are indexed by I and whose columns are indexed by J it is easily seen (by similar arguments to those used in (2.9)) then that the minimality of $\ell(C)$ implies that N is a circuit matrix. Now write

$$S = B \cup \{e_{i_{m-1}}, e_{i_{m-2}}, \dots, e_{i_1}, e_n\}$$

$$T = B \setminus \{e_{j'}, e_{j_{m-2}}, \dots, e_{j_1}, e_j\}$$

Then the minor $M' = (M|_S)/T$ of M is binary (by(1.33)) and by construction the matrix $\left[\frac{I_m}{N}\right]$ is an F-representation of M' with respect to the ordering $e_{j'}, e_{j_{m-2}}, \dots, e_j,\ e_{i_{m-1}}, \dots, e_{i_1}, e_n$. By (2.16), det N = 0. But N satisfies the hypothesis of (2.18) so (up to sign), det N $= 1 \pm a_{nj}$ and so $a_{nj} = \pm 1$.

If (n,j) is the only non-atomic entry in the last row we are done. If not then we proceed to:-

stage II there is at least one u-chain from a non-atomic entry $(\neq(n,j))$ in the last row to either an atomic entry or (n,j) in the last row. Choose one such chain of minimal length, and suppose it is from the atomic entry (n,j''). Proceeding exactly as in stage I, we again deduce that $a_{n,j''} = \pm 1$ since the only possible difference is that the (non-atomic) entry a_{nj} may be the other entry in the last row used in the proof and this has now been uniquely determined to be ± 1.

If $(n,j),(n,j'')$ are the only non-atomic entries in the last row we are done. If not we consider u-chains from other non-atomic entries in the last row to atomic entries or (n,j), (n,j'') in the last row, and proceed as before. It is clear that the result must follow after a finite number of these steps.

(2.17) Remark The method used in the above proof once again provides an algorithm for determining the matrix A. This theorem appears in a slightly different form in [12], and a weaker result is also proved in [39]. It is not difficult to deduce that the matrix A is always unimodular if M is also F-representable for some field F with char F $\neq 2$ (see, [11] for an elementary proof of this). Consequently, this provides an alternative and more direct proof of Tutte's famous Unimodular Theorem (which is essentially stated in (1.39)). Another immediate consequence is that a binary matroid is uniquely F-representable (that is, any two F-representations are projectively equivalent) for any field F over which M is representable.

The next result has also been proved in [12] and [30].

(2.18) Theorem Suppose M is ternary. Then any two representations of M over GF(3) are projectively equivalent.

Proof Let A_1, A_2 be two representations of M over GF(3) in p.c.f. Suppose $A_1 = [a_{ij}]$ $(= [I_r \mid A_1']^T)$ and $A_2 = [a_{ij}']$ $(= [I_r \mid A_2']^T)$. We have to show that $a_{ij} = a_{ij}'$ for each i, j. By a similar induction argument to that used in the proof of (2.13), we may assume that all the corresponding entries of A_1, A_2 are equal except possibly those in the last row. If all the corresponding entries in the last row are equal there is nothing to prove, so we may assume w.l.o.g. that for some (n, j), $a_{nj} = 1$ and $a_{nj}' = -1$ and seek a contradiction. Using exactly the same argument as in (2.13) we may assume there is an entry (n, j_0) in the last row with $a_{n,j_0} = a_{n,j_0}'$ and a u-chain from (n, j) to (n, j_0) such that if I is the set of row indeces and J the set of column indeces appearing in this chain then the submatrices N_1, N_2 of A_1', A_2' respectively, indexed by I, J, are circuit matrices. Now, $[I_m \mid N_1]^T$, $[I_m \mid N_2]^T$ are representations over GF(3) of the same minor of M. Consequently det $N_1 = 0$ if and only if det $N_2 = 0$. But, by (2.15),

$$\det N_1 = 1 \pm a_{nj} \quad \text{(up to sign)}$$

$$\text{and,} \quad \det N_2 = 1 \pm a_{nj}' \quad \text{(up to sign)}$$

Since $a_{nj} = 1$ and $a'_{nj} = -1$, it follows that one of $\det N_1$, $\det N_2$ is equal to zero and the other is equal to ± 2, which is a contradiction since $2 \neq 0$ in $GF(3)$.

We conclude this section by describing the connection between the projective canonical form and the work done by Brylawski and Lucas in [12]. For an arbitrary $(s \times t)$ matrix $A = [a_{ij}]$ with row set R and column set C we may associate a bipartite graph H_A whose vertices are partitioned into the two sets $R = \{r_1, \ldots, r_s\}$, $C = \{c_1, \ldots, c_t\}$ and for which there is an edge joining r_i to c_j if and only if $a_{ij} = 0$. Denote such an edge by $[i,j]$. Brylawski and Lucas now define a coordinatizing path P of A to be a spanning forest of the graph H_A, or equivalently a basis of the cycle matroid $M(H_A)$ defined in (1.20.3). In the case of a matroid M with basis B and P a coordinatizing path for A_B (the B-basic c.i.matrix) they also define a representation matrix N of M to be in (B,P)-basic form if $N(B) = I_r$ and the entries corresponding to P in the non-identity submatrix of N are all equal to 1. Obviously there may be many coordinatizing paths P; we now show that for a certain natural choice of P, the (B,P)-basic form corresponds precisely to our p.c.f,(allowing for the fact that the role of rows and columns are interchanged).

First we observe that the set of edges of H_A is totally ordered by the lexicographic order

$[i,j] < [i',j']$ if and only if either

(a) $i < i'$ or (b) $i = i'$ and $j < j'$

This order now induces a (total) lexicographic order on the set of all coordinatizing paths. Let P^* be the minimal path in this order. With this notation we have

(2.19) Theorem The edge $[i,j] \in P^*$ if and only if the entry (i,j) is atomic in A.

Proof Suppose first that $[i,j] \in P^*$ but that (i,j) is non-atomic. Then for some $j' < j$ there is a chain in A of the form

$$(i,j),(i_1,j),(i_1,j_1),\ldots,(i_k,j_{k-1}),(i_k,j'),(i,j') \quad \text{where } i_1,\ldots,i_k < i \qquad (2.19.1)$$

By 'shortening' this chain if necessary we may assume that $i,i_1,\ldots,i_k$ are all distinct and similarly $j,j_1,\ldots,j'$ are all distinct. Then the set $C = \{[i,j],[i_1,j],[i_1,j_1],\ldots,[i_k,j'],[i,j']\}$ is a circuit in $M(H_A)$. Thus the set $X = C\setminus\{[i,j]\}$ is independent in $M(H_A)$, and so by (1.17.2) there is an $e \in X$ for which the set

$$P = P^*\setminus\{[i,j]\} \cup \{e\}$$

is a basis of $M(H_A)$, that is, a coordinatizing path for A. By (2.19.1) $e < [i,j]$ so the choice of P^* is contradicted.

Conversely suppose that (i,j) is atomic in A but that $[i,j] \notin P^*$. Then $P^* \cup \{[i,j]\}$ contains a cycle C of H_A which we may write as

$$C = \{[i,j],[i_1,j],[i_1,j_1],\ldots,[i_k,j'],[i,j']\} \qquad (k \geq 1)$$

First we show that

$$i_1,\ldots,i_k < i \qquad (2.19.2)$$

For suppose not. Then we must have $i_q > i$ for some $1 \leq q \leq k$. Since C is the fundamental circuit of $[i,j]$ in $M(H_A)$, $P^*\setminus\{[i_q,j_{q-1}]\}\cup\{[i,j]\}$ is a basis (interpreting $j_0=j$). This contradicts the choice of P^* since $[i,j] < [i_q,j_{q-1}]$, and hence proves (2.19.2). But now

$$(i,j),(i_1,j),\ldots,(i_k,j'),(i,j')$$

is a u-chain in A. This is impossible if $j' < j$ since (i,j) is atomic. But if $j < j'$ then (by reversing the terms of this chain) we infer that (i,j') is non-atomic. But $[i,j'] \in P^*$, so by the 'if' part proved above, (i,j') is atomic - a contradiction.

(2.20) Corollary (with the same notation as above) A representation matrix for M over a field F is in (B,P)-basic form if and only if it is in projective canonical form.

(2.21) Corollary Suppose A is an $(s \times t)$ matrix with r' zero rows, c' zero columns and k blocks after zero rows and columns have been deleted. Then A has $(s+t) - (r' + c' + k)$ atomic entries. In particular if A is block irreducible then A has $s + t - 1$ atomic entries.

Proof The bipartite graph H_A has $s + t$ vertices and $k + r' + c'$ connected components. By (1.16) every spanning forest of H_A has $s + t - (k + r' + c')$ edges so the result follows from (2.19).

(2.22) Corollary Suppose the matroid M (of size n, rank r) has k connected components. Then for any basis B of M the matrix A_B has $n - k$ atomic entries.

Proof If M has r' loops, c' coloops and k' (non-trivial) connected components, then $k = k' + r' + c'$. The result follows from (1.45),(2.22).

(2.23) Corollary Suppose A is a block irreducible matrix. Then there is an atomic chain in A joining any two atomic entries.

Proof The graph H_A is connected. Any coordinatizing path of A , in particular P^* , is thus a spanning tree of H_A any two of whose edges must be connected by a path of this tree. The result now follows from (2.19).

It has already been noted that for a given matrix A there may be atomic entries in A which are not the leading entries in their respective row or column. With the help of the following definition (and the above results) we will show that we can always rearrange rows and columns of A so that the only atomic entries of the resulting matrix are the leading entries - a result of some significance in §5.

(2.24) Definition Let A be an $(s \times t)$ matrix. For $i=1,\dots,s$ suppose the leading entry in the i^{th} row of A appears in the α_i^{th} position, and for $j=1,\dots,t$ the leading entry in the j^{th} column appears in the β_j^{th} position. Then A is in step diagonal form (s.d.f) if both of the sequences $\alpha_1,\dots,\alpha_s$ and $\beta_1,\dots,\beta_t$ are non-decreasing.

(2.25) Proposition Every matrix can be brought into step diagonal form by rearranging rows and columns, that is, every matrix is permutation equivalent to a matrix in s.d.f.

Proof It suffices to prove the result for block irreducible matrices, since by rearranging rows and columns, an arbitrary matrix A can always be brought into the form

$$\left[\begin{array}{ccc|c} B_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & B_k & \\ \hline & 0 & & 0 \end{array}\right]$$

where the B_i's are the blocks of A. By definition (2.24) A is in s.d.f. if each B_i is in s.d.f. So assume A is block irreducible. Then the graph H_A is connected. We now relabel the vertices as follows:-

Choose an arbitrary r_1, then label the adjacent vertices as $c_1, c_2, \dots$ then the remaining vertices adjacent to c_1 (if any) as $r_2, r_3, \dots$ and so on. Since H_A is connected this procedure will relabel each vertex, and the induced rearrangement of rows and columns of A yields a matrix which is in s.d.f.

(2.26) Proposition Suppose the matrix A is in s.d.f. Then the only atomic entries of A are the leading entries.

Proof Again it suffices to assume that A is an $(s\times t)$ block irreducible matrix. By (2.21), A has $(s+t-1)$ atomic entries. But since A is in s.d.f it now follows that A has exactly $(s+t-1)$ leading entries since no (i,j) except $(1,1)$ can be the leading entry in both row and column. The result now follows by (2.7.1).

§3 CHARACTERIZATION OF ATOMIC MATROIDS

The work of the previous chapter leads us naturally to the following definition :-

(3.1) Definition A matrix A is atomic if every non-zero entry of A is atomic, or equivalently (by(2.19)) if the bipartite graph H_A is a forest. A matroid is atomic if for some basis B of M the matrix A_B is atomic.

(3.2) Proposition The expansion of any subdeterminant of an atomic matrix A has at most one non-vanishing term. In particular every zero-one atomic matrix is unimodular.

Proof Since H_A contains no cycle there can be at most one matching between any set of t rows and t columns. Thus any $(t\times t)$ subdeterminant of A has at most one non-zero permutation product.

(3.3) Remark

1) The representation problem for atomic matroids is immediately classified; for suppose M is atomic with (atomic) B-basic c.i. matrix A_B. Then by (2.11) and (1.42) every representation matrix of M is projectively equivalent to $[I_r \mid A_B]^T$,a unimodular matrix. Thus by (1.39) if M is representable it must be regular.

2) Rearranging rows or columns of a matrix does not affect its 'atomicity'. In particular, although for a matroid M(E) the matrix A_B is dependent on the ordering of E, its atomicity is independent of this ordering.

By a consideration of the bipartite graph H_A the following statements are obvious:-

3) A matrix is atomic if and only if each of its blocks is atomic.

4) A matrix A is atomic if and only if A^T is atomic.

5) Any submatrix of an atomic matrix is atomic.

(3.4) Corollary

1) A matroid is atomic if and only if each of its connected components is atomic.

2) A matroid M is atomic if and only if M^* is atomic.

3) If a matroid is atomic then so too is its underlying simple matroid.

Proof

1) Follows from (3.2.3) and (1.46).

2) Follows from (3.2.4) and (1.41).

3) Follows from (3.2.5) and (1.24).

(3.5) Definition (using the notation of (1.20.6)) A matroid M is a fundamental transversal matroid (FT matroid) if for some cobasis B^*, $M = M[C_1^*,\dots,C_r^*]$ where $C_1^*,\dots,C_r^*$ are the fundamental circuits of B^* in M^*.

Because of the following result, the main theorem of this chapter (3.12) is also a characterization of binary FT matroids.

(3.6) Theorem A matroid is atomic if and only if it is a binary FT matroid.

Proof First suppose that M is an atomic matroid with atomic B-basic c.i.matrix A_B. Write $B = \{e_1,\dots,e_r\}$. If $B^* = E\backslash B$ and for $j=1,\dots,r$ C_j^* is the fundamental circuit of $B^* \cup \{e_j\}$ in M^*, then the matrix induced by the transversal matroid

$M' = M[C_1,\dots,C_r]$ is precisely $A = \left[\dfrac{I_r}{A_B}\right]$.

By (3.2) the matrix A represents the transversal matroid M' over any field. If we can show that M is representable it follows from (3.3.1) that A is also a representation of M (over any field) and hence that $M = M'$ as required.

We shall prove that M is representable by induction on the size n of M. If $n=1$ the result is trivial so assume $n>1$ and that the result holds for atomic matroids on less than n elements. We may assume M is simple, for otherwise we could apply (3.4.3) to the underlying simple matroid and deduce the result from (1.34). Now, since A_B is atomic, its associated bipartite graph is a forest which thus has a terminal vertex. Consequently A_B has either a column or a row with only one non-zero entry; since M is simple it follows from (1.45.4) that the latter is impossible, so we may assume that the j^{th} column say, of A_B has only one non-zero entry. Let A' be the matrix formed from A_B by deleting the j^{th} column and let $B' = B\backslash\{e_j\}$. Then B' is a basis for the matroid $M/\{e_j\}$ and with respect to the ordering

$$e_1,\ldots,e_{j-1},e_{j+1},\ldots e_r, \quad e_{r+1},\ldots,e_n$$

the matrix A' is the B'-basic c.i.matrix for $M/\{e_j\}$. By (3.3.5) A' is atomic, and thus by the inductive hypothesis $M/\{e_j\}$ is representable, hence by (1.32) so is its dual. But by (1.26) $(M/\{e_j\})^* = M^*\backslash\{e_j\}$ so the latter is representable. By choice of the j^{th} column it follows from (1.41) and (1.45.4) that e_j is a parallel in M^*, and so by (1.34) M^* is representable. The result now follows from another application of (1.32).

For sufficiency, suppose that M is binary and $M = M[C_1^*,\ldots,C_r^*]$ where the C_j^*'s are defined as above with respect to some basis B of M. If the bipartite graph associated with A_B contained a cycle, then there would be a transversal of M for which the corresponding subdeterminant of $[I_r|A_B]^T$ is equal to zero over GF(2), which contradicts the fact that this matrix is a representation of M over GF(2). Thus A_B is an atomic matrix and the theorem follows.

The above result is closely connected to a theorem attributed to Edmunds (see[37],Ex.(14.4.1)) which states that

> A transversal matroid is binary if and only if it can be presented by a bipartite forest.

<u>Corollary</u> <u>A matroid is a binary transversal matroid if and only if it can be represented (over every field) by a zero-one atomic matrix.</u>

<u>A-GRAPHS</u>

Our next (and most important) aim is to show that atomic matroids are precisely the cycle matroids of a special class of graphs. A graph will be denoted by G(V,E) (or simply G) and any subgraph of G will be simultaneously identified with its edge set as a subset of E in the matroid M(G) (defined in (1.20.3)). In particular, if C is a cycle of G then it is also a circuit in M(G).

(3.7) <u>Definition</u> An <u>A-graph</u> G(V,E) consists of a pair $((C_1,\dots,C_m),\ \dot{P})$ where $(C_1,\dots,C_m)$ is an ordered m-tuple of cycles of G (called the <u>fundamental cycles</u>) none of which are loops, for which $E = \cup\, C_i$ and for which P (the '<u>pivot</u>'set) is defined by

$$P = \{ e \in E;\ e \in C_i \cap C_j \text{ for some } 1 \leq i \neq j \leq m \}$$

In addition we must have:-

1) P contains no cycle of G, and

2) For each k=1,...,m-1 the cycle C_{k+1} has exactly one edge x_k say, (called the k^{th} <u>pivot</u>) in common with $\bigcup_{i=1}^{k} C_i$ and exactly 2 vertices (namely the endpoints of x_k) in common.

It is clear that $P = \{x_1,\ldots,x_{m-1}\}$, but these pivots may not all be distinct (see later example). It is also not difficult to see that A-graphs are precisely those graphs which can be constructed inductively on the number of fundamental cycles in the following manner:-

(3.8) (recursive construction for A-graphs)

1) A single cycle C (not a loop) is an A-graph with $P = \phi$.

2) Suppose $G(V,E) = ((C_1,\ldots,C_m), P)$ is an A-graph. Let $x_m \in E$ for which $P \cup \{x_m\}$ does not contain a cycle. Let G' be a new graph in which a cycle C_{m+1} (not a loop) is added to G, having only the edge x_m and its endpoints in common with G. Then G' is an A-graph with defining pair $((C_1,\ldots,C_{m+1}), P \cup \{x_m\})$.

(3.9) Examples

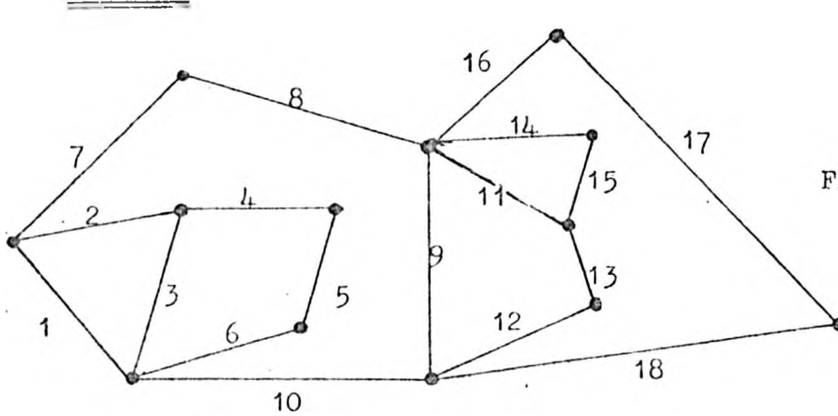


FIGURE 1

1) The graph of figure 1 is an A-graph. There are several ways we can define the fundamental cycles recursively as in (3.8), one such way is $C_1 = \{1,2,3\}$, $C_2 = \{3,4,5,6\}$, $C_3 = \{1,7,8,9,10\}$, $C_4 = \{9,11,12,13\}$, $C_5 = \{9,16,17,18\}$, $C_6 = \{11,14,15\}$. In this case $x_1 = 3$, $x_2 = 1$, $x_3 = 9$, $x_4 = 9$, $x_5 = 11$,

and hence $P = \{3,1,9,11\}$

2) A-graphs are series parallel networks.

3) A-graphs are planar, 2-connected graphs.

4) The complete bipartite graph $K_{2,3}$ is <u>not</u> an A-graph since it consists of just three cycles, any two of which intersect in two edges (so that (3.7.2) can never be satisfied). Moreover no graph which contains a subgraph homeomorphic to $K_{2,3}$ is an A-graph.

5) For similar reasons no graph which contains a subgraph homeomorphic to K_4 or C_k^2 $(k>2)$ can be an A-graph.

(3.10) <u>Definition</u> A <u>generalised A-graph</u> is a graph whose (graphically connected) components are A-graphs, loops or trees.

(3.11) <u>Remark</u> As for graphs in general it is quite possible that for two non-isomorphic (generalised) A-graphs G_1, G_2, the matroids $M(G_1)$, $M(G_2)$ are isomorphic. Since we are primarily interested in the cycle matroid structures we shall not distinguish between G_1, G_2 in this case. With this convention, it follows from (1.27) that graphs whose 2-connected components are A-graphs and coloops are also to be considered generalised A-graphs, and loops can be added anywhere with the graph remaining a generalised A-graph.

(3.12) <u>Theorem</u> <u>A matroid is atomic if and only if it is the cycle matroid of a generalised A-graph.</u>

<u>Proof</u> Since loops and coloops are trivially atomic matroids (and of course generalised A-graphs) it suffices by (3.4.1) to prove that

a connected matroid M is atomic if and only if $M=M(G)$ for some A-graph G.

First suppose $G(V,E)$ is an A-graph on the pair $((C_1,\ldots,C_m), P)$. By (3.9.3) and (1.27), $M(G)$ is certainly connected. We have to find a basis B of $M(G)$ for which A_B is an atomic matrix. Now since P contains no cycle of G we may choose a $y_i \in C_i \setminus P$

(for each $i=1,\ldots,m$). Write $B = E\backslash\{y_1,\ldots,y_m\}$. Using (3.8) it follows easily by induction on m that

$$|V| = \sum_{i=1}^{m} t_i - 2m + 2 \qquad \text{where } t_i = |C_i| \quad (i=1,\ldots,m)$$

and similarly that

$$|B| = \sum_{i=1}^{m} t_i - 2m + 1$$

Thus, since B is clearly a spanning subgraph for the connected graph G and $|B| = |V| - 1$, it follows from (1.16) that B is a spanning tree, that is, a basis for $M(G)$. We now show that A_B is an atomic matrix.

By construction $C_i = C(B,y_i)$ $(i=1,\ldots,m)$. Write $D_i = C_i \cap P$ and $B_i = C_i\backslash(P \cup \{y_i\})$ (which may be empty). Then if $p_1,\ldots,p_k$ are the distinct elements of P there is a suitable ordering of B for which A_B has the form

$$\begin{array}{c}
\\
y_1 \\ y_2 \\ \vdots \\ y_m
\end{array}
\begin{array}{c}
\overbrace{\qquad\qquad}^{B_1} \quad \overbrace{\qquad\qquad}^{B_2} \quad \cdots \quad \overbrace{\qquad\qquad}^{B_m} \quad \begin{array}{cccc} p_1 & p_2 & \cdots & p_k \\ \downarrow & \downarrow & & \downarrow \end{array} \\
\left[\begin{array}{cccc|c}
1\ 1\ \ldots\ 1 & & & & \\
 & 1\ 1\ \ldots\ 1 & & & A' \\
 & & \ddots & & \\
 & & & 1\ 1\ \ldots\ 1 &
\end{array}\right]
\end{array}$$

Clearly the atomicity of A_B will follow if we can show A' is atomic. Certainly A' is block irreducible (since by (1.45.3) A_B is block irreducible), thus by (2.21) it suffices to show that A' has exactly $(m + k - 1)$ non-zero entries. For $i=1,\ldots,m$ the i^{th} row of A' has $|D_i|$ non-zero entries, so it suffices to prove that

$$\sum_{i=1}^{m} |D_i| = m + P - 1 \qquad (3.12.1)$$

We use induction on m. If $m=1$, $P = \phi$ and both sides of (3.12.1) are zero. So assume $m > 1$. Consider the A-graph $G' = C_1 \cup \ldots \cup C_{m-1}$. This graph has pivot set

$$P' = \{e \,;\, e \in C_i \cap C_j \text{ for some } 1 \leq i \neq j \leq m-1\}$$

Writing $D'_i = C_i \cap P'$, it follows by the inductive hypothesis that

$$\sum_{i=1}^{m-1} |D'_i| = m + |P'| - 2 \qquad (3.12.2)$$

Without loss of generality assume that p_k is the $(m-1)^{th}$ pivot of G. We distinguish two cases:-

case (a) $p_k \in P'$. In this case $P' = P$, and so $D'_i = D_i$ for $i=1,\ldots,m-1$ and $D_m = \{p_k\}$. Thus

$$\sum_{i=1}^{m} |D_i| = \sum_{i=1}^{m-1} |D'_i| + 1 = m + |P'| - 1 = m + |P| - 1$$

case (b) $p_k \notin P'$. By construction $p_k \; (= x_{m-1}) \in C_m$ and $D_m = \{p_k\}$, so in this case there is exactly one C_i $(1 \leq i \leq m-1)$ for which $p_k \in C_i$. Then $p_k \in D_i$, and since $P' = P \backslash \{p_k\}$ we must have $D'_i = D_i \backslash \{p_k\}$ and $D'_j = D_j$ for each $j=1,\ldots,i-1,i+1,\ldots,m-1$. Thus (3.12.1) follows from (3.12.2).

This proves sufficiency.

Conversely, suppose that M is a connected atomic matroid on the set E. Assume that $B = \{e_1,\ldots,e_r\}$ is a basis of M for which A_B is atomic. Write $E \backslash B = \{f_1,\ldots,f_m\}$ (so the rows of A_B are indexed by $f_1,\ldots,f_m$) and let $C_i = C(B,f_i)$ for $i=1,\ldots,m$. Since H_A (the bipartite graph associated with A_B) is a tree, we can certainly reorder the C_i's so that

$$C_{t+1} \cap \bigcup_{i=1}^{t} C_i \neq \phi \qquad \text{for } t=1,\ldots,m-1$$

Moreover, since H_A contains no cycle it follows that

$$|C_{t+1} \cap \bigcup_{i=1}^{t} C_i| = 1 \qquad (3.12.3)$$

(for $t=1,\ldots,m-1$)

Let $\{x_t\} = C_{t+1} \cap \bigcup_{i=1}^{t} C_i$ (for $t=1,\ldots,m-1$), and write $p_1,\ldots,p_k$ for the distinct elements in $\{x_1,\ldots,x_{m-1}\}$.

We may now construct an A-graph G by identifying the edges with the elements of E and by taking $C_1,\ldots,C_m$ as the fundamental cycles; by (3.12.3) each C_{t+1} $(t=1,\ldots,m-1)$ has exactly one 'edge' x_t in common with $\bigcup_{i=1}^{t} C_i$ so we can also ensure that in the construction the endpoints of x_t are the only vertices in common with $\bigcup_{i=1}^{t} C_i$. The set $P = \{p_1,\ldots,p_t\}$ is clearly the pivot set and does not contain a cycle since $P \subset B$. As in the above proof of sufficiency, B is a basis (spanning forest) for M(G), and by construction the B-basic c.i. matrix of M(G) is precisely A_B. Now M(G) is certainly binary (graphic matroids are in fact regular), and by (3.6), M is binary. Thus by (3.3.1) both matroids have the same representation matrix $[I_r|A_B]^T$ over GF(2) from which it follows that M = M(G) as required.

Theorem (3.12) appears to be the first characterization of binary FT matroids. It has been proved in [16] that binary transversal matroids are graphic, and this result has since been subsumed by Theorem 14.4.1 of [37] identifying the larger class of binary gammoids with the cycle matroids of series parallel networks. Also in [5] graphical transversal matroids are characterized as those graphs which contain no subgraph homeomorphic to K_4 or C_k^2 $(k>2)$; of course A-graphs are more restrictive since $K_{2,3}$ is not an A-graph (so that $M(K_{2,3})$ provides an example of a transversal matroid which is not an FT matroid). It seems reasonable to conjecture that $K_{2,3}$ is the only extra 'obstruction' for A-graphs .

§ 4 PROJECTIVE SPACES AND THEIR MATROID REPRESENTATIONS

In this chapter we are primarily concerned with the representations of those matroids (of example (1.20.2)) arising from a collection of points in the projective space $PG(r,F)$ (where F is a field and $r \geq 3$). Suppose that M is such a matroid defined on the points $P_1,\ldots,P_n$. Then the $(n \times r)$ matrix A over F, whose i^{th} row (for $i=1,\ldots,n$) is the natural coordinate vector of P_i, is trivially a representation of M (since M is isomorphic to the matroid induced by linear dependence over F of the rows of A). We shall call A the natural representation of M (over F).

Providing there is no possibility of ambiguity, we shall identify each point in $PG(r,F)$ with its natural coordinate vector in F^r. If M contains the $r+1$ points $(1,0,\ldots,0),(0,1,\ldots,0),\ldots,(0,\ldots,0,1),(1,1,\ldots,1)$ we shall always assume that in the matrix A these correspond to the first $r+1$ rows, in which case, by (2.10) and (2.12.4), the natural representation matrix of M is already in projective canonical form.

The natural representation is certainly not (even up to projective equivalence) the only representation of M in general. However if F is a finite prime field and M the collection of all the points of $PG(r,F)$ then it is shown in [12] that M is uniquely F-representable, so that every representation is projectively equivalent to the natural representation. We generalise this result to all fields and this requires our extending the notion of projective equivalence in a way which we will show is naturally justified.

First we describe a procedure for constructing matroids whose representations are easily classified, with interesting characteristic sets, This procedure will also be used to prove the result mentioned above.

Geometric addition and multiplication

Most classical proofs of the Coordinatization theorem (1.10) involve the concept of geometric 'addition' and 'multiplication' of points on a line as originated in the famous 'Von Staudt Calculus'. The idea behind the proofs is to show that with respect to these operations, the collection of points on a line form a division ring which is a field if and only if the projective space is Pappian. The reader is referred to [24,25,27] for a full account of this process. If we now 'turn the tables' and actually start with a collection of points in PG(r,F) we may mimick the type of constructions for addition and multiplication defined for an arbitrary projective space and derive some very useful consequences for our study of matroid representations.

Let us label once and for all certain points of the projective plane PG(3,F) :-

For each $x \in F$, write $P_x = (1,0,x)$. In particular

$$P_0 = (1,0,0), \quad P_1 = (1,0,1)$$

Let $I = (0,0,1)$, $Q_0 = (0,1,0)$, $Q_1 = (0,1,1)$, $J = (1,-1,0)$.

The points P_0, Q_0, I, P_1, Q_1 will be called the five basic points.

For any two distinct lines ℓ_1, ℓ_2 the unique point of intersection of ℓ_1 and ℓ_2 will be denoted by $\ell_1 \wedge \ell_2$.

Let $\mathcal{F}$ denote the collection of points $\{P_x;\ x \in F\}$, so that $\mathcal{F}$ consists of precisely the set of points on P_0P_1 with the exception of I . We now define the geometrical addition and multiplication of any two points in $\mathcal{F}$.

(4.1) Addition in $\mathcal{F}$ (see fig.(4.1.1)).

Let P_x, $P_{x'}$ be any two points in $\mathcal{F}$.

Let $A = (P_xQ_1) \wedge (P_0Q_0)$, $B = (AI) \wedge (P_{x'}Q_0)$

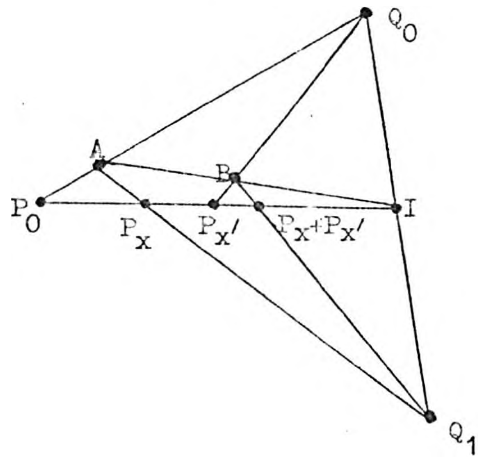


FIGURE (4.4.1)

Now define the point $P_x + P_{x'}$ to be the point $(P_0P_1) \wedge (BQ_1)$

A simple argument on determinants shows that $A = (1,-x,0)$, since P_0, Q_0, A, collinear implies A must be of the form $(1,z,0)$ for some $z \in F$ and now P_x, Q_1, A collinear implies

$$\begin{vmatrix} 0 & 1 & 1 \\ 1 & z & 0 \\ 1 & 0 & x \end{vmatrix} = 0$$

whence $z = -x$. By similar arguments it follows that $B = (1,-x,x')$ and hence also, that

$$P_x + P_{x'} = (1,0,x+x') = P_{x+x'} \qquad (4.4.2)$$

Thus 'addition' is a commutative, binary operation on $\mathscr{F}$, with unique identity P_0, and each point P_x has unique inverse P_{-x}.

(4.2) Multiplication in $\mathscr{F}$ (fig.(4.2.1))

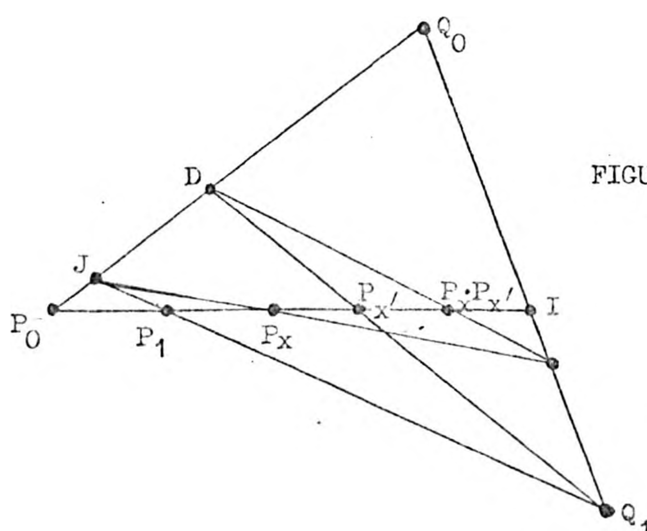


FIGURE (4.4.2)

For any two points P_x, $P_{x'}$ in

$$\text{Let} \quad C = (P_x J) \wedge (Q_0 Q_1) \ , \quad D = (P_{x'} Q_1) \wedge (P_0 Q_0)$$

Now define $P_x \cdot P_{x'}$ to be the point $(P_0 P_1) \wedge (DC)$

Again by an argument on determinants it follows that

$C = (0,1,x)$, $D = (1,-x',0)$ and hence that

$$P_x \cdot P_{x'} = (1,0,xx') = P_{xx'} \qquad (4.2.2)$$

Thus 'multiplication' is a commutative, binary operation on $\mathcal{F}$ with unique identity P_1, and each point P_x $(x \neq 0)$ has unique inverse $P_{x^{-1}}$.

(4.3) Corollary The set $\mathcal{F}$ together with 'addition' and 'multiplication' defined in (4.1),(4.2) respectively, is a field and the mapping $x \rightarrow P_x$ is an isomorphiem of F onto $\mathcal{F}$.

Proof Immediate from (4.1.2) and (4.2.2)

Although the existence of an additive and multiplicative inverse for each P_x in $\mathcal{F}$ $(x \neq 0)$ is already ensured, we next exhibit geometrical constructions of $-P_x$ and $(P_x)^{-1}$ from the five basic points together with P_x :-

(4.4) Construction of $-P_x$ (fig (4.4.1))

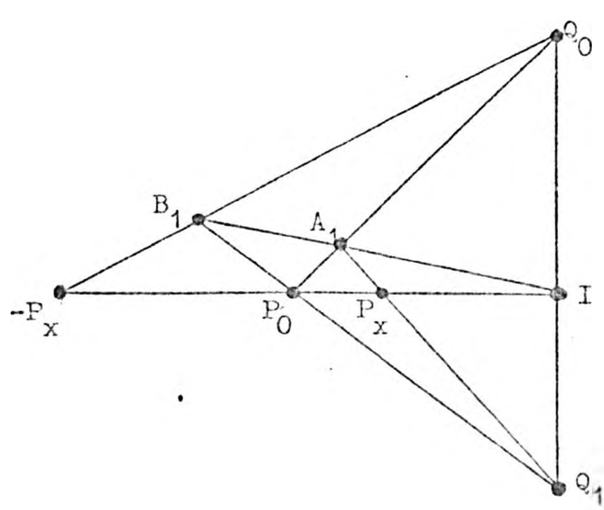


FIGURE (4.4.1)

Let $A_1 = (P_0Q_0) \wedge (P_xQ_1)$, $B_1 = (P_0Q_1) \wedge (A_1I)$

Now define $-P_x = (B_1Q_0) \wedge (P_0P_1)$

It follows that $A_1 = (1,-x,0)$, $B_1 = (1,-x,-x)$ and hence that

$$-P_x = (1,0,-x) = P_{-x}$$

(4.5) <u>Construction of $(P_x)^{-1}$</u> $(x \neq 0)$

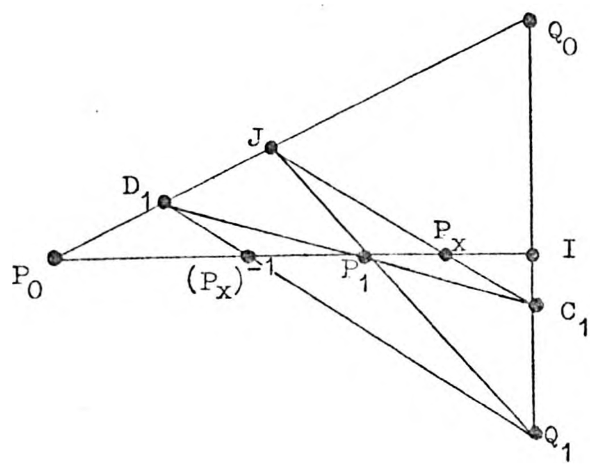


FIGURE (4.5.1)

Let $C_1 = (JP_x) \wedge (Q_0Q_1)$, $D_1 = (C_1P_1) \wedge (P_0Q_0)$

Now define $(P_x)^{-1} = (D_1Q_1) \wedge (P_0P_1)$

It follows that $C_1 = (0,1,x)$, $D_1 = (1,-x^{-1},0)$ and hence that

$$(P_x)^{-1} = (1,0,x^{-1}) = P_{x^{-1}}$$

(4.6) <u>Definition</u> Let $z, x_1,\ldots,x_n \in F$. Then z is <u>constructible from $x_1,\ldots,x_n$</u> if the point P_z may be constructed by some finite sequence of the four operations (given above) starting with the points $P_{x_1},\ldots,P_{x_n}$ and the five basic points.

For example, if x_1,x_2 $(\neq 0) \in F$. then the element $z = (x_1+x_2)x_1^{-1} - x_1^2x_2$ is constructible from x_1,x_2. The construction may be achieved in several ways; one way would be to first construct x_1+x_2 (by (4.1)), x_1^2 (by (4.2)), and x_1^{-1} (by (4.5)). Next construct $x_1^2 \cdot x_2$ (by (4.2)) and hence then $-(x_1^2 \cdot x_2)$ (by (4.4)). Next construct $(x_1 + x_2) \cdot x_1^{-1}$ (by (4.2)) and finally we get P_z the result of the construction (4.1), $P_{(x_1+x_2)\cdot x_1^{-1}} + P_{-x_1^2 x_2}$.

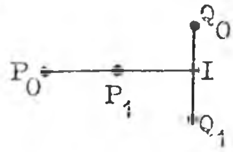
Given just the basic five we can still construct new points since $P_1 + P_1 = P_2$. Any point which is constructible from the basic five points alone will simply be called constructible.

(4.7) Proposition For $z \in F$, z is constructible if and only if $z \in k$ (the prime subfield of F).

Proof For each positive integer m we can construct (inductively) $P_m = P_{m-1} + P_1$. Using (4.4) and (4.5) we can thus deal with either of the cases $k = GF(p)$ or $k = \mathbb{Q}$

(4.8) Corollary For $z, x_1, \ldots x_n \in F$, z is constructible from $x_1, \ldots, x_n$ if and only if $z \in k(x_1, \ldots, x_n)$.

Suppose then that $z \in k(x_1, \ldots, x_n)$. For a particular construction of P_z from $x_1, \ldots, x_n$ the matroid induced (in the sense of (1.20.2)) by precisely the set of points occuring in the construction (including the basic five) will be denoted by M_z . (For an arbitrary point P, not necessarily on P_0P_1, if P is constructible from a given set of points then we can also define M_P in the same way). Before examining the representability of M_z we note that there is another very closely related matroid induced by the construction of P_z ; let C_z be the planar configuration consisting only of those points and those lines actually drawn in the construction of P_z (with the exception that we always assume C_z 'contains' the basic configuration below)



Since all the 'points' and 'lines' of C_z were derived from a projective plane we know that each pair of lines of C_z meets in at most one point of C_z. Hence it follows by a well known result (see,e.g. [37] p.31) that C_z induces a unique simple matroid M'_z whose bases are those 3-sets of points which are not collinear in C_z. Of course M'_z contains the same set of 'points' as M_z and any 3 collinear point in M'_z must be collinear in M_z. In general however the converse is not true; consider for example the construction of the point $P = (1,-1, 1)$ (in an arbitrary field) shown in Figure (4.8.1). If char $F = 2$ then the points

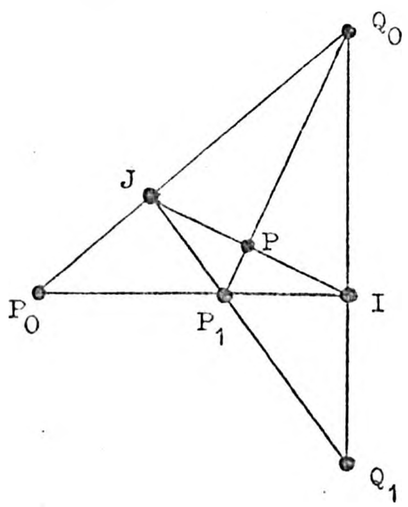


FIGURE (4.8.1)

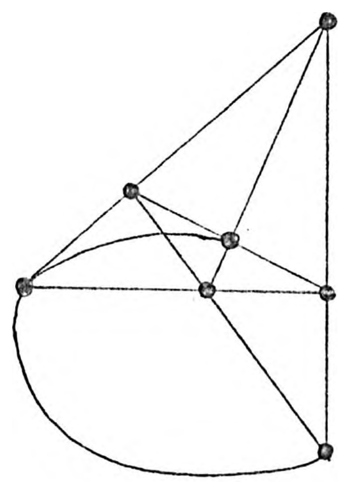


FIGURE (4.8.2)

P, P_0, Q_1 are necessarily collinear in PG(3,F) since

$$\begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & -1 & 1 \end{vmatrix} = 2$$

Consequently the matroid M_P (shown in fig.(4.8.2)) differs from M'_P since the extra line joining P, P_0, Q_1 has had to be added. (The discerning reader will notice that in this particular case M_P is precisely the Fano matroid and M'_P the non-Fano matroid - we shall have more to say about this example in (4.14.1)).

In general then the best we can say is that M_z is always a 'weak map image' of M'_z. In the cases when $M_z = M'_z$ the matroid M_z will assume added significance.

Suppose now that the matrix A_z is the natural representation of the matroid M_z. We shall always assume the points of M_z are listed in order of their construction and that the first five are the basic five in the order P_0, Q_0, I, P_1, Q_1 (this ensures A_z is already in p.c.f.) followed by $P_{x_1}, \ldots, P_{x_n}$. Suppose for example that $z = x_1 + x_2$ is constructed from x_1, x_2 by (4.1).

$$\text{Then} \quad A_z^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & -x_1 & -x_1 & 0 \\ 0 & 0 & 1 & 1 & 1 & x_1 & x_2 & 0 & x_2 & z \end{bmatrix}$$

(4.9) <u>Convention</u> Let $f = f(X_1, \ldots, X_n)$ be a rational function over $Z[X_1, \ldots, X_n]$ (that is, f is a quotient of polynomials in $Z[X_1, \ldots, X_n]$). If F is any field and $x_1, \ldots, x_n$ any elements in F, then the expression $F(x_1, \ldots, x_n)$ will denote the natural evaluation of f at $x_1, \ldots, x_n$ in F (providing that the denominator is non-zero in this evaluation).

Suppose that M_z is the matroid induced by the construction of z from $x_1, \ldots, x_n$ with natural matrix representation A_z. Because of the values of the points $A, B, C, D, A_1, B_1, C_1, D_1$ determined in (4.1), (4.2), (4.4), (4.5) it follows that for each entry (i,j) of A_z there is a rational function $f_{ij}(X_1, \ldots, X_n)$ for which the (i,j) entry is $f_{ij}(x_1, \ldots, x_n)$ (in the sense of (4.9)). In fact each entry of A_z is uniquely determined in this way by some previous rows. With this terminology we have

(4.10) <u>Proposition</u> <u>Suppose that the matrix A is a representation of M_z in p.c.f. over some field K. Then there exist elements $y_1, \ldots, y_n$ of K such that the (i,j) entry of A is $f_{ij}(y_1, \ldots, y_n)$.</u>

Proof Since A is a representation of M_z in p.c.f. it follows from (1.42) that its first 5 rows are precisely

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

(noting that the last entry in the 5^{th} row is atomic hence equal to 1). Also, the first non-zero entry in each subsequent row is equal to 1, so all the rows of A are natural coordinate vectors of points in PG(3,K) - and we shall identify them as such. The next n rows of A (corresponding to the P_x's) have the form $(1,0,y_1),\dots,(1,0,y_n)$ for elements $y_1,\dots,y_n$ of K. We show that these are the required elements. Suppose the i^{th} row of A_z is the point R_i (of PG(3,F)) and the i^{th} row of A is the point R_i' (of PG(3,K)). For each $i \leq n+5$ the rows R_i, R_i' correspond in the ascribed way. By induction assume $s > n+5$ and that the result holds for all rows R_i with $i<s$. By construction R_s is the unique point of intersection of two lines in PG(3,F) of the form R_iR_j where $1 \leq i,j < s$. So suppose $R_s = R_{i_1}R_{i_2} \wedge R_{i_3}R_{i_4}$ where $1 \leq i_1,i_2,i_3,i_4 < s$. We may assume that $R_s = (1,a,b)$ say, (the proof is even easier if the first coordinate is zero) where $a = f(x_1,\dots,x_n)$, $b = g(x_1,\dots,x_n)$ for some rational functions $f(X_1,\dots,X_n)$, $g(X_1,\dots,X_n)$. Suppose $R_s' = (1,\alpha,\beta)$ for $\alpha,\beta \in K$. We have to show that $\alpha = f(y_1,\dots,y_n)$, $\beta = g(y_1,\dots,y_n)$.

Since R_{i_1}, R_{i_2}, R_s are collinear and R_{i_3}, R_{i_4}, R_s are collinear, we have the equations

$$\begin{aligned} \det R_{i_1}R_{i_2}R_s &= 0 \\ \det R_{i_3}R_{i_4}R_s &= 0 \end{aligned} \qquad (4.10.1)$$

which are two simultaneous equations in a,b whose coefficients are the entries of $R_{i_1}, R_{i_2}, R_{i_3}, R_{i_4}$ and whose unique solution is precisely a,b (this is how R_s was constructed). But since A is a representation of M_z, we also have

$$\det R'_{i_1} R'_{i_2} R'_s = 0$$

$$\det R'_{i_3} R'_{i_4} R'_s = 0$$

which are two simultaneous equations in α,β. By the inductive hypothesis, these equations are the same as (4.10.1) except that every occurence of a coefficient say $h(x_1,\dots,x_n)$ of one of the R_{i_j}'s is replaced by $h(y_1,\dots,y_n)$ and every occurence of a,b is replaced by α,β respectively. It now follows that α,β are of the ascribed form.

(4.11) Corollary For any $z \in \mathcal{k}$ the matroid M_z induced by the construction of z (recalling (4.7)) is uniquely K-representable for any field K over which M_z is representable.

Proof In this case the 'rational functions' which determine the entries of A_z all lie in $\mathbb{Q}$, so by (4.10) the p.c.f. of any representation is uniquely determined.

(4.12) Corollary Let $f(X)$ be an irreducible polynomial in $\mathbb{Z}[X]$. Then we can construct a matroid M (of rank 3) with the property that M is only K′-representable for fields K′ in which there is a $\beta \in K'$ for which $f(\beta) = 0$.

Proof The ideal $(f(X))$ of $\mathbb{Z}[X]$ is prime. Consequently $\mathbb{Z}[X]/(f(X))$ is an integral domain with quotient field K say. If π is the natural homomorphism from $\mathbb{Z}[X]$ into K, then clearly π is the identity on $\mathbb{Z}$, and if $\pi(X) = x$ then $f(x) = 0$ in K. Suppose that $f(X) = a_0 + a_1X + \dots + a_tX^t$; certainly $f(x)$ is constructible from x in PG(3,K). First we construct a_tx^t from x and then $a_0 + a_1x + \dots + a_{t-1}x^{t-1}$ (= $g(x)$, say). Now since

$f(x) = g(x) + a_t x^t$ we now construct $f(x)$ by the addition $(1,0,g(x)) + (1,0,a_t x^t)$ described in (4.1). This part of the construction yields the new points $A = (1,-g(x),0)$ and $B = (1,-g(x),a_t x^t)$. The fact that $f(x) = 0$ is now indicated by the dotted line in fig(4.12.1), since P_0 must be the point of intersection of BQ_1 and P_0P_1.

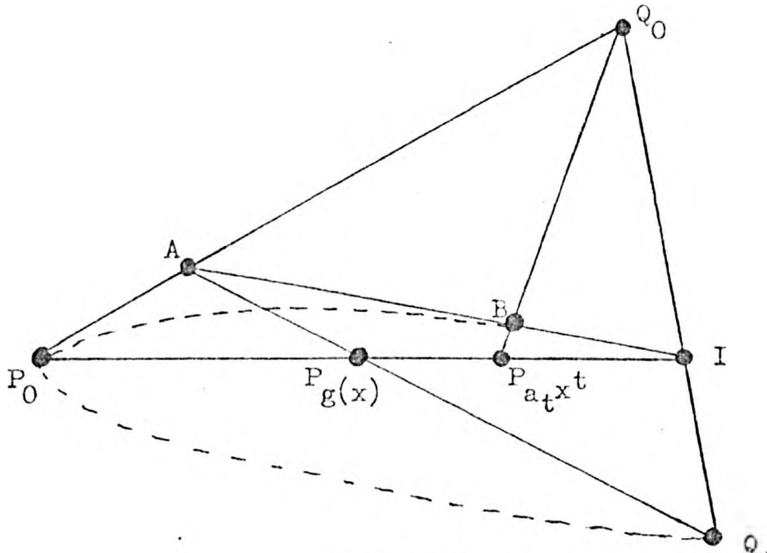


FIGURE (4.12.1)

Now let M be the matroid $M_{f(x)}$ induced by this construction, and let A be the natural representation matrix of M. Suppose that M is K'-representable, and let A' be a K'-representation in p.c.f. By (4.10) there is a $\beta \in K'$ such that the rows of A' corresponding to $(1,0,0)$, $(0,1,1)$, $(1,-g(x),a_t x^t)$ are respectively $(1,0,0)$, $(0,1,1)$, $(1,-g(\beta), a_t\beta^t)$. But these three points are dependent since P_0,A,B are collinear in PG(3,K) and A' is a representation of M. Thus in K'

$$\begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & -g(\beta) & a_t\beta^t \end{vmatrix} = 0$$

that is, $f(\beta) = g(\beta) + a_t\beta^t = 0$ as claimed.

A straightforward generalisation of the above proof yields:-

(4.13) Corollary Let $f_1(X_1,\ldots,X_n),\ldots,f_t(X_1,\ldots,X_n)$ be polynomials in $\mathbb{Z}[X_1,\ldots,X_n]$ which generate an ideal whose radical is prime. Then there is a matroid M with the property that for any field K', M is K'-representable only if there are $\beta_1,\ldots,\beta_n \in K'$ such that $f_i(\beta_1,\ldots,\beta_n) = 0$ for $i=1,\ldots,t$.

(4.14) Examples

1) In the case of (4.12) when $f(X)= p$ (p a positive prime), the construction is none other than the construction of $p = 0$ in GF(p). Provided that we now construct each n $(2\leq n<p)$ inductively by $(1,0,1) + (1,0,n-1)$, the resulting matroid M_p has natural representation matrix A where

$$A^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & -1 & -1 & 0 & -1 & 0 & -1 & 0 & -1 & \cdots & 0 & -1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 2 & 2 & 3 & 3 & 4 & 4 & \cdots & p-1 & p-1 \end{bmatrix}$$

The last line in this construction joins $(1,0,0),(0,1,1),(1,-1,p-1)$ and the corresponding determinant is equal to p. It follows that $c(M_p) = \{p\}$ since by (4.11) any K-representation of M_p in p.c.f. is equal to A. We also note that if the last line is omitted the resulting matroid has characteristic set equal to $P\setminus\{p'$ prime, $p'\leq p\}$. In the case when p=2 these constructions yield respectively the Fano and non-Fano matroids of figs.(4.8.2) and (4.8.1).

2) The preceding example suggests a very naïve procedure for constructing matroids with two-prime characteristic set $\{p_1,p_2\}$ say. The idea would be to construct the number $n=p_1p_2$ over either $GF(p_1)$ or $GF(p_2)$. By (4.12) the resulting matroid is only representable over fields of characteristic p_1 or p_2, but we encounter the problem that the representation matrix may have determinants (other than the one corresponding to the 'last line') divisible by p_1 or p_2. Not surprisingly then the whole problem of finding finite (non-singleton) characteristic sets is an

extremely difficult one. Until very recently the only known example was that of Reid who exhibited a matroid with characteristic set $\{1103, 2809\}$. More recently Ingleton,[21] has exhibited a matroid with characteristic set $\{13, 19\}$. Neither of these examples have been published and (to the best of my knowledge) only the matrices which induce the matroids have been exhibited in private communications. We now provide a geometrical motivation for both these examples; what is remarkable is that they can be constructed by only a slightly more subtle approach than that suggested above:-

The Mersenne non-prime $2^{29}-1$ has the prime factorisation $2^{29}-1 = 233.1103.2809$. Consequently $2^{29} = 1$ over each of the fields $GF(p)$, $p = 233, 1103, 2809$. We now construct 2^{29} (over any of these fields) in the following manner:- first construct $P_1 + P_1 = P_2$ $(=(1,0,2))$ which involves the new points $(1,-1,0),(1,-1,1)$ and P_2. Next construct $P_2 . P_2 = P_4$ $(=(1,0,4))$ which involves the new points $(0,1,2),(1,-2,0)$ and $(1,0,2^2)$. Now inductively for each $2 \leq n \leq 28$ construct $P_{2^{n-1}} . P_2 = P_{2^n}$. At each of these stages the only new points occuring are $(0,1,2^{n-1})$ and $(1,0,2^n)$. The last part of the construction is $P_{2^{28}} . P_2 = (1,0,2^{29}) = (1,0,1)$ which will mean that the points $(1,-2,0)$, $(0,1,2^{28})$, $(1,0,1)$ are collinear. By (4.11) the resulting matroid M is uniquely representable by its natural representation matrix A where

$$A^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & \cdots & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & -1 & -1 & 0 & -2 & 1 & 0 & 1 & 0 & 1 & 0 & \cdots & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 2 & 0 & 2 & 2^2 & 2^2 & 2^3 & 2^3 & 2^4 & & 2^{27} & 2^{28} & 2^{28} \end{bmatrix}$$

Since

$$\begin{vmatrix} 1 & 0 & 1 \\ 1 & -2 & 0 \\ 0 & 1 & 2^{28} \end{vmatrix} = 1 - 2^{29}$$

it follows that $\{233, 1103, 2809\} \supset c(M)$. It is not difficult to check that no other subdterminants of A are divisible by 1103 or 2809 and so $\{1103, 2809\} \subset c(M)$. We note that $233 \notin c(M)$ since

$$\begin{vmatrix} 1 & -1 & 1 \\ 1 & 0 & 2^6 \\ 0 & 1 & 2^{16} \end{vmatrix} = 2^{16} - 2^6 + 1$$

which is divisible by 233, and so $c(M) = \{1103, 2809\}$. The matrix A was precisely that which was presented by Reid .

We note that $2^{29}-1$ is the smallest Marsenne non-prime for which the above construction yields a two-prime characteristic set. For example the construction of $2^{11} - 1 = 23.89$ yields the subdeterminant

$$\begin{vmatrix} 1 & -1 & 1 \\ 1 & 0 & 2^2 \\ 0 & 1 & 2^8 \end{vmatrix} = 2^8 - 2^2 + 1 = 253$$

which is divisible by 23, so again we can only obtain a singleton characteristic set.

3) (Ingleton's matroid)

We notice that $13.19 = 8.32 - 9$ and so $8.32 = 9$ in GF(13) or GF(19). First then we construct 8.32 :-

$P_1 + P_1 = P_2$ which yields new points $(1,-1,0)$, $(1,-1,1)$ and P_2

Next $P_2 . P_2 = P_4$ which yields points $(0,1,2)$, $(1,-2,0)$ and P_4

Next $P_2 . P_4 = P_8$ " " " $(1,-4,0)$ and P_8

Next $P_8 . P_4 = P_{32}$ " " " $(0,1,8)$ and P_{32}

Now the construction of $P_8 . P_{32}$ yields new point $(1,-32,0)$. If we construct P_9 then the fact that $8.32 = 9$ will be indicated by the collinearity of the points $(1,-32,0)$, $(0,1,8)$, P_9. But the points $(1,-1,1)$, $(0,1,8)$, $(1,-32,0)$ already constructed are collinear over GF(13) and GF(19) since

$$\begin{vmatrix} 1 & -1 & 1 \\ 0 & 1 & 8 \\ 1 & -32 & 0 \end{vmatrix} = 8.32 - 8 - 1 = 13.19$$

Consequently the matroid M constructed up to the point (1,-32,0) is by (4.11) uniquely representable by its natural representation matrix A, where

$$A^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & -1 & -1 & 0 & 1 & -2 & 0 & -4 & 0 & 1 & 0 & -32 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 2 & 2 & 0 & 4 & 0 & 8 & 8 & 32 & 0 \end{bmatrix}$$

It is easily checked that no other subdeterminants of A are divisible by 13 or 19 and consequently $c(M) = \{13, 19\}$.

The matrix A^T, with the first column deleted, is precisely the matrix which was presented by Ingleton.

Remark In all the above work we have restricted ourselves to the plane and rank 3 matroids. However it follows from the work in [23] that if for any r>3, M is a matroid of rank r and characteristic set C, then there is a matroid M_1 of rank 3 and characteristic set C (M_1 is formed by the 'Dilworth truncation'). Since we have been primarily interested in the characteristic set problem we are thus justified in concentrating our attentions on planar configurations.

Generalised Projective Equivalence

Suppose that the (n×r) matrix $A=[a_{ij}]$ is a natural representation matrix (in p.c.f) for a collection of points of PG(r,F). If σ is an automorphism of F it is clear that the matrix $A'=[\sigma(a_{ij})]$ is again a representation (in p.c.f.). Unless σ is the identity mapping the matrices A,A′ will not be projectively equivalent (by (2.11)). Indeed (by (1.2)) this is precisely why Brylawski and Lucas' result about unique representability of full projective geometries (in [12]) only holds for (finite) prime fields. However, what is unmistakable is that the automorphism induces (by (1.12)) an auto-projectivity of $PG(r,F)$ in which the i^{th} row of A is mapped onto the i^{th} row of A' (identifying points of $PG(r,F)$ with their natural coordinate vectors as usual) for $i=1,\ldots,n$. Thus the geometrical viewpoint suggests that we extend our definition of projective equivalence to include this case since in the sense of (1.9) the matrices A,A' are 'projectively' equivalent. From an algebraic viewpoint there are also grounds for suggesting that we extend the definition of projective equivalence to include this case, since (for reasons on which we shall elucidate later) we can always find a division ring D containing F and an element $x \in D$ for which $xa = \sigma(a)x$ for each $a \in F$; consequently the matrices A,A' are projectively equivalent over D, since

$$(xI_n)\ A\ (x^{-1}I_r) = [xa_{ij}x^{-1}] = [\sigma(a_{ij})] = A'$$

Inspired by these examples we make the following definition

(4.15) Definition Let $A=[a_{ij}]$, $A'=[b_{ij}]$ be $(s\times t)$ block irreducible matrices over fields F_1, F_2 respectively (see (4.16) below) which are in p.c.f. The matrices A,A' are <u>generally projectively equivalent</u> (<u>g.p.e.</u>) if there is an isomorphism $\sigma:F_1\to F_2$ in which $\sigma(a_{ij}) = b_{ij}$ for each entry a_{ij} of A. Two arbitrary block irreducible matrices are generally projectively equivalent if their associated p.c.f.'s are g.p.e. Two arbitrary matrices are g.p.e. if their blocks are g.p.e.

(4.16) Note When we say that A is a matrix over a field F we shall always assume that the smallest subfield of F generated by the entries of F is F itself.

When $F_1 = F_2$ and $\sigma = id_{F_1}$, definition (4.15) reduces to projective equivalence. We will eventually show that there are both natural algebraic and geometrical characterizations of generalised projective equivalence exactly along the lines suggested above, and the work in §5 will yield another surprising characterization. First however we present the promised generalisation of the result of Brylawski and Lucas.

(4.17) Theorem For any finite field F and integer $r \geq 3$, any two representations of $PG(r,F)$ (viewed as a matroid) are g.p.e.

I present two proofs of this result ; the first (short) proof relies on two classical results of projective geometry already mentioned in §1, while the second is an elementary and intuitive proof using only the constructions of (4.1) and (4.2).

First Proof It suffices to show that any representation of $PG(r,F)$ is g.p.e. to the natural representation. (which we have already noted is in p.c.f.). Let $A=[a_{ij}]$ be the natural representation and let $A'=[b_{ij}]$ be another representation in p.c.f. over some field F' say. Since A' is in p.c.f. it follows (by (1.42)) that the first $r+1$ rows of A' are precisely

$$\begin{bmatrix} I_r \\ \hline 1 \; 1 \ldots 1 \end{bmatrix}$$

and the leading entry in each row is equal to 1. For each row i of A, A' respectively let P_i, Q_i denote the corresponding points of $PG(r,F), PG(r,F')$. Then since A' is a matroid representation of $PG(r,F)$ - a Desarguesian projective space - it follows that the Q_i's themselves form a Desarguesian projective subspace of $PG(r,F')$ of rank r. By (1.10) this subspace must be of the form $PG(r,F'')$ for some subfield F'' of F', which by (4.16) must be equal to F'. Thus the mapping $\pi: PG(r,F) \longrightarrow PG(r,F')$ defined by $\pi(P_i) = Q_i$ for each i, is clearly a projectivity of $PG(r,F)$ onto $PG(r,F')$. By (1.13), π is induced by a semi-linear transformation (σ',σ'') $F^r \rightarrow F'^r$ defined as in (1.11). This means that for each $\underline{v} \in F^r$, $\pi(F\underline{v}) = F'(\sigma'(\underline{v}))$. In particular, for $i=1,\ldots,r$

$$F'(0,\ldots,\underset{\substack{\uparrow \\ i^{\text{th}} \text{ place}}}{1},\ldots,0) = \pi(F(0,\ldots,1,\ldots,0) = F'(\sigma'(0,\ldots,1,\ldots,0))$$

Thus $\sigma'(0,\ldots,1,\ldots,0) = (0,\ldots,\lambda_i,\ldots,0)$ for some $0 \neq \lambda_i \in F'$.
Also, $F'(1,1,\ldots,1) = \pi(F(1,1,\ldots,1)) = F'(\sigma'(1,1,\ldots,1))$
so that $\sigma'(1,1,\ldots,1) = \lambda(1,1,\ldots,1)$ for some $0 \neq \lambda \in F$.
But then

$$\begin{aligned}\lambda(1,1,\ldots,1) &= \sigma'(1,0,\ldots,0) + \ldots + \sigma'(0,\ldots,0,1)\\ &= (\lambda_1,\ldots,\lambda_r)\end{aligned}$$

$$\text{Thus } \lambda = \lambda_1 = \lambda_2 = \ldots = \lambda_r$$

Consequently, for each $(c_1,\ldots,c_r) \in F^r$, we have

$$\begin{aligned}\sigma'(c_1,\ldots,c_r) &= \sigma'(c_1,0,\ldots,0) + \ldots + \sigma'(0,\ldots,0,c_r)\\ &= \sigma''(c_1)\,\sigma'(1,0,\ldots,0) + \ldots + \sigma''(c_r)\,\sigma'(0,\ldots,1)\\ &= \sigma''(c_1)\,(\lambda,0,\ldots,0) + \ldots + \sigma''(c_r)(0,\ldots,0,\lambda)\\ &= \lambda\,(\sigma''(c_1),\ldots,\sigma''(c_r))\end{aligned}$$

In particular, if we consider the i^{th} row of A we get

$$\begin{aligned}F'(b_{i1},\ldots,b_{ir}) = \pi(F(a_{i1},\ldots,a_{ir})) &= F'(\sigma'(a_{i1},\ldots,a_{ir}))\\ &= F'(\lambda\,(\sigma''(a_{i1}),\ldots,\sigma''(a_{ir}))\\ &= F'(\sigma''(a_{i1}),\ldots,\sigma''(a_{ir})) \qquad (4.17.1)\end{aligned}$$

Now $(a_{i1},\ldots,a_{ir})$, $(b_{i1},\ldots,b_{ir})$ both have their leading entry equal to 1, appearing in the same corresponding position. Since $\sigma''(1) = 1$, the same is true of $(\sigma''(a_{i1}),\ldots,\sigma''(a_{ir}))$ and $(b_{i1},\ldots,b_{ir})$. Consequently by (4.17.1) we deduce that $(\sigma''(a_{i1}),\ldots,\sigma''(a_{ir})) = (b_{i1},\ldots,b_{ir})$, and since this is true for each row of A, it follows that σ'' is the required isomorphism of F onto F' which makes A,A' g.p.e.

Second proof We proceed by induction on r, the most important step being the first, r = 3. Let $A=[a_{ij}]$ be the natural representation of PG(3,F) and let $A'=[b_{ij}]$ be another representation (in p.c.f.) over some field F'. As usual we identify points of PG(3,F) (and PG(3,F')) with their natural coordinate vectors and the points I,Q_0,Q_1,J and P_x (for each $x \in F$) are defined as before.

Let γ be the mapping of PG(3,F) into PG(3,F') which takes rows of A onto the corresponding rows of A'. Then for any three points P,Q,R of PG(3,F), the fact that A' is a representation of PG(3,F) (viewed as a matroid) means that

> P,Q,R are collinear if and only if $\gamma(P),\gamma(Q),\gamma(R)$, are collinear and this happens precisely when the corresponding subdeterminants of A,A' are zero.

The above fact will be assumed henceforth without further comment. Now all the points of PG(3,F) (that is, rows of A) have the form:-

$$\begin{array}{lll} \text{(i)} & (1,0,x)\ (=P_x) & \text{for some } x \in F \\ \text{(ii)} & (1,x,0) & \text{for some } x \in F \\ \text{(iii)} & (0,1,x) & \text{for some } x \in F \\ \text{(iv)} & (1,x,x') & \text{for some } x,x' \in F \end{array} \qquad (4.17.2)$$

The first four rows of A are P_0,Q_0,I,J' respectively, where $J'=(1,1,1)$. Since A' is in p.c.f. it follows immediately that

$$\gamma(P_0)=(1,0,0),\quad \gamma(Q_0)=(0,1,0),\ \gamma(I)=(0,1,0) \quad \text{and} \quad \gamma(J')=(1,1,1) \qquad (4.17.3)$$

By (1.42), $\gamma(P_1) = (1,0,\alpha)$ for some $\alpha \in F'$. But J,P_1,Q_0 are collinear, so by (4.17.3) we have

$$0 = \begin{vmatrix} 1 & 1 & 1 \\ 1 & 0 & \alpha \\ 0 & 1 & 0 \end{vmatrix} = 1 - \alpha$$

So in fact we have

$$\gamma(P_1) = (1,0,1) \quad \text{and} \quad \gamma(Q_1) = (0,1,1) \qquad (4.17.4)$$

(the latter following by a similar argument).

Let us now define a mapping $\sigma : F \to F'$ by $\sigma(x) = y$, where y is the (uniquely defined) element of F' for which $\gamma(P_x) = (1,0,y)$. The mapping σ must be injective for otherwise we would have $P_x, P_{x'}, Q_0$ collinear for some $x \neq x'$ which is absurd. Also by (4.17.3) and (4.17.4) we have $\sigma(0) = 0$ and $\sigma(1) = 1$, so if we can show that σ is additive and multiplicative it will follow that $\sigma(F)$ is a subfield of F' isomorphic (under σ) to F :-

σ additive: Let $x, x' \in F$. We may assume neither are zero. Suppose that $\gamma(P_x)=(1,0,y)$ and $\gamma(P_{x'})=(1,0,y')$. We have to show that $\gamma(P_{x+x'})=(1,0,y+y')$ and for this we refer back to fig.(4.1.1); we have established (4.1.2) that $P_x + P_{x'} = P_{x+x'}$. Now $\gamma(Q_1),\gamma(P_x),\gamma(A)$ collinear implies that $\gamma(A)=(1,-y,0)$. Next, $\gamma(A),\gamma(B),\gamma(I)$ collinear and $\gamma(Q_0),\gamma(B),\gamma(P_{x'})$ collinear together imply that $\gamma(B)=(1,-y,-y')$. Finally $\gamma(B),\gamma(Q_1),\gamma(P_x+P_{x'})$ collinear implies that $\gamma(P_{x+x'}) = \gamma(P_x + P_{x'}) = \gamma(1,0,y+y')$.

σ multiplicative: This time we assume x, x' are as above but that neither are equal to 0 or 1. We refer back to fig.(4.2.1). We have established (4.2.2) that $P_x . P_{x'} = P_{x.x'}$ and we have to show that $\gamma(P_{x.x'})= (1,0,yy')$. The collinearity of $\gamma(J),\gamma(P_x),\gamma(C)$ implies that $\gamma(C)=(0,1,y)$, and the collinearity of $\gamma(D),\gamma(P_{x'}),\gamma(Q_1)$ implies that $\gamma(D)=(1,-y',0)$. Finally the collinearity of $\gamma(D),\gamma(C),\gamma(P_x . P_{x'})$ implies that

$$\gamma(P_{x.x'}) = \gamma(P_x . P_{x'}) = \gamma(1,0,yy') \quad \text{as required.}$$

In order to prove the theorem (for r=3) we now have to show (by (4.17.2)) that

$$\begin{array}{llcll} \text{(i)} & (1,0,x) & = & (1,0,\sigma(x)) & \text{for each } x \in F \\ \text{(ii)} & (1,x,0) & = & (1,\sigma(x),0) & \text{for each } x \in F \\ \text{(iii)} & (0,1,x) & = & (0,1,\sigma(x)) & \text{for each } x \in F \\ \text{and (iv)} & (1,x,x') & = & (1,\sigma(x),\sigma(x')) & \text{for each } x,x' \in F \end{array}$$

since in that case $\sigma(F) = F'$ and σ is the required isomorphism. Certainly (i) holds since this is how σ was defined. For (ii) let $Q=(1,x,0)$. Then Q,P_{-x},Q_1 collinear forces $\gamma(Q) = (1,\sigma(x),0)$, since $\gamma(P_{-x}) = (1,0,\sigma(-x)) = (1,0,-\sigma(x))$.

For (iii) let $Q' = (0,1,x)$. Then J,P_x,Q' collinear forces $\gamma(Q') = (0,1,\sigma(x))$.

For (iv) let $Q'' = (1,x,x')$. If $A = (1,-x,0)$, then by (ii) we have $\gamma(A) = (1,-\sigma(x),0)$. But then $Q'',Q_0,P_{x'}$ collinear and Q'',A,I collinear together imply that $\gamma(Q'') = (1,\sigma(x),\sigma(x))$.

This proves the theorem for $r=3$.

Next, assume $r \geq 4$ and that the result holds for full projective spaces of rank $< r-1$. Let $A=[a_{ij}]$ be the natural representation of $PG(r,F)$ and $A'=[b_{ij}]$ another representation (in p.c.f.) over some field F'. Without loss of generality, we may assume that the first $(2r + 1)$ rows of A are

$$\begin{bmatrix} & & I_r & & \\ \hline 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & \cdots & 1 & 0 \\ 1 & 1 & \cdots & 0 & 1 \\ \vdots & & & & \vdots \\ 0 & 1 & \cdots & 1 & 1 \end{bmatrix} \qquad (4.17.5)$$

For each $i=1,\ldots,r$ consider the set of points of $PG(r,F)$ having zero entry in the i^{th} entry. This collection of points is a rank $(r-1)$ subspace (hyperplane) of $PG(r,F)$, isomorphic to $PG(r-1,F)$. Moreover, if A_i is the submatrix of A obtained by deleting all those rows with non-zero entry in the i^{th} position and deleting the i^{th} column, then because of (4.17.5), it is easily seen that A_i is the natural representation of $PG(r-1,F)$ with first r rows equal to

$$\begin{bmatrix} & I_r & \\ \hline 1 & 1 \ldots & 1 \end{bmatrix}$$

and is thus in p.c.f. It is also easily seen that the corresponding submatrix A_i' of A' is a representation (in p.c.f.) of $PG(r-1,F)$ over some subfield F_i' of F' (which we will deduce are all equal to F' presently).

For each $i=1,\ldots,r$ we can thus deduce by the inductive hypothesis that there is an isomorphism $\sigma_i: F \to F_i'$ in which $\sigma(a_{ts}) = b_{ts}$ for each entry $a_{ts} \in A_i$, $b_{ts} \in A_i'$.

We show that $\sigma_i = \sigma_j$ for each $1 \leq i,j \leq r$. Let $\alpha \in F$, then since $r \geq 4$ there must be a row of A in which there are zeros in the i^{th} and j^{th} positions and α appears as the second non-zero entry (the first is always equal to 1). Suppose the corresponding entry (to this α) in A' is $\beta \in F'$. By choice, the selected row of A appears in A_i (with the i^{th} entry deleted) and in A_j (with the j^{th} entry deleted). Thus $\sigma_i(\alpha) = \beta = \sigma_j(\alpha)$, and so $\sigma_i = \sigma_j = \sigma$ say, and $F_i' = F_j' = F''$,say for all $1 \leq i,j \leq r$.

Thus we have an isomorphism σ from F onto a subfield F'' of F in which $\sigma(a_{ts}) = b_{ts}$ provided that row t contains at least one zero entry. So finally we need only consider those rows of A which have only non-zero entries. Let $(1,\alpha_2,\ldots,\alpha_r)$ be such a row and let $(1,\beta_2,\ldots,\beta_r)$ be the corresponding row of A'. Suppose that $\sigma(\alpha_i) = \beta_i'$ for $i=2,\ldots,r$ $(\beta_i' \in F')$. We must show that $\beta_i' = \beta_i$ for each $i=2,\ldots,r$

Write $Q_i = (1,0,\ldots,\underset{\substack{\uparrow \\ i^{th}\text{ place}}}{\alpha_i},\ldots,0)$ and $E_i = (0,\ldots,\underset{\substack{\uparrow \\ i^{th}\text{ place}}}{1},\ldots,0)$

for each $i=2,\ldots,r$ and let H_i be the hyperplane generated by the (r-1) independent points $Q_i, E_2, \ldots, E_{i-1}, E_{i+1}, \ldots, E_r$. The point $P=(1,\alpha_2,\ldots,\alpha_r)$ is the unique point of intersection $\bigcap_{i=2}^{r} H_i$. In particular, for each $i=2,\ldots,r$, the collection of r points $Q_i, E_2, \ldots, E_{i-1}, E_{i+1}, \ldots, E_r, P$ is dependent in PG(r,F). Consequently, the corresponding r rows of A' have zero determinant. But the row corresponding to Q_i must be $(1,0,\ldots,\beta_i,\ldots,0)$. Thus,

$$0 = \begin{vmatrix} 1 & 0 & \cdots & \beta_i & \cdots & & 0 \\ 0 & 1 & \cdots & 0 & \cdots & & 0 \\ \vdots & & & & & & \\ 0 & & & \cdots & & 1 & 0 \\ 0 & & & \cdots & & 0 & 1 \\ 1 & \beta'_2 & \cdots & \beta'_i & \cdots & \beta'_{r-1} & \beta'_r \end{vmatrix} = \beta'_i - \beta_i .$$

and so $\beta_i = \beta'_i$ as claimed for each $i=2,\ldots,r$. Thus $F'' = F'$ and $\sigma : F \to F'$ is the required isomorphism.

(4.18) Corollary (Brylawski and Lucas, [12]) For F = GF(p), where p is prime, the projective space PG(r,F) is uniquely F-representable, that is , any two F-representations of PF(r,F) are projectively equivalent.

Proof By (1.2) there are no (non-identity) automorphisms of F, so the result is immediate from (4.17).

(4.19) Representations of PG(r,F) where F is infinite

Although projective equivalence is not defined for infinite matrices, there is a natural analogue for the p.c.f. for a representation of PG(r,F) when F is infinite; again we may identify PG(r,F) with its natural representation and say that a K-representation of PG(r,F) is in 'p.c.f.' if the simplex $\left[\frac{I_r}{1\ 1 \ldots 1}\right]$ is mapped onto the natural simplex of PG(r,K) and each point is mapped onto a vector in K^r whose first non-zero entry is equal to 1. The only occasion in the proof of (4.17) where the finiteness of F was used was in deducing that the homomorphism σ was surjective. In the light of this we deduce the following result (where A, A' denote infinite sets of r-tuples) :-

If A is the natural representation of PG(r,F), and A' is another representation over some field K (in 'p.c.f.' defined above), then there is an injective homomorphism $\sigma : F \longrightarrow K$ mapping the entries of A onto the corresponding entries of A'.

This result shows the close connection between coordinatizing (arbitrary) projective spaces and representing them when viewed as matroids.

Geometrical and algebraic characterizations of projective equivalence

(4.20) Lemma Suppose A is an (s×t) block irreducible matrix, and B an arbitrary (p×t) matrix without zero rows. Then the atomic entries of the matrix $C = \left[\frac{A}{B}\right]$ are precisely the atomic entries of A together with the leading entries of each row of B.

Proof It is clear that C is block irreducible and hence by (2.21) has (s+p+t-1) atomic entries. By (2.7.3) the atomic entries of the first s rows of C are precisely the atomic entries of A, so there are (s+t-1) atomic entries in these rows. But by (2.7.1) the leading entry in each of the p rows of B is atomic in C, so the result now follows.

Suppose now that A,B are block irreducible (s×r) matrices of rank r over fields F_1, F_2 respectively, in p.c.f. Then the

i^{th} row of A (for $i=1,\dots,s$) is a natural coordinate vector of the point P_i say in $PG(r,F_1)$ and similarly the i^{th} row of B corresponds to the point Q_i say of $PG(r,F_2)$. With these assumptions we now present the promised geometrical characterization of generalised projective equivalence.

(4.21) Theorem T.F.A.E.

(i) The matrices A,B are g.p.e.

(ii) There is a projectivity $\gamma: PG(r,F_1) \longrightarrow PG(r,F_2)$ in which $\gamma(P_i) = Q_i$ for $i=1,\dots,s$.

Proof (i) implies (ii) Let $\sigma : F_1 \longrightarrow F_2$ be the isomorphism mapping entries of A onto the corresponding entries of B. The mapping $\sigma' : F_1^r \longrightarrow F_2^r$ defined by

$$\sigma'(a_1,\dots,a_r) = (\sigma(a_1),\dots,\sigma(a_r))$$

clearly makes the pair (σ',σ) a semi-linear transformation from F_1^r into F_2^r which by (1.12) induces the required projectivity.

(ii) implies (i) We may view A as the first s rows of the natural representation matrix A' of $PG(r,F_1)$ where the remaining rows are the natural coordinate vectors of the remaining points of $PG(r,F_1)$. Since A is block irreducible and in p.c.f. it follows from (4.20) that A' is in p.c.f. (this had to be verified since in this case we may not assume that the first $r+1$ rows of A are $\left[\begin{array}{c} I_r \\ \hline 1\ 1\ \dots\ 1 \end{array}\right]$). Now let B' be the matrix over F_2 whose rows are the image under γ of the corresponding rows of A'. Since $\gamma(P_i) = Q_i$ for $i=1,\dots,s$ the first s rows of B' is the matrix B. As for A', the matrix B' is in p.c.f. Since γ is a projectivity, it follows that B' is a representation of $PG(r,F_1)$ (as well as $PG(r,F_2)$ viewed as a matroid). By (4.17) we deduce that A',B' are g.p.e., and since both these matrices are already in p.c.f. it follows from definition (4.15) that A,B are g.p.e.

(4.22) Note The hypothesis of theorem (4.21) is in no way restrictive for our purposes, since we shall usually be considering matrix representations (in p.c.f.) of a connected, rank r matroid M. If A,B are two such representations then (4.21) (which, by (1.45) is certainly applicable) is of great significance, particularly when both representations are over the same field F ; for then, via the matrices A,B respectively , M generates two subgeometries M_1, M_2 say, of PG(r,F) which by (4.16) and (1.10) are the full space in each case. If A,B are not g.p.e. then (4.21) implies that there is no auto-projectivity of PG(r,F) in which the 'points' of A are mapped onto the 'points' of B. This means in particular that there will be three points (lines) of M_1 which are collinear (concurrent) in M_1 but not collinear (concurrent) in M_2

Example Let M be the rank 3 matroid on $E = \{a,b,c,d,e,f\}$ in which all 3-sets except $\{a,b,c\}$ and $\{c,d,f\}$ are dependent (that is, M is the planar configuration of two disjoint lines of 3 points). Let $F = GF(4) = \{0,1,\varepsilon,\varepsilon^2\}$ where ε is a primitive cube root of unity. It is easily seen that the matrices

$$A_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \hline 1 & 1 & 1 \\ 1 & \varepsilon & 0 \\ 1 & 1 & \varepsilon \end{bmatrix} \qquad A_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \hline 1 & 1 & 1 \\ 1 & \varepsilon & 0 \\ 1 & 1 & \varepsilon^2 \end{bmatrix}$$

are both representations (in p.c.f.) of M over F with respect to the ordering a,b,c,d,e,f. These matrices are clearly not g.p.e. For i=1,2, let γ_i be the mapping from E into PG(3,4) taking points of E onto the corresponding rows of A_i . The three lines $\gamma_1(a)\gamma_1(c)$, $\gamma_1(b)\gamma_1(d)$ and $\gamma_1(e)\gamma_1(f)$ are concurrent in PG(3,4) at the point (1,0,1). However the 'same' three lines $\gamma_2(a)\gamma_2(c)$, $\gamma_2(b)\gamma_2(d)$ and $\gamma_2(e)\gamma_2(f)$ are not concurrent in PG(3,4) since (1,0,1) is not on the line $\gamma_2(e)\gamma_2(f)$.

The promised algebraic characterization of generalised projective equivalence is stated in the following theorem

(4.23) Theorem Let A,B be block irreducible matrices (in p.c.f.) over fields F_1, F_2 respectively. T.F.A.E.

(i) A,B are g.p.e.

(ii) There is a division ring D containing both F_1 and F_2 such that A,B are projectively equivalent over D.

Before proving this theorem we need two lemmas :-

(4.24) Lemma Let A,B be (s×t) block irreducible matrices over fields F_1, F_2 respectively, in which each atomic entry is equal to 1 (so A,B are in s.c.f.). Suppose that D is a division ring containing F_1, F_2 and that A,B are s-projectively equivalent over D. Then there is an $x \in D$ such that $(xI_s)\,A\,(x^{-1}I_t) = B$.

Proof Let $A=[a_{ij}]$ $B=[b_{ij}]$. There are non-zero elements $x_1,\ldots,x_s,\ y_1,\ldots,y_t$ in D for which

$$\operatorname{diag}(x_1,\ldots,x_s)\ A\ \operatorname{diag}(y_1,\ldots,y_t) = B$$

that is, $x_i a_{ij} y_j = b_{ij}$ for each i,j.

Since every atomic entry of A,B equals 1 (and of course they appear in the same corresponding positions) it follows that $y_j = x_i^{-1}$ whenever (i,j) is atomic. Thus if we can show that $x_1 = \ldots = x_s = x$, say, it will follow that $y_1 = \ldots = y_t = x^{-1}$ since every column j contains an atomic entry (i,j) for some i.

So let $1 \leq i < i' \leq s$. We will show $x_i = x_{i'}$.
Certainly every row contains an atomic entry, so suppose (i,j), (i′,j′) are atomic entries in the i^{th} and i'^{th} rows respectively. By (2.23) there is an atomic chain joining (i,j) and (i′,j′). Without loss of generality, assume that this chain has

the form

$$(i,j),(i_1,j),(i_1,j_1),\ldots,(i_k,j'),(i',j')$$

Then $x_i = y_j^{-1} = x_{i_1} = y_{j_1}^{-1} = \ldots = x_{i_k} = y_{j'}^{-1} = x_{i'}$

(4.25) Lemma <u>Suppose F_1,F_2 are subfields of a field F (finitely generated over their prime fields) and that $\sigma : F_1 \to F_2$ is an isomorphism. Then there is a field $K \supset F$ and an automorphism of K which extends σ</u>.

<u>Proof</u> Let K be the algebraic closure of F (1.5), and for $i=1,2$ let E_i be the subfield of K formed by adjoining to F_i a transcendence basis of K over F_i. By (1.3) K/E_i is an algebraic extension. If k is the common prime field of F_1,F_2, then we have the lattice of inclusion

$$\begin{tikzcd}
 & K & \\
E_1 \arrow[ur, dash] & & E_2 \arrow[ul, dash] \\
F_1 \arrow[u, dash] & & F_2 \arrow[u, dash] \\
 & k \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

Since F_1,F_2 are isomorphic, we certainly have

$$\text{tr.d. } F_1/k = \text{tr.d. } F_2/k < \infty$$

But also, by (1.4),

$$\text{tr.d. } K/k = \text{tr.d. } K/F_1 + \text{tr.d. } F_1/k$$

and

$$\text{tr.d. } K/k = \text{tr.d. } K/F_2 + \text{tr.d. } F_2/k$$

Thus it follows that $\text{tr.d. } K/F_1 = \text{tr.d. } K/F_2$. But K/E_i is algebraic $(i=1,2)$, so by another application of (1.4),

$$\text{tr.d. } E_1/F_1 = \text{tr.d. } K/F_1 = \text{tr.d. } K/F_2 = \text{tr.d. } E_2/F_2 .$$

Consequently there is a set I, and transcendence bases $\{X_i\}_{i\in I}$, $\{Y_i\}_{i\in I}$ for E_1/F_1, E_2/F_2 respectively. Now

$E_1 = F_1(\{X_i\}_{i\in I})$ and $E_2 = F_2(\{Y_i\}_{i\in I})$, so we may extend σ to an isomorphism $\sigma_1 : E_1 \longrightarrow E_2$ by defining $\sigma(X_i) = Y_i$ for each $i \in I$, and $\sigma_1(a) = \sigma(a)$ for each $a \in F_1$.

Now K is the algebraic closure of both E_1, E_2, so by (1.7) the isomorphism σ_1 extends to an automorphism of K.

Proof of (4.23)

(i) implies (ii) Suppose $A=[a_{ij}]$, $B=[b_{ij}]$. Let $\sigma : F_1 \longrightarrow F_2$ be an isomorphism in which $\sigma(a_{ij}) = b_{ij}$. We can certainly find a field containing both F_1, F_2 and so by (4.16) we may apply (4.25) to deduce the existence of a field K (containing F_1, F_2) and an automorphism τ of K which extends σ. A well known procedure in Ring Theory (described, for example in [14] Vol II, p.436) allows us to construct under these circumstances a (non-commutative) ring - called the Skew Polynomial Ring of K, τ and denoted by $K[x,\tau]$ - which contains K and an element $x\ (\neq 0)$ for which $xa = \tau(a)x$ for each $a \in K$. This ring in turn is contained in a division ring D (again see [14] Vol II, pp.448-450). But now, over D we have,

$$(x\, I_s)\ A\ (x^{-1} I_r) = [x a_{ij} x^{-1}] = [\tau(a_{ij})] = [b_{ij}] = B$$

so that, A,B are projectively equivalent over D

(ii) implies (i) Let $A' = [a_{ij}]$, $B' = [b_{ij}]$ be the non-identity submatrices of A,B respectively (defined in (2.3)). Then by (2.3), A', B' are s-projectively equivalent over D. Thus by (4.24) there is a non-zero element $x \in D$ such that

$$x\, a_{ij}\, x^{-1} = b_{ij} \qquad (4.23.1)$$

If $\mathcal{k}$ is the (common) prime field of F_1, F_2, it follows from (4.16) that $F_1 = \mathcal{k}(\{a_{ij}\}_{i,j})$ and $F_2 = \mathcal{k}(\{b_{ij}\}_{i,j})$. Thus F_1, F_2 are the quotient fields respectively of the rings

$$R_1 = \mathcal{k}[\{a_{ij}\}_{i,j}], \quad R_2 = \mathcal{k}[\{b_{ij}\}_{i,j}]$$

The mapping $\sigma: R_1 \to D$ defined by $\sigma(r) = xrx^{-1}$ is clearly a well-defined monomorphism, for which (by (4.23.1)) $\sigma(a_{ij}) = b_{ij}$ for each i,j. Thus $\sigma(R_1) = R_2$ and σ is thus an isomorphism of R_1 onto R_2. By the universal property of quotient fields, it follows that σ extends in the natural way to an isomorphism $F_1 \to F_2$ of the respective quotient fields of R_1, R_2.

Maximal k-arcs and representations of uniform matroids

For any integer $k \geq r$, a k-arc in PG(r,q) is a set of k (distinct) points such that no r lie in a subspace of dimension r-2 . An important problem in the theory of finite projective spaces is to determine the maximum value of k for which there exist k-arcs in PG(r,q). This number is denoted by m(r,q) (or m(r-1,q) by those authors who refer to PG(r,q) as PG(r-1,q)) and the reader is referred to [7,13,18,19,26,27,31,32,33] for some of the extensive work which has gone into determining this number for various values of r and q ; in general only the values m(i,q) and m(q-i+2,q) for i=2,3,4,5 appear to have been satisfactorily solved.

We approach this problem from an entirely different viewpoint. It is easily seen that uniform matroids are representable over any sufficiently large field, so the relevant representation problem in this case is to determine the smallest field over which $U_{r,n}$ is representable. We will show that this problem is essentially equivalent to determining the value m(r,q) (for various q) and consequently show how considerable simplifications (of the projective geometry) can be achieved by using straightforward matroid arguments.

The result which links the two different approaches is :-

(4.26) Proposition The matroid $U_{r,n}$ is representable over $GF(q)$ if and only if $n \leq m(r,q)$.

Proof For any integer $k \geq r$ a set of k points in $PG(r,q)$ form a k-arc if and only if no r of the points lie in a subspace of dimension $(r-2)$, that is, if and only if any r of the points form an independent set in $PG(r,q)$. But $U_{r,k}$ is representable over $GF(q)$ if and only if there are k points in $PG(r,q)$ for which any subset of r points is independent, that is, if and only if there is a k-arc in $PG(r,q)$. The result now follows if we note that $U_{r,n}$ is representable over $GF(q)$ implies $U_{r,k}$ is representable over $GF(q)$ for each integer $k<n$.

Before examining this correspondence any further, we note that for $r \geq 2$ and $n \geq r+2$ an F-representation of $U_{r,n}$ in p.c.f. will be of the form

$$\left[\begin{array}{cccc} & I_r & & \\ \hline 1 & 1 & \cdots & 1 \\ 1 & a_{11} & \cdots & a_{1,r-1} \\ \vdots & & & \\ 1 & a_{s,1} & \cdots & a_{s,r-1} \end{array}\right] \qquad (4.26.1)$$

where $s=n-r-1$, $a_{ij} \neq 0,1$ for each i,j. Moreover, for each $i=1,\ldots,s$ the elements $a_{i1},\ldots,a_{ir-1}$ are all distinct , and for each $j=1,\ldots,r-1$ the elements $a_{1j},\ldots,a_{sj}$ are all distinct. We also note that when $r=1$, $n=r$, or $n=r+1$, it follows from (4.26.1) that $U_{r,n}$ is regular, so we shall ignore these trivial cases henceforth .

(4.27) Lemma If $q \leq r$, then $m(r,q) = r+1$

Proof Since $U_{r,r+1}$ is representable over every field, we have by (4.26) that $r+1 \leq m(r,q)$. Suppose that $r+2 \leq m(r,q)$. Then by (4.26) $U_{r,r+2}$ is representable over GF(q). Because of (4.26.1) any representation of $U_{r,r+2}$ over GF(q) will have p.c.f.

$$\left[\begin{array}{cccc} & I_r & & \\ \hline 1 & 1 & \cdots & 1 \\ 1 & a_1 & \cdots & a_{r-1} \end{array}\right]$$

where $1, a_1, \ldots, a_{r-1}$ are distinct non-zero elements of GF(q). But then $q \geq r+1$, a contradiction, so we must have $m(r,q) = r+1$.

In the light of the above result we shall always assume that $q>r$ in PG(r,q).

(4.28) Lemma For any $r \geq 2$ and q (a prime power),

1) $m(r,q) \leq m(r-1,q) + 1$

2) $m(2,q) = q+1$

3) $q+1 \leq m(r,q) \leq q+r-1$

Proof

1) Suppose $m(r,q) \geq m(r-1,q) + 2$. Then by (4.26), $U_{r,m(r-1,q)+2}$ is representable over GF(q). By contracting and deleting respectively two distinct elements ot this matroid, we deduce by (1.33) that $U_{r-1,m(r-1,q)+1}$ is representable over GF(q), and hence by (4.26) $m(r-1,q) \geq m(r-1,q) + 1$ which is absurd.

2) (and we prove 3) at the same time)

Write $GF(q) = \{0, a_1, \ldots, a_{q-1}\}$. Consider the $q+1 \times r$ matrix

$$A = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ 1 & a_1 & \cdots & a_1^{r-2} & a_1^{r-1} \\ \vdots & & & & \\ 1 & a_{q-1} & & a_{q-1}^{r-2} & a_{q-1}^{r-1} \end{bmatrix}$$

over GF(q). By a consideration of the well known Vandermonde determinant, the fact that the a_i's are distinct non-zero elements of GF(q) implies that each $(r\times r)$ subdeterminant of A is non-zero. Thus A is a representation for $U_{r,q+1}$ over GF(q). By (4.26) we deduce

$$q+1 \leq m(r,q) \qquad \text{for each } r\geq 2 \qquad (4.28.4)$$

In particular it follows that $q+1 \leq m(2,q)$. Write $m = m(2,q)$. Then by (4.26) $U_{2,m}$ is representable over GF(q) in which case (because of (4.26.1)) a representation in p.c.f. has the form

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & b_1 \\ \vdots & \vdots \\ 1 & b_{m-3} \end{bmatrix}$$

where $1, b_1, \ldots, b_{m-3}$ are $(m-2)$ distinct non-zero elements of GF(q). Thus $q \geq m-1$, and so $m(2,q) = q+1$, proving 2).

By iteration of 1), we get

$$m(r,q) \leq m(2,q) + r - 2 = q + r - 1$$

which, together with (4.28.4) proves 3).

Next we present a much shorter and elementary proof of a result originally proved in [7] and [26] and which can be found in [18].

(4.29) Theorem For any prime power q,

$$m(3,q) = \begin{cases} q+1 & (q \text{ odd}) \\ q+2 & (q \text{ even}) \end{cases}$$

Proof For q even it suffices, by (4.26) and (4.28.2) to prove that $U_{3,q+2}$ is representable over GF(q). With GF(q) listed as above, consider the $(q+2)\times 3$ matrix

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & a_1 & a_1^2 \\ \vdots & & \\ 1 & a_{q-1} & a_{q-1}^2 \end{bmatrix}$$

over GF(q). The ,only (3×3) subdeterminants of A which are not of the Vandermonde type are those of the form

$$\begin{vmatrix} 0 & 1 & 0 \\ 1 & a_i & a_i^2 \\ 1 & a_j & a_j^2 \end{vmatrix} = a_j^2 - a_i^2 \qquad (1 \leq i, j \leq q-1)$$

Since q is even, $a_j^2 - a_i^2 = (a_j - a_i)^2 \neq 0$. Thus A is a representation of $U_{3,q+2}$ over GF(q) as required.

For q odd it suffices to prove that $U_{3,q+2}$ is not representable over GF(q). Suppose it were, then by (4.26.1) there would be a representation of the form

$$A' = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & a_1 & \sigma(a_1) \\ \vdots & & \vdots \\ 1 & a_{q-1} & \sigma(a_{q-1}) \end{bmatrix}$$

where σ is a permutation of $GF(q)^+$ $(= GF(q)\backslash\{0\})$. An elementary result from group theory states that in a finite abelian group G, if there is exactly one element, say a, of order 2 then the product of all the elements of G is equal to a. Consequently in the multiplicative group $GF(q)^+$, we have the relations (amounting to the well known 'generalised' Wilson Theorem) :-

$$\Pi x = -1 \quad \text{and} \quad \Pi\sigma(x) = -1 \quad (\text{products over all } x \in GF(q)^+)$$

Consider now the function $f : GF(q)^+ \to GF(q)^+$ defined by $f(x) = x^{-1}\sigma(x)$. This function is not surjective (i.e. a permutation of $GF(q)^+$) for if it were we would have

$$-1 = \Pi f(x) = \Pi x^{-1}\sigma(x) = (\Pi x^{-1})(\Pi\sigma(x)) = (\Pi x)^{-1}(\Pi\sigma(x)) = 1$$

(all products over all $x \in GF(q)^{+}$)

This is a contradiction since q is odd.

Thus for some $i \neq j$, we must have $a_i^{-1}\sigma(a_i) = a_j^{-1}\sigma(a_j)$.

But then

$$\begin{vmatrix} 1 & 0 & 0 \\ 1 & a_i & (a_i) \\ 1 & a_j & (a_j) \end{vmatrix} = a_i\sigma(a_j) - a_j\sigma(a_j) = 0$$

which contradicts the fact that A' is a representation of $U_{3,q+2}$.

Results in [10,24,27] yield the important results that for any prime power q,

$$m(4,q) = m(5,q) = q+1$$

From $m(5,q) = q+1$, we deduce now from (4.28.3), that for $r \geq 5$, $q>r$,

$$q+1 \leq m(r,q) \leq q+r-4$$

At present these are the best known bounds in general for $m(r,q)$, since for $11 \leq q < 225$ it is not known whether $m(r,q) = q+2$ or $q+1$. In 1970 Hirschfeld conjectured that $m(r,q) = q+1$ for any odd prime power q and $r \leq q$. In matroid terms (by (4.26)) this can now be restated as

Conjecture For any integers $r,n,q=p^s$ (p prime $\neq 2$), and $n-2 \geq r$.

T.F.A.E. (i) $U_{r,n}$ is representable over $GF(q)$

(ii) $n \leq q+1$

Finally we turn our attention to the determining of $m(q-j\ ,q)$ for $j=0,1,2,3$.

(4.30) Proposition If $m(r,q) = q+1$, then $m(q-r+2,q) = q+1$

Proof By (4.28.2) it suffices to prove that $m(q-r+2,q) \leq q+1$. Suppose not. Then $m(q-r+2,q) \geq q+2$ in which case $U_{q-r+2,q+2}$

is representable over GF(q). The dual matroid of $U_{q-r+2,q+2}$ is $U_{r,q+2}$, so by (1.32) this matroid is representable over GF(q), whence by (4.26), $m(r,q) \geq q+2$, a contradiction.

For q odd we have seen that $m(i,q) = q+1$ for $i=2,3,4;5$ hence by (4.30) we deduce that $m(q-j,q) = q+1$ for $j=0,1,2,3$ a result proved in [32]. Moreover, since $m(i,q) = q+1$ for $i=2,4,5$ and q even, we may deduce that $m(q-j,q) = q+1$ for $j=0,2,3$ and q even (a result which does not appear in [32]). Thas does prove however in [29] that with q even, $m(q-1,q) = q+2$, thus completing this 'dual' set of results. Again this result can be proved easily by dual matroids :-

(4.31) <u>Proposition</u> <u>For q even, $m(q-1,q) = q+2$</u>

<u>Proof</u> By (4.29), $m(3,q) = q+2$ for q even and so $U_{3,q+2}$ is representable over GF(q). As above this implies $U_{q-1,q+2}$ is representable over GF(q), and so $m(q-1,q) \geq q+2$.
If $m(q-1,q) \geq q+3$ then we must have $U_{q-1,q+3}$ representable over GF(q). Again taking duals this means that $U_{4,q+3}$ is representable over GF(q) and so $m(4,q) \geq q+3$, contradicting the fact that $m(4,q) = q+1$ for <u>any</u> q. The result now follows.

§5 VÁMOS RINGS

The algebra in this chapter will be of a slightly more specialised nature than any previously used and, although adequately covered in [2], we shall begin by listing some definitions and results for purposes of reference.

For any ideal $\underline{b}$ of a ring A, the radical of $\underline{b}$, denoted $\sqrt{\underline{b}}$ is defined by

$$\sqrt{\underline{b}} = \{a \in A \ ; \ a^m \in \underline{b} \ \text{ for some positive integer } m\}$$

The nilradical of A, denoted $N(A)$ is the ideal $\sqrt{0}$, that is, the collection of all nilpotent elements of A, or equivalently, the intersection of all prime ideals of A. The ring A is reduced if $N(A)=0$. In particular, for each ideal $\underline{b}$ of A, the ring $A/\sqrt{\underline{b}}$ is reduced. The Jacobson radical of A, denoted $J(A)$ is the intersection of all the maximal ideals of A. The ring A is called a Jacobson (or Hilbert) ring if every prime ideal of A is the intersection of a family of maximal ideals. Clearly $N(A) = J(A)$ if A is a Jacobson ring.

(5.1) Theorem Suppose A is finitely generated (as a $\mathbb{Z}$-algebra) Then

1) A is a Jacobson ring, and

2) For each $\underline{p} \in \operatorname{Spec} A$, $\underline{p}$ is maximal if and only if $A/\underline{p}$ is finite

Proof See [6] pp.352-354.

For each multiplicatively closed subset (m.c.s.) S of A, the ring of quotients of A with respect to S (see [2] pp.36-40) is denoted by A_S or $S^{-1}A$. This ring is zero if and only if

$0 \in S$. For any m.c.s. S, the mapping $\Phi: A \to A_S$ defined by $\Phi(a) = a/1$ for each $a \in A$, is called the natural homomorphism, and we have the following well known 'universal property of A_S'

(5.2) Proposition Suppose that $\Phi: A \to A_S$ is the natural homomorphism, and that $f: A \to A'$ is a ring homomorphism satisfying

1) $f(s)$ is a unit in A' for each $s \in S$

Then there is a unique homomorphism $\psi: A_S \to A'$ making the diagram I commute

$$\begin{tikzcd} A \arrow[r, "\Phi"] \arrow[d, "f"'] & A_S \arrow[dl, dashed, "\Psi"] \\ A' & \end{tikzcd} \qquad \text{(I)}$$

Moreover, if in addition, f satisfies

2) Whenever $f(a)=0$, then $sa = 0$ for some $s \in S$, and

3) Every element in A' may be written in the form $f(a)(f(s))^{-1}$ for some $a \in A$, $s \in S$

Then ψ is an isomorphism.

(5.3) If A is Noetherian, then $A[X_1,\ldots,X_n]$ is Noetherian and A_S is Noetherian for any m.c.s. S.

(5.4) If S is a m.c.s. and $\underline{b}$ is an ideal of A for which $\underline{b} \cap S = \phi$ then there is a prime ideal $\underline{p} \supset \underline{b}$ for which $\underline{p} \cap S = \phi$

As a final preliminary we note that for a non-nilpotent $x \in A$, the set $S = \{ x^m ;\ m \text{ an integer} \geq 0\}$ is a m.c.s. of A for which the ring A_S will usually be denoted by $A_{(x)}$.

For the remainder of this chapter, unless otherwise stated, M will denote a matroid of rank r on the set $E = \{e_1,\ldots,e_n\}$ where the ordering is fixed.

Let X be the generic $(n\times r)$ matrix of indeterminants $[X_{ij}]$ whose rows are indexed by the elements of E, and let $T = \mathbb{Z}[\{X_{ij}\}_{i,j}]$,the polynomial ring over $\mathbb{Z}$ in the nr indeterminates $\{X_{ij}\}_{i,j}$. For each r-set $U \subset E$, U is either a basis (independent) or a non-basis (dependent) in M, and $\det X(U)$ is a well-defined element of the ring T.

$$\text{Let} \quad a = \Pi\{\det X(U)\ ;\ U \text{ basis of } M\}$$

and let $\underline{b}$ be the ideal of T generated by the set of elements

$$\{\det X(U)\ ;\ U \text{ non-basis of } M\}$$

With these definitions Vámos has proved the following remarkable characterization of representability which inspired this study:-

(5.5) Theorem (Vámos, [35]) The matroid M is representable if and only if $a \notin \sqrt{\underline{b}}$.

Proof Suppose first that M is representable over some field F by the $(n\times r)$ matrix $N = [\alpha_{ij}]$. Let $\gamma: T \to F$ be the ring homomorphism induced by $\gamma(X_{ij}) = \alpha_{ij}$ for each $1\leq i\leq n$, $1\leq j\leq r$. For each r-set $U \subset E$, U is a non-basis if and only if $\det N(U) = 0$. But $\det N(U) = \gamma(\det X(U))$, so if U is a non-basis then $\gamma(\det X(U)) = 0$. Consequently $\underline{b} \subset \operatorname{Ker}\gamma$, and since $\operatorname{Ker}\gamma$ is a prime ideal with F a domain, it follows that $\sqrt{\underline{b}} \subset \operatorname{Ker}\gamma$.

$$\text{Now} \qquad \gamma(a) = \gamma(\Pi \det X(U)) = \Pi\gamma(\det X(U)) = \Pi\det N(U)$$

(where the products are over all the bases U of M)

Hence $\gamma(a) \neq 0$ since $\det N(U) \neq 0$ for each basis U . Thus $a \notin \operatorname{Ker}\gamma$ and so $a \notin \sqrt{\underline{b}}$ since $\sqrt{\underline{b}} \subset \operatorname{Ker}\gamma$.

Conversely suppose $a \notin \sqrt{\underline{b}}$. Then the set

$$S = \{a^t\ ;\ t \text{ integer} \geq 0\}$$

is a m.c.s. of T disjoint from $\underline{b}$. By (5.4) there is a prime ideal $\underline{p} \supset \underline{b}$ with $\underline{p} \cap S = \phi$. Let K be the quotient field of

$T/\underline{p}$, and let π be the composition map $T \xrightarrow{nat} T/\underline{p} \xrightarrow{inc} K$.
Let N be the $(n \times r)$ matrix $N = [\pi(X_{ij})]$ over K.

Then N is a K-representation of M. For suppose U is an r-subset of E. If U is dependent then $\det X(U) \in \underline{b} \subset \underline{p}$ so that $0 = \pi(\det X(U)) = \det N(U)$. If U is independent then $\det X(U)$ divides a. Consequently $\det X(U) \notin \underline{p}$ for otherwise $a \in \underline{p}$ which contradicts the choice of $\underline{p}$. But then
$\det N(U) = \pi(\det X(U)) \neq 0$.

Suppose now that $\bar{\ } : T \longrightarrow T/\sqrt{\underline{b}}$ denotes the canonical homomorphism . Then the set $\bar{S} = \{\bar{a}^m \ ; \ m \geq 0\}$ is a m.c.s. of $T/\sqrt{\underline{b}}$

(5.6) Definition The Vámos ring of the matroid M is the ring

$$A_M = (T/\sqrt{\underline{b}})_{(\bar{a})} \qquad (= (T/\sqrt{\underline{b}})_{\bar{S}} \ )$$

Although A_M has been defined with respect to a fixed ordering of E, it is clear that if σ is any permutation of $\{1,\dots,n\}$ then the Vámos ring A'_M defined with respect to the ordering $e_{\sigma(1)},\dots,e_{\sigma(n)}$ is isomorphic to A_M (if $[Y_{ij}]$ is the generic matrix of indeterminates used to define A'_M then the mapping $Y_{ij} \longrightarrow X_{\sigma(i)j}$ induces an isomorphism between A'_M and A_M).

(5.7) Proposition

1) $A_M = (0)$ if and only if M is representable.

2) A_M is a Noetherian ring.

Proof 1) The ring $A_M = (0)$ if and only if $\bar{0} \in \bar{S}$, that is, if and only if $a^m \in \underline{b}$ for some positive integer m. This is true if and only if $a \in \sqrt{\underline{b}}$, so the result follows from (5.5).

2) Follows from the results in (5.3) since $\mathbb{Z}$ is Noetherian.

Let $\theta: T \longrightarrow A_M$ denote the composition map $T \longrightarrow T/\sqrt{\underline{b}} \xrightarrow{\Phi} A_M$ where Φ is the natural homomorphism defined previously. Write $\theta(X_{ij}) = x_{ij}$ and let $\mathcal{X}$ denote the $(n \times r)$ matrix $[x_{ij}]$ over A_M. Also, if $N = [\alpha_{ij}]$ is an F-representation of M, write g^N for the homomorphism $g^N: T \to F$ induced by $g^N(X_{ij}) = \alpha_{ij}$.

(5.8) Proposition *With the above definitions, the ring A_M, together with the matrix $\mathcal{X}$ satisfies :-*

1) *A_M is a reduced ring.*

2) *Every $(r \times r)$ subdeterminant of $\mathcal{X}$ is either zero or a unit in A_M and A_M is finitely generated as a $\mathbb{Z}$-algebra by the x_{ij}'s together with the inverses of these subdeterminants.*

3) *For any field F and $(n \times r)$ matrix $N = [\alpha_{ij}]$ which is an F-representation of M, there is a unique homomorphism $f: A_M \to F$ making the diagram below commute.*

$$\begin{tikzcd} T \arrow[r, "\theta"] \arrow[d, "g^N"'] & A_M \arrow[dl, dashed, "f"] \\ F & \end{tikzcd}$$

4) *For any homomorphism $f: A_M \to F$ (F a field), there is a unique F-representation N which makes the above diagram commute.*

Proof

1) We have already noted that $T/\sqrt{\underline{b}}$ is reduced, and any ring of quotients of a reduced ring is again reduced.

2) Let U be any r-subset of E. If U is a non-basis then $\det X(U) \in \underline{b}$, whence $\theta(\det X(U)) = 0$ in A_M. If U is a basis then $\det X(U)$ divides a whence $\theta(\det X(U))$ divides $\theta(a)$; now by definition of A_M, $\theta(a)$ is a unit in A_M, hence $\theta(\det X(U))$ is a unit in A_M. The first statement now follows since every

$(r\times r)$ subdeterminant of $\mathcal{X}$ has the form $\det\mathcal{X}(U) = \theta(\det X(U))$ for some r-set $U \subset E$. The second statement follows from the fact that

$$\theta(a)^{-1} = \Pi(\theta(\det X(U))^{-1} = \Pi(\det\mathcal{X}(U))^{-1}$$

(where products are over the set of bases U of M)

since every element in A_M has the form $\bar{h}/\theta(\bar{a})^m$ where $h \in T$.

3) By (5.2) and the definition of θ, it suffices to show that $\sqrt{\underline{b}} \subset \operatorname{Ker} g^N$ (so g^N 'factors' through $T/\sqrt{\underline{b}}$) and that $g^N(a)$ is a unit (i.e. is non-zero) in F.

For any r-set $U \subset E$, $g^N(\det X(U)) = \det N(U)$ which is zero if and only if U is a non-basis. So clearly $\underline{b} \subset \operatorname{Ker} g^N$, and since the latter is a prime ideal and F a domain we deduce that $\sqrt{\underline{b}} \subset \operatorname{Ker} g^N$. Also $g^N(a) = g^N(\Pi\det X(U)) = \Pi\det N(U) \neq 0$ (products over all bases U), so $g^N(a)$ is indeed a unit.

4) Suppose $f(x_{ij}) = \alpha_{ij} \in F$ for each $1\leq i\leq n$, $1\leq j\leq r$. Let N be the $(n\times r)$ matrix $[\alpha_{ij}]$ over F. We have only to show that N is an F-representation of M. For any r-set $U \subset E$, $\det N(U) = f(\det\mathcal{X}(U))$, and by 2) $\det\mathcal{X}(U)$ is zero in A_M if U is a non-basis and is a unit if U is a basis. Hence $\det N(U) = f(0) = 0$ if U is a non-basis and $\det N(U) \neq 0$ if U is a basis since any ring homomorphism into a field maps units onto units (i.e. non-zero elements of F).

In (5.15) we will show that the four properties listed in (5.8) characterize the ring A_M

(5.9) <u>Corollary and definition</u> <u>To each $\underline{p} \in \operatorname{Spec} A_M$ there corresponds a representation $N_{\underline{p}}=[\pi(x_{ij})]$ of M over $K_{\underline{p}}$ the quotient field of $A_M/\underline{p}$ (where π is the composite map $A_M \longrightarrow A_M/\underline{p} \longrightarrow K_{\underline{p}}$). Conversely, to each F-representation $N = [\alpha_{ij}]$ of M, there</u>

corresponds a ring homomorphism $f_N : A_M \longrightarrow F$ in which $f(x_{ij}) = \alpha_{ij}$, and hence a corresponding prime ideal p_N of A_M, where $p_N = \text{Ker } f_N$.

The natural correspondence given above between the prime ideals of A_M and the representations of M is not in general a bijection. The most important by-product of our later refinement of A_M will be that this correspondence does become a bijection.

(5.10) Proposition The ring A_M is a Jacobson ring for which $A_M/\underline{m}$ is a finite field for each maximal ideal $\underline{m}$ of A_M.

Proof By (5.8.2), A_M is finitely generated as a $\mathbb{Z}$-algebra, so the result follows from (5.1).

(5.11) Corollary (Rado) If M is representable, then it is representable over a finite field.

Proof By (5.7.1) $A_M \neq (0)$. Consequently A_M possesses a maximal ideal $\underline{m}$, say. By (5.10), $A_M/\underline{m}$ is a finite field, so by virtue of the canonical homomorphism $A_M \longrightarrow A_M/\underline{m}$, it follows from (5.8.4) (or (5.9)) that M is representable over $A_M/\underline{m}$.

(5.12) Lemma Suppose M is representable (so $A_M \neq (0)$), and for each $n \in \mathbb{Z}$, let $\tilde{n}$ denote the image of n in A_M under Φ. Then

1) For every non-zero element $x \in A_M$ there is a maximal ideal $\underline{m}$ of A_M with $x \notin \underline{m}$.

2) If $n = p_1^{m_1} \cdots p_t^{m_t}$ where $p_1, \ldots, p_t$ are distinct prime numbers, then $\tilde{n} = 0$ if and only if $c(M) \subset \{p_1, \ldots, p_t\}$. In particular, for any prime p, $\tilde{p} = 0$ if and only if $c(M) = \{p\}$.

3) For any prime p, $\tilde{p}$ is a non-unit in A_M if and only if $p \in c(M)$.

Proof

1) By (5.8.1) A_M is a reduced ring so $N(A_M) = 0$. But A_M is a Jacobson ring, whence $J(A_M) = N(A_M) = 0$. Thus $x \neq 0$ implies $x \notin \cap\{\underline{m}\ ;\ \underline{m}$ maximal ideal of $A_M\}$ and the result follows.

2) First suppose $\tilde{n} = 0$. Let F be any field over which M is representable. Then by (5.8.3) there is a homomorphism $f: A_M \rightarrow F$. Thus,

$$0 = f(0) = f(\tilde{n}) = f(n.\tilde{1}) = n.1_F$$

so char F divides n. But then char $F = p_i$ for some $1 \leq i \leq t$ and hence $c(M) \subset \{p_1, \ldots, p_t\}$.

Conversely, suppose $c(M) \subset \{p_1, \ldots, p_t\}$ but that $\tilde{n} \neq 0$. By 1) there is a maximal ideal $\underline{m}$ of A_M for which $\tilde{n} \notin \underline{m}$. Consider the field $F = A_M/\underline{m}$ and the canonical homomorphism $\pi: A_M \rightarrow F$. By (5.8.4), M is representable over F. But $n.1_F = \pi(\tilde{n}) \neq 0$, and consequently char $F \neq p_i$ for each $i=1,\ldots,t$ which contradicts $c(M) \subset \{p_1, \ldots, p_t\}$.

The second statement now follows from (5.7.2) and (5.11).

3) Suppose $\tilde{p}$ is a non-unit in A_M. Then $\tilde{p}$ is contained in a maximal ideal $\underline{m}$ of A_M so that the field $A_M/\underline{m}$ must have characteristic p. By (5.8.4), M is representable over $A_M/\underline{m}$, so $p \in c(M)$. Conversely suppose $p \in c(M)$. Then by (5.8.3) there is a field F of characteristic p and a homomorphism $f: A_M \rightarrow F$. Since $f(\tilde{p}) = p.1_F = 0$, $\tilde{p}$ cannot be a unit in A_M.

(5.13) Theorem (Rado and Vámos) For a matroid M, $|c(M)| = \infty$ if and only if $0 \in c(M)$.

Proof First suppose $|c(M)| = \infty$. Then since every integer $m \neq 0$ has a prime factor decomposition, it follows from (5.12.2) that $\tilde{m} \neq 0$. Consequently the set $W = \{\tilde{m}\ ;\ 0 \neq m \in Z\}$ is a m.c.s. of A_M which is disjoint from the zero ideal (0). By (5.4) there is a prime ideal $\underline{q}$ of A_M with $\underline{q} \cap W = \phi$. Let K be the quotient field of $A_M/\underline{q}$, so that by (5.9) M is representable over K. By definition of $\underline{q}$, $m.1_K \neq 0$ for each $0 \neq m \in Z$ hence char K = 0 which proves necessity.

Conversely, suppose $0 \in c(M)$. By (5.11), M is representable over a finite field so c(M) contains at least one prime $p \neq 0$. Suppose that $c(M)\backslash\{0\}$ consists only of a finite number of primes $p_1,\ldots,p_t$ and seek a contradiction. If we write $n = \prod_{i=1}^{t} p_i$, then by (5.12.2) $\tilde{n} \neq 0$, since $0 \notin \{p_1,\ldots,p_t\}$. By (5.12.1), there is a maximal ideal $\underline{m}$ of A_M with $\tilde{n} \notin \underline{m}$. As in the proof of (5.12.2), M is representable over the field $F = A_M/\underline{m}$ which is finite (by (5.10)), hence having characteristic p', say with $p' \neq 0$. This means that $p' = p_i$ for some $1 \leq i \leq t$ in which case $p_i.1_F = 0$, and hence $\tilde{n} \in \underline{m}$, a contradiction.

(5.14) Corollary Suppose M is representable and A_M a domain. Then $|c(M)| = 1$ or $|c(M)| = \infty$

Proof By (5.7.1), $|c(M)| \geq 1$. Suppose that $2 \leq |c(M)| < \infty$ and seek a contradiction. By (5.13) $0 \notin c(M)$, so $c(M) = \{p_1,\ldots,p_t\}$ for some distinct primes $p_1,\ldots,p_t$. Since $t \geq 2$, the second statement of (5.12.2) implies $\tilde{p}_i \neq 0$ for each $i=1,\ldots,t$, whereas by the first statement $\prod_{i=1}^{t} \tilde{p}_i = 0$ in A_M . This contradicts the fact that A_M is a domain.

(5.15) Theorem (universal property) Let S be a ring and $Y = [y_{ij}]$ an (nxr) matrix over S, such that the 'pair' (S,Y) satisfy the following conditions :-

1) S is a reduced ring
2) Every (rxr) subdeterminant of Y is either zero or a unit in

S, and S is finitely generated as a $\mathbb{Z}$-algebra by the y_{ij}'s together with the inverses of these units.

3) For any field F and $(n \times r)$ matrix $N = [\alpha_{ij}]$ which is an F-representation of M, there is a unique homomorphism $h : S \longrightarrow F$ making the diagram below commute.

$$\begin{tikzcd} T \arrow[r, "\partial"] \arrow[d, "g^N"'] & S \arrow[dl, dashed, "h"] \\ F & \end{tikzcd}$$

(where ∂ is induced by $\partial(x_{ij}) = y_{ij}$)

4) For any homomorphism $h: S \to F$ (F a field), there is a unique F-representation N of M making the above diagram commute.

Then the rings A_M and S are isomorphic, under an isomorphism taking x_{ij} to y_{ij}.

Proof We first note that $S = (0)$ if and only if M is not representable ; for if $S \neq (0)$ then S contains a maximal ideal $\underline{m}$, and because of the canonical homomorphism $S \dashrightarrow S/\underline{m}$, it follows from 4) that M is representable over $S/\underline{m}$. Conversely, if M is, say F-representable then the existence of a homomorphism of S into F (by 3)) ensures that $S \neq (0)$ (since, by our definition of homomorphism, $h(1) = 1_F$). Thus by (5.7.1) we deduce that $A_M = (0)$ if and only if $S = (0)$, and we may now assume that both rings are non-zero.

So let $\pi: S \dashrightarrow S/\underline{m}$ denote the canonical homomorphism where $\underline{m}$ is a maximal ideal of S. By 4) the matrix $N = [\pi(y_{ij})]$ is a representation of M over $S/\underline{m}$. Let U be an r-subset of E, so then $\det N(U) = 0$ if and only if U is dependent. But $\pi(\det Y(U)) = \det N(U)$, so $\det Y(U) \in \underline{m}$ if and only if U is dependent. Since, by 2), $\det Y(U)$ is either 0 or a unit (the latter of which is not contained in any maximal ideal) we deduce,

$$\det Y(U) = 0 \text{ if and only if } U \text{ is dependent in } M \qquad (5.15,5)$$

Next we appeal to (5.2.1) to show that the homomorphism $\partial: T \to S$ induces the required homomorphism $\bar{\partial}: A_M \to S$, and for this we must show show that $\sqrt{\underline{b}} \subset \operatorname{Ker} \partial$ and $\partial(a)$ is a unit in S. Clearly $\partial(\det X(U)) = \det Y(U)$ for each r-set $U \subset E$, so by (5.15.5), $\underline{b} \subset \operatorname{Ker} \partial$. By 1) S is a reduced ring, hence we deduce $\sqrt{\underline{b}} \subset \operatorname{Ker} \partial$. Also, $\partial(a) = \Pi\{\det Y(U);\ U \text{ basis}\}$, which, by (5.15.5) and 2) is a product of units in S, hence is itself a unit in S. Thus, by (5.2.1) there is a (unique) homomorphism $\bar{\partial}: A_M \to S$ in which $\bar{\partial}(x_{ij}) = y_{ij}$. We have only to show that $\bar{\partial}$ is a bijection:-

<u>$\bar{\partial}$ surjective</u> :- By 2) and (5.15.5), S is generated (as a $\mathbb{Z}$-algebra) by the y_{ij}'s together with those elements of the form $(\det Y(U))^{-1}$ where U is a basis of M. By (5.8.2), $\det \mathcal{X}(U)$ is a unit in A_M, and since $\bar{\partial}(\det \mathcal{X}(U)) = \det Y(U)$ we also have $\bar{\partial}(\det \mathcal{X}(U)^{-1}) = (\det Y(U))^{-1}$, hence $\bar{\partial}$ is surjective.

<u>$\bar{\partial}$ injective</u> :- We need only show that $\bar{\partial}(x) = 0$ implies $x = 0$ for each $x \in A_M$. Suppose not, and $\bar{\partial}(x) = 0$ for some $x \neq 0$. By (5.12.1) there is a maximal ideal $\underline{m}'$ of A_M for which $x \notin \underline{m}'$. Let $\pi': A_M \to A_M/\underline{m}'$ denote the canonical homomorphism and the matrix $N = [\pi'(x_{ij})]$. Then by (5.8.3) and 3) there is a (unique) homomorphism $h: S \to A_M/\underline{m}'$ which makes the diagram below commute.

$$\begin{tikzcd}
T \arrow[r, "\theta"] \arrow[dr, "g^N"'] & A_M \arrow[r, "\bar{\partial}"] \arrow[d, "\pi'"] & S \arrow[dl, dashed, "h"] \\
 & A_M/\underline{m}' &
\end{tikzcd}$$

But then $\pi' = h\bar{\partial}$. Hence $\pi'(x) = h\bar{\partial}(x) = h(0) = 0$, in which case $x \in \underline{m}'$, a contradiction. The result now follows.

(5.16) Remark In the light of (5.8) and (5.15) we can view the ring A_M as any pair (S,Y) where S is a ring and Y is an $(n \times r)$ matrix over S satisfying the conditions of (5.15). In particular, of course $(A_M, \mathcal{X})$ is such a pair.

The simplified Vámos ring

The ring A_M is based on too many indeterminates for practical use, since even for the simplest matroids M, A_M cannot easily be explicitly described. When we eventually define the canonical Vámos ring we will have reduced the number of indeterminates sufficiently to be able to compute the ring easily for many important matroids. However, since we wish to establish the precise algebraic relationship between these rings it is necessary to define the intermediate ring R_M , which we will call the simplified Vámos ring, and which is of genuine interest in its own right.

Once again we shall assume the same fixed ordering of E, but in this case we assume in addition that the first r elements $e_1, \dots, e_r$ form a basis B. In §2 we noted that a representation matrix of M is in column echelon form if and only if the first r rows form the identity matrix I_r , and that every matrix is column equivalent to a matrix in column echelon form. With this consideration we define R_M in an exactly analagous way to A_M, except that now the definitions of T, $\underline{b}$, a are made with respect to the matrix

$$X = \left[\frac{I_r}{X'}\right] \qquad \text{where} \quad X' = \begin{bmatrix} X_{r+1,1} & \cdots & X_{r+1,r} \\ \vdots & & \\ X_{n,1} & \cdots & X_{n,r} \end{bmatrix}$$

instead of the previous matrix of nr indeterminates. To emphasize the analagy we are using the same labels X, T, $\underline{b}$, a ,as before, but now $T = Z[\{X_{ij}\}_{\substack{r+1\leq i\leq n \\ 1\leq j\leq r}}]$, $\underline{b}$ is the ideal in T generated by the elements $\{\det X(U);\ U \text{ non-basis}\}$, $a = \Pi\{\det X(U);\ U \text{ basis}\}$, and $R_M = (T/\sqrt{\underline{b}})_{(\bar{a})}$.

Unlike A_M it is by no means obvious that the ring R_M is independent of the ordering of E (in the sense that if we define the ring with respect to some other ordering the resulting ring is isomorphic to R_M). There is no problem if we merely permute the elements of B among themselves or the elements of $E\backslash B$ among themselves since these operations correspond (respectively) to permutations of the columns and rows of X' and the resulting ring is then isomorphic to R_M under the mapping induced by the corresponding permutation of the X_{ij}'s. However things are much more difficult in the case of an arbitrary permutation of E since this may result in defining the ring with respect to a basis different to B. We defer the proof of the isomorphism in this case until we have established the basic properties of R_M.

As before let $\theta: T\to R_M$ denote the natural mapping. Write $\theta(X_{ij}) = x_{ij}$ and the matrices $\mathcal{X}' = [x_{ij}]_{\substack{r+1\leq i\leq n \\ 1\leq j\leq r}}$ and $\mathcal{X} = [I_r|\mathcal{X}']^T$. One elementary but useful property which now is possessed by $(R_M, \mathcal{X})$ is :-

(5.17) <u>Proposition</u> <u>For each $r+1\leq i\leq n$, $1\leq j\leq r$,</u>

1) <u>x_{ij} is (up to sign) an $(r\times r)$ subdeterminant of $\mathcal{X}$.</u>

2) <u>$x_{ij} = 0$ in R_M if and only if $e_j \notin C(B,e_i)$ and is a unit otherwise. Thus the matrix $\mathcal{X}'$ over R_M has its zero entries in the same corresponding positions to the matrix A_B .</u>

<u>Proof</u> 1) Write $U_{ij} = B\backslash\{e_j\} \cup \{e_i\}$. Then $\det(U_{ij}) = \pm x_{ij}$.

2) With U_{ij} as above, $\det X(U_{ij}) = \pm X_{ij}$. Thus $X_{ij} \in \underline{b}$ if and only if U_{ij} is a non-basis, and X_{ij} divides a if and only if U_{ij} is a basis. But then $x_{ij} = 0$ in R_M if and only if U_{ij} is a non-basis, and x_{ij} is a unit if and only if U_{ij} is a basis. The result now follows since U_{ij} is a non-basis if and only if it contains a circuit which must be $C(B,e_i)$.

The following set of results (5.7)′,(5.8)′,(5.9)′,(5.10)′, (5.15)′ for R_M are analagous results to those corresponding to A_M. In each case the new proof requires such minor modifications as to make their statement here unnecessary.

(5.7)′ 1) $R_M = (0)$ if and only if M is not representable.

2) R_M is a Noetherian ring.

(5.8)′ The ring R_M, together with the matrix $\mathcal{X}$ satisfies:-

1) R_M is a reduced ring.

2) Every $(r \times r)$ subdeterminant of $\mathcal{X}$ is either zero or a unit in R_M, and R_M is finitely generated (as a Z-algebra) by these units together with their inverses.

3) For any field F, and $(n \times r)$ column echelon matrix $N = [I_r | N']^T$ which is an F-representation of M, there is a unique homomorphism $f: R_M \to F$ making the diagram below commute.

$$\begin{tikzcd} T \arrow[r, "\theta"] \arrow[d, "\varepsilon^N"'] & R_M \arrow[dl, dashed, "f"] \\ F & \end{tikzcd}$$

4) For any homomorphism $f: R_M \to F$ (F a field) there is a unique column echelon F-representation N which makes the above diagram commute.

(Note:- (5.8.2)′ is stronger than (5.8.2) thanks to (5.17.1)).

(5.9)′ To each $p \in \operatorname{Spec} R_M$ there corresponds a column echelon representation $N_p = [I_r | \pi(x_{ij})]^T$ of M over K_p the quotient field of R_M/p (where π is the composite map $R_M \to R_M/p \to K_p$). Conversely, to each column echelon F-representation $N = [I_r | N']^T$ (where $N' = [\alpha_{ij}]_{\substack{r+1 \leq i \leq n \\ 1 \leq j \leq r}}$) of M there corresponds a homomorphism $f_N : R_M \to F$ in which $f_N(x_{ij}) = \alpha_{ij}$ (for each i, j), and hence a corresponding prime ideal p_N of R_M , where $p_N = \operatorname{Ker} f_N$.

(5.10)′ The ring R_M is a Jacobson ring for which $R_M/\underline{m}$ is a finite field for each maximal ideal $\underline{m}$ of R_M.

(5.15)′ (universal property) Let S be a ring and $Y = [I_r | Y']^T$ an $(n \times r)$ matrix over S (where $Y' = [y_{ij}]_{\substack{r+1 \leq i \leq n \\ 1 \leq j \leq r}}$, say) such that the pair (S,Y) satisfy the conditions :-

1) S is a reduced ring.

2) Every $(r \times r)$ subdeterminant of Y is either zero or a unit in S and S is finitely generated (as a $\mathbb{Z}$-algebra) by these units together with their inverses.

3) For any field F, and $(n \times r)$ column echelon matrix $N = [I_r | N']^T$ which is an F-representation of M, there is a unique homomorph-ism h which makes the diagram below commute.

$$\begin{tikzcd} T \arrow[r, "\partial"] \arrow[d, "g_N"'] & S \arrow[dl, dashed, "h"] \\ F & \end{tikzcd}$$

(where ∂ is induced by $\partial(X_{ij}) = y_{ij}$)

4) For any homomorphism $h: S \to F$ (F a field) , there is a unique column echelon F-representation of M which makes the above diagram commute.

Then the rings R_M and S are isomorphic under an isomorphism taking x_{ij} to y_{ij}.

(5.18) Theorem The ring R_M is (up to isomorphism) independent of the ordering of E.

Proof Let $(R_M, \mathfrak{X})$ be defined as above, with respect to the ordering $e_1, \ldots, e_n$ where $B = \{e_1, \ldots, e_r\}$ is a basis. Now let R' $(=R'_M)$ be the simplified Vamos ring defined with respect to some new ordering $e_{\sigma(1)}, \ldots, e_{\sigma(n)}$ where σ is a permutation of $(1, \ldots, n)$. We may assume $B' = \{e_{\sigma(1)}, \ldots, e_{\sigma(n)}\}$ is a basis. By (1.22) (basis exchange) it suffices to prove the theorem in the case when B, B' differ by only one element, so by our previous comments, we may assume that $B' = \{e_1, \ldots, e_{r-1}, e_{r+1}\}$ and that R' is defined with respect to the ordering $e_1, \ldots, e_{r-1}, e_{r+1}, e_r, e_{r+2}, \ldots, e_n$.

Now suppose that R' is defined with respect to the generic (column echelon) matrix of indeterminates Y_0 where

$$Y_0 = \begin{array}{c} e_1 \\ \vdots \\ e_{r-1} \\ e_{r+1} \\ e_r \\ \vdots \\ e_n \end{array} \left[\begin{array}{ccc} & I_r & \\ \hline Y_{r+1,1} & \cdots & Y_{r+1,r} \\ \vdots & & \\ Y_{n,1} & \cdots & Y_{n,r} \end{array} \right]$$

Let y_{ij} denote the natural image of Y_{ij} in R' and let $Y = [I_r | Y']^T$ where $Y' = [y_{ij}]$. Since $(5.8)'$ is true for any simplified Vámos ring defined on a fixed ordering, it is certainly true for (R', Y) with respect to the new ordering of E. Also, we note that

$$e_{r+1} \in C(B', e_r) \qquad (5.18.2)$$

for otherwise $C(B', e_r) \subset \{e_1, \ldots, e_{r-1}\} \cup \{e_r\} = B$, which is a contradiction. So by (5.17) applied to (R', Y) it follows that $y_{r+1,r}$ is a unit in R'. Write $(y_{r+1,r})^{-1} = z$, say.

We now define a new matrix Y_1 over R' which is the matrix resulting when we interchange the r^{th} and $(r+1)^{th}$ rows of Y and reduce this matrix to column echelon form. Explicitly.:-

$$Y_1 = P_{r,r+1}\, Y \begin{bmatrix} 1 & 0 & & 0 & 0 \\ 0 & 1 & & 0 & 1 \\ \vdots & & & & \\ 0 & 0 & & 1 & 0 \\ -(y_{r+1,1})z & -(y_{r+1,2})z & \cdots & -(y_{r+1,r-1})z & z \end{bmatrix} \qquad (5.18.2)$$

(where $P_{r,r+1}$ is the $(n\times n)$ permutation matrix obtained from I_n by interchanging the r^{th} and $(r+1)^{th}$ rows).

Thus Y_1 is an $(n\times r)$ column echelon matrix, say $Y_1 = [I_r | Y_1']^T$ where $Y_1' = [y_{ij}']\ \begin{smallmatrix} r+1\leq i\leq n \\ 1\leq j\leq r\end{smallmatrix}$. We now show that the rings R_M, R' are isomorphic by showing that the pair (R', Y_1) satisfies all the conditions of $(5.15)'$ (in which case the isomorphism takes x_{ij} to y_{ij}') :-

1) By $(5.8.1)'$ applied to R', certainly R' is reduced.

2) By $(5.8.2)'$ applied to Y, every $(r\times r)$ subdeterminant of Y is either zero or a unit in R' and R' is generated by these units and their inverses. By (5.18.2) it is clear that the $(r\times r)$ subdeterminants of Y_1 differ from those of Y by at most a factor of $\pm z$ which is itself an $(r\times r)$ subdeterminant of Y_1 (since $y_{r+1,r}' = z$). Thus $(5.15.2)'$ holds for (R', Y_1).

3) Let $N = [I_r | N']^T$ be a column echelon F-representation of M (where $N' = [\alpha_{ij}]$) with respect to the original ordering of E. By (5.18.1) $\alpha_{r+1,r} \neq 0$. Write $\beta = (\alpha_{r+1,r})^{-1}$.

Then the matrix N_1 (defined overleaf by (5.18.3)) is a column echelon F-representation of M with respect to the new ordering of E. Suppose the (i,j) entry of N_1 is α_{ij}' . Then by $(5.8.3)'$ applied to (R', Y) there is a homomorphism $f: R' \to F$ in which $f(y_{ij}) = \alpha_{ij}'$. It is clear from (5.18.3) that $\alpha_{r+1,r}' = \beta$

$$N_1 = P_{r,r+1} \quad N \begin{bmatrix} 1 & \cdots & 0 & 0 \\ 0 & & & \\ \vdots & & & \\ 0 & & 1 & 0 \\ -(\alpha_{r+1,1})\beta & \cdots & -(\alpha_{r+1,r-1})\beta & \beta \end{bmatrix} \qquad (5.18.3)$$

and that , for each $i=1,\ldots,r-1$, $\alpha'_{r+1,i} = -(\alpha_{r+1,i})$.

Now, $f(z) = f(\alpha'_{r+1,r})^{-1} = \beta^{-1}$, and so for $i=1,\ldots r-1$

$f(-(y_{r+1,i})z) = -f(y_{r+1,i})\,\beta^{-1} = \alpha_{r+1,i}$.

So applying f to (5.18.2), we get

$$f([Y_1]) = P_{r,r+1}N_1 \begin{bmatrix} 1 & \cdots & 0 \\ 0 & & 0 \\ \vdots & & \\ 0 & & 1 \\ \alpha_{r+1,1} & \cdots & \alpha_{r+1,r} \end{bmatrix} = N \qquad \text{(by (5.18.3))}$$

and so $f(y'_{ij}) = \alpha_{ij}$, in which case $(5.15.3)'$ holds for (R',Y_1).

4) Let $f\colon R'\longrightarrow F$ be a homomorphism. Suppose $f(y'_{ij}) = \alpha_{ij}$. We have to show $N = [I_r|N']^T$ (where $N'=[\alpha_{ij}]$) is an F-representation of M (with respect to the original ordering of E).

Let N_1 be defined as in (5.18.3). By (5.18.2) we have

$$Y = P_{r,r+1} \ Y_1 \begin{bmatrix} 1 & \cdots & 0 \\ 0 & & 0 \\ \vdots & & \\ 0 & & 1 \\ y_{r+1,1} & \cdots & y_{r+1,r} \end{bmatrix}$$

Applying f to this expression yields

$$f([Y]) = P_{r,r+1} \ N \begin{bmatrix} 1 & \cdots & 0 \\ 0 & & 0 \\ \vdots & & \\ 0 & & 1 \\ f(y_{r+1,1}) & \cdots & f(y_{r+1,r}) \end{bmatrix} = N_1 \qquad \text{(by (5.18.2) and (5.18.3))}$$

Thus, if the (i,j) entry of N_1 is α'_{ij} we have $f(y_{ij}) = \alpha'_{ij}$. Now by $(5.8.4)'$ applied to (R',Y), it follows that N_1 is a representation of M with respect to the new ordering of E, in which case, by definition of N_1, we must have N is a representation of M with respect to the original ordering.

Thus $(5.15.4)'$ holds for (R',Y_1) and the theorem follows.

(5.19) Theorem For a matroid M, $R_M \approx R_{M^*}$.

Proof By (5.18) we may certainly assume that R_{M^*} is defined with respect to the ordering $e_{r+1},\dots,e_n,e_1,\dots e_r$ where of course $B = \{e_{r+1},\dots,e_n\}$ is a basis of M.

Suppose that $Z = \left[\begin{array}{c} I_{n-r} \\ \hline Z_1 \end{array}\right]$ (where $Z_1 = [z_{ij}]_{\substack{1\le i\le r \\ r+1\le j\le n}}$) is the matrix over R_M for which (R_M, Z) satisfy $(5.8)'$.

Let $Z' = \left[\begin{array}{c} I_r \\ \hline Z_1^T \end{array}\right]$. Once again we appeal to the univeral property by showing that the pair (R_{M^*}, Z') satisfy the conditions of $(5.8)'$.

1) Certainly R_{M^*} is reduced.

2) For any r-set $U \subset E$, it is easily seen that $\det Z'(U) = \det Z(E\backslash U)$, in which case the set of $(r\times r)$ subdeterminants of Z' is precisely the same as the set of $((n-r)\times(n-r))$ subdeterminants of Z which have the desired property.

3) Suppose $N = \left[\begin{array}{c} I_r \\ \hline N_1 \end{array}\right]$ is an F-representation of M, where say $N_1 = [\alpha_{ij}]_{\substack{r+1\le i\le n \\ 1\le j\le r}}$. Then the matrix $N' = \left[\begin{array}{c} I_{n-r} \\ \hline N_1^T \end{array}\right]$ is an F-representation of M^* with respect to the ordering $e_{r+1},\dots, e_n,e_1,\dots,e_r$. Thus by $(5.8.3)'$ applied to (R_{M^*}, Z) it follows that there is a unique homomorphism $f: R_{M^*} \to F$ in which $f(z_{ij}) = \alpha_{ji}$. But the (i,j) entry of Z' is y_{ji} and so $f(y_{ji}) = \alpha_{ij}$ as required.

4) Suppose $f: R_{M^*} \to F$ is a homomorphism in which $f(y_{ij}) = \alpha_{ij}$, say. If $N_1 = [\alpha_{ij}]$ we have to show that $\left[\dfrac{I_r}{N_1^T}\right]$ is an F-representation of M. Now, by $(5.8.4)'$ applied to (R_{M^*}, Z) we have that $\left[\dfrac{I_{n-r}}{N_1}\right]$ is an F-representation of M^*, so the result follows.

We now deduce by $(5.15)'$ that R_M, R_{M^*} are isomorphic under a mapping which takes x_{ij} to z_{ji}.

(5.20) Theorem For a matroid M, $R_M \approx R_{M_0}$, where M_0 is the underlying simple matroid of M (defined in (1.24)).

Proof With the notation of (1.24) we may assume that the first m elements of E $(m \leq n)$ are precisely E_0. Hence the elements, $e_{m+1}, \ldots, e_n$ are either loops or parallel elements. We now define R_{M_0} with respect to $e_1, \ldots, e_m$; suppose $Y = [I_r | Y']^T$ is the $(n \times r)$ matrix over R_{M_0} for which (R_{M_0}, Y) satisfy $(5.8)'$. Now let Y_1 be the $(n \times r)$ matrix over R_{M_0} defined by

$$Y_1 = \begin{bmatrix} Y \\ \hline -\underline{v}_{m+1}- \\ \vdots \\ -\underline{v}_m- \end{bmatrix}$$

where the row $\underline{v}_t$ $(m+1 \leq t \leq n)$ is zero if e_t is a loop in M, and if e_t is parallel to some e_i $(1 \leq i \leq m)$ then $\underline{v}_t$ is precisely the t^{th} row of Y repeated. It is now routine to check that the pair (R_{M_0}, Y_1) satisfy all four conditions of $(5.15)'$.

(5.21) Theorem With the same hypothesis as (1.35) (for t=2), suppose $M = M_1 + M_2$. Then $R_M \approx \dfrac{R_{M_1} \otimes_Z R_{M_2}}{N(R_{M_1} \otimes_Z R_{M_2})}$ (= S, say)

<u>Proof</u> Suppose that $Y = [I_{r_1} | [y_{ij}]]^T$, $Z = [I_{r_2} | [z_{ij}]]^T$ are the matrices over R_{M_1}, R_{M_2} respectively for which (R_{M_1}, Y), (R_{M_2}, Z) satisfy $(5.8)'$. We shall identify elements of $R_{M_1} \otimes_{\mathbb{Z}} R_{M_2}$ with their natural images in S. Define the matrices

$$V = \left[\begin{array}{c|c} \multicolumn{2}{c}{I_r} \\ \hline [y_{ij} \otimes 1] & 0 \\ \hline 0 & [1 \otimes z_{ij}] \end{array}\right], \quad Y' = \left[\begin{array}{c} I_{r_1} \\ \hline [y_{ij} \otimes 1] \end{array}\right], \quad Z' = \left[\begin{array}{c} I_{r_2} \\ \hline [1 \otimes z_{ij}] \end{array}\right]$$

We now show that (S,V) satisfy the conditions of $(5.15)'$.

1) By definition S is a reduced ring.

2) For any r-set $U \subset E$, if $U = U_1 \cup U_2$ where U_i is an r_i-subset of E_i $(i=1,2)$, then it is easily seen that

$$\det V(U) = \det Y'(U_1).\det Z'(U_2) = (\det Y(U_1) \otimes 1).(1 \otimes \det Z(U_2))$$
$$= \det Y(U_1) \otimes \det Z(U_2)$$

and since $\det Y(U_1)$, $\det Z(U_2)$ are either zero or units in R_{M_1}, R_{M_2} respectively, it follows that $\det V(U)$ is either zero or a unit in S. By similar arguments it is routine to check that every $(r \times r)$ subdeterminant of V is zero or a unit in S, and that S is generated by these elements together with their inverses.

3) If N is any F-representation of M then it follows from (1.35) that N has the form

$$N = \left[\begin{array}{c|c} \multicolumn{2}{c}{I_r} \\ \hline [\alpha_{ij}] & 0 \\ \hline 0 & [\beta_{ij}] \end{array}\right]$$

By $(5.8)'$ there are homomorphisms $f_i : R_{M_i} \longrightarrow F$ $(i=1,2)$ in which $f_1(y_{ij}) = \alpha_{ij}$ and $f_2(z_{ij}) = \beta_{ij}$. It now follows from (1.1) that there is a homomorphism $f: R_{M_1} \otimes R_{M_2} \longrightarrow F$ in which $f(y_{ij} \otimes 1) = \alpha_{ij}$ and $f(1 \otimes z_{ij}) = \beta_{ij}$. Since f clearly factors through S, we get the required homomorphism $f: S \to F$.

4) Suppose $f: S \to F$ is a homomorphism in which, say $f(y_{ij} \otimes 1) = \alpha_{ij}$ and $f(1 \otimes z_{ij}) = \beta_{ij}$. Certainly f induces homomorphisms $f_i: R_{M_i} \to F$ (for i=1,2), in which $f_1(y_{ij}) = \alpha_{ij}$ and $f_2(z_{ij}) = \beta_{ij}$. Thus by (5.8.4)′ applied to (R_{M_1}, Y), (R_{M_2}, Z) we deduce that the matrices $[I_{r_1} | [\alpha_{ij}]]^T$, $[I_{r_2} | [\beta_{ij}]]^T$ are respectively F-representations of M_1, M_2. By (1.36) it now follows that f induces the required F-representation of M.

Thus by (5.15)′, $R_M \approx S$.

To complete this section we now establish the exact algebraic relationship between the rings A_M and R_M

(5.22) <u>Theorem</u> <u>Suppose $Z = [Z_{ij}]_{\substack{1 \le i \le r \\ 1 \le j \le r}}$ is an $(r \times r)$ generic matrix of indeterminates Z_{ij}.</u>

<u>Then $A_M \approx R_M[\{Z_{ij}\}_{i,j}]_{(\det Z)}$</u>

<u>Proof</u> To avoid confusion we assume that $(A_M, \mathfrak{X})$ is defined as before and that Y is the matrix over R_M for which (R_M, Y) satisfy (5.8)′. Then Y has the form

$$Y = [I_r | Y']^T \quad \text{where} \quad Y' = [y_{ij}]_{\substack{1 \le i \le n-r \\ 1 \le j \le r}}$$

Write $S = R_M[\{Z_{ij}\}_{i,j}]_{(\det Z)}$. We shall identify elements of R_M with their natural images in S. In particular we form the $(n \times r)$ matrix $V = YZ$ over S. We now show that (S,V) satisfy the conditions of (5.15) :-

1) It is clear that S is a reduced ring since R_M is.

2) Every $(r \times r)$ submatrix of V has the form $Y_1 Z$ where Y_1 is an $(r \times r)$ submatrix of Y. But $\det Y_1 Z = \det Y_1 . \det Z$ which is

either zero or a unit in S since (by (5.8.2)$'$) det Y_1 is either zero or a unit in R_M (hence also in S) and by construction, det Z is a unit in S. Now by (5.8.2)$'$, R_M is finitely generated (as a $\mathbb{Z}$-algebra) by elements of the form det Y_1,(det $Y_1)^{-1}$ where Y_1 is an (r×r) submatrix of Y. By definition of S it follows that these elements together with the Z_{ij}'s (which are entries of V) and the element $(\det Z)^{-1}$ (which is the inverse of an (r×r) subdeterminant of V) generate S as a $\mathbb{Z}$-algebra. Also,

$$\det Y_1 = (\det Y_1 Z).(\det Z)^{-1}$$

$$\text{and,}\qquad (\det Y_1)^{-1} = (\det Y_1 Z)^{-1}(\det Z)$$

Consequently it follows that S is generated as a $\mathbb{Z}$-algebra by the entries of V together with the inverses of the (r×r) non-zero subdeterminants of V.

3) Suppose N is an F-representation of M. We may write

$N = \left[\begin{array}{c} N_1 \\ \hline N_2 \end{array}\right]$, where $N_1 = [\alpha_{ij}]_{\substack{1\le i\le r\\ 1\le j\le r}}$, and $N_2 = [\beta_{ij}]_{\substack{1\le i\le n-r\\ 1\le j\le r}}$.

We have to show that there is a homomorphism $f: S \to F$ in which $f(Z_{ij}) = \alpha_{ij}$ $(1\le i,j\le r)$, and the (i,j) entry of $Y'Z$ is mapped by f onto β_{ij} $(1\le i\le n-r,\ 1\le j\le r)$. Now since $B = \{e_1,\ldots,e_r\}$ is a basis of M, det N_1 = det $N(B) \neq 0$. Thus N_1 is invertible. Suppose that $N_1^{-1} = [\zeta_{ij}]_{\substack{1\le i\le r\\ 1\le j\le r}}$. This means that

$$\left.\begin{array}{lll} \displaystyle\sum_{k=1}^{r} \zeta_{ik}\,\alpha_{ki} = 1 & (i=1,\ldots,r) \\ \text{and} \quad \displaystyle\sum_{k=1}^{r} \zeta_{ik}\,\alpha_{kj} = 0 & (i \neq j) \end{array}\right\} \qquad (5.22.1)$$

Moreover, NN_1^{-1} is again an F-representation of M which is in column echelon form, since $NN_1^{-1} = [\,I_r \mid N_2N_1^{-1}]^T$. Thus by (5.8.3)$'$ applied to (R_M, Y), there is a homomorphism $f: R_M \to F$ in which y_{ij} is mapped to the (i,j) entry of $N_2N_1^{-1}$. That is

$$f(y_{ij}) = \sum_{\ell=1}^{r} \beta_{i\ell}\, \zeta_{\ell j} \qquad \text{for} \quad 1 \leq i \leq n-r,\ 1 \leq j \leq r \qquad (5.22.2)$$

We may now extend f to a homomorphism $f : R_M[\{Z_{ij}\}_{i,j}] \longrightarrow F$ by defining $f(Z_{ij}) = \alpha_{ij}$. Since then $f(\det Z) = \det N_1 \neq 0$ this homomorphism in turn induces a homomorphism $f: S \rightarrow F$. We have only to show that the (i,j) entry of $Y'Z$ is mapped by f to β_{ij}. Now the (i,j) entry of $Y'Z$ is $\sum_{k=1}^{r} y_{ik} Z_{kj}$ $(1 \leq i \leq n-r,\ 1 \leq j \leq r)$ and

$$\begin{aligned}
f\Big(\sum_{k=1}^{r} y_{ik} Z_{kj}\Big) = \sum_{k=1}^{r} f(y_{ik})\, f(Z_{kj}) &= \sum_{k=1}^{r} f(y_{ik})\, \alpha_{kj} \\
&= \sum_{k=1}^{r} \Big(\sum_{\ell=1}^{r} \beta_{i\ell}\, \zeta_{\ell k}\Big) \alpha_{kj} \\
&= \sum_{\ell=1}^{r} \Big(\sum_{k=1}^{r} \zeta_{\ell k}\, \alpha_{kj}\Big) \beta_{i\ell} \\
&= \beta_{ij} \qquad \text{by } (5.22.1)
\end{aligned}$$

4) Suppose $f: S \rightarrow F$ is a homomorphism, with say $f(Z_{ij}) = \alpha_{ij}$ $(1 \leq i,j \leq r)$, and $f(\sum_{k=1}^{r} y_{ik} Z_{kj}) = \beta_{ij}$ $(1 \leq i \leq n-r,\ 1 \leq j \leq r)$. Then if $N_1 = [\alpha_{ij}]$ and $N_2 = [\beta_{ij}]$ we have to show that the matrix $N = [N_1 | N_2]^T$ is an F-representation of M. We first note that $\det N_1 = f(\det Z) \neq 0$ (since $\det Z$ is a unit in S), so that N_1 is invertible.

$$\text{Let} \quad N' = \begin{bmatrix} f(y_{11}) & \cdots & f(y_{1r}) \\ \vdots & & \vdots \\ f(y_{n-r,1}) & \cdots & f(y_{n-r,r}) \end{bmatrix}$$

Then the (i,j) entry of $N'N_1$ is

$$\sum_{k=1}^{r} f(y_{ik})\, \alpha_{kj} = \sum_{k=1}^{r} f(y_{ik})\, f(Z_{kj}) = f\Big(\sum_{k=1}^{r} y_{ik} Z_{kj}\Big) = \beta_{ij}$$

$$\text{Thus} \quad N'N_1 = N_2 \quad \text{, and hence} \quad N' = N_2 N_1^{-1} .$$

Since f restricts in the natural way to a homomorphism from R_M

into F, it now follows from $(5.8.4)'$ applied to (R_M, Y), that $\left[\frac{I_r}{N_2 N_1^{-1}}\right]$ is an F-representation of M. Post-multiplication by the invertible matrix N_1 still yields an F-representation – namely N as required.

It now follows from (5.15) that $A_M \approx R_M$ under an isomorphism taking x_{ij} to the (i,j) entry of V.

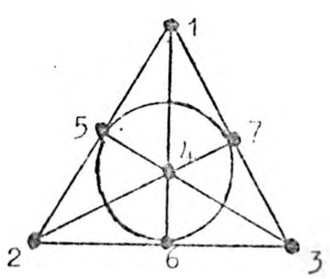
The Canonical Vámos Ring

In studying matroid representations we have already seen in §2 that it really suffices to study representations which are in p.c.f. This is the motivation behind the following construction of the canonical Vámos ring :-

(5.23) Once again we assume the usual fixed ordering of E with basis B. Suppose that the B-basic c.i.matrix A_B has exactly s non-zero, non-atomic entries. Let $T = \mathbb{Z}[X_1, \ldots, X_s]$, the polynomial ring over $\mathbb{Z}$ in s indeterminates.

We now replace each one of the non-zero, non-atomic entries of A_B by exactly one of the X_i's. Suppose the resulting matrix is $D' = [d_{ij}]_{\substack{r+1 \leq i \leq n \\ 1 \leq j \leq r}}$. Write $D = [I_r | D']^T$. Although T is not a field, the matrix D over T is in p.c.f. in the sense of (2.10).

Example Suppose M is the Fano matroid on $E = \{1, \ldots, 7\}$ with planar representation given below



Clearly $B = \{1,2,3\}$ is a basis of M . Now

$$A_B = \begin{array}{c} 4 \\ 5 \\ 6 \\ 7 \end{array} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

(where the non-zero, non-atomic entries are ringed)

Thus $T = \mathbb{Z}[X_1, X_2, X_3]$, and

$$D' = \begin{bmatrix} 1 & 1 & 1 \\ 1 & X_1 & 0 \\ 0 & 1 & X_2 \\ 1 & 0 & X_3 \end{bmatrix} \qquad \text{and} \quad D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & X_1 & 0 \\ 0 & 1 & X_2 \\ 1 & 0 & X_3 \end{bmatrix}$$

Based on the matrix D we now construct the canonical Vámos ring V_M in an entirely analagous way as before; we let $\underline{b}$ be the ideal of T generated by the set $\{\det D(U);\ U \text{ non-basis of } M\}$ and let $a = \Pi\{\det D(U);\ U \text{ basis of } M\}$. The <u>canonical Vámos ring</u> is the ring

$$V_M = (T/\sqrt{\underline{b}})_{(\bar{a})}$$

In much the same way as R_M is a universal object with respect to column echelon representations of M, we will see that V_M is universal with respect to representations in p.c.f.

Let θ denote the natural map of T into V_M and let $\theta(d_{ij}) = t_{ij}$. Write $L' = [t_{ij}]$ and $L = [I_r | L']^T$. Once again we can now list all the analagous results which hold for the pair (V_M, L). The only 'new' part of the proofs is to note that every representation matrix is projectively equivalent to a representation in p.c.f.

<u>(5.5)''</u> <u>With T, $\underline{b}$, a as above, M is representable if and only if $a \notin \sqrt{\underline{b}}$</u>

<u>(5.7)''</u> 1) <u>$V_M = (0)$ if and only if M is not representable</u>

2) <u>V_M is a Noetherian ring</u>

(5.8)″ The ring V_M, together with the matrix L, satisfies :-

1) V_M is a reduced ring.

2) Every $(r\times r)$ subdeterminant of L is either zero or a unit in V_M, and V_M is finitely generated (as a $\mathbb{Z}$-algebra) by these units together with their inverses.

3) For any field F and $(n\times r)$ matrix N which is an F-representation of M in p.c.f., there is a unique homomorphism $f: V_M \to F$ which makes the diagram below commute.

$$\begin{tikzcd} T \arrow[r, "\theta"] \arrow[d, "g^N"'] & V_M \arrow[dl, dashed, "f"] \\ F & \end{tikzcd}$$

4) For any homomorphism $f: V_M \to F$ (F a field) there is a unique F-representation N in p.c.f. which makes the above diagram commute.

(5.9)″ To each $p \in \operatorname{Spec} V_M$ there corresponds a representation of M in p.c.f. over K_p, the quotient field of V_M/p, namely $N_p = [I_r|\pi(t_{ij})]^T$ (where π is the composite map $V_M \to V_M/p \to K_p$). Conversely, to each F-representation $N = [I_r||\alpha_{ij}]]^T$ in p.c.f. there corresponds a homomorphism $f_N: V_M \to F$ in which $f(t_{ij}) = \alpha_{ij}$, and hence a corresponding prime ideal p_N of V_M, where $p_N = \operatorname{Ker} f_N$.

(5.10)″ The ring V_M is a Jacobson ring for which V_M/m is a finite field for each maximal ideal m.

(5.15)″ (universal property) Let S be a ring and $Y = [I_r|Y']^T$ (where $Y' = [y_{ij}]_{\substack{r+1\leq i\leq n \\ 1\leq j\leq r}}$, say) an $(n\times r)$ matrix over S in p.c.f. such that the pair (S,Y) satisfy :-

1) S is a reduced ring.

2) Every $(r\times r)$ subdeterminant of Y is either zero or a unit in S, and S is finitely generated as a $\mathbb{Z}$-algebra by these units together with their inverses.

3) For any field F and $(n\times r)$ matrix N which is an F-representation of M in p.c.f., there is a unique homomorphism h making the diagram below commute.

$$\begin{tikzcd} T \arrow[r, "\delta"] \arrow[d, "g^N"'] & S \arrow[dl, dashed, "h"] \\ F & \end{tikzcd}$$

(where δ is induced by $\delta(d_{ij}) = y_{ij}$)

4) For any homomorphism $h: S\to F$ (F a field) there is a unique F-representation in p.c.f. which makes the above diagram commute.

<u>Then the rings V_M and S are isomorphic under an isomorphism taking t_{ij} to y_{ij}.</u>

In §4 we saw that the notion of generalised projective equivalence was, in every natural sense, the same essentially as projective equivalence. In the light of this observation the following theorem is of great significance :-

(5.24) <u>Theorem</u>. <u>The correspondence in $(5.9)''$ between the prime ideals of V_M and the representations of M in p.c.f. is actually a bijection, providing we do not distinguish between g.p.e. representations. That is, there is a natural one-to-one correspondence between the prime ideals of V_M and the (g.p.e) classes of representations of M.</u>

<u>Proof</u> By $(5.9)''$ we have to prove that if N_1, N_2 are representations of M in p.c.f. over fields F_1, F_2 respectively, then

$\operatorname{Ker} f_{N_1} = \operatorname{Ker} f_{N_2}$ if and only if N_1, N_2 are g.p.e.

For ease of notation write f_i for f_{N_i} $(i=1,2)$. Suppose that $N_1 = [I_r \| [\alpha_{ij}]]^T$, and $N_2 = [I_r \| [\beta_{ij}]]^T$.

First suppose N_1, N_2 are g.p.e. This means that there is an isomorphism $\sigma: F_1 \longrightarrow F_2$ in which $\sigma(\alpha_{ij}) = \beta_{ij}$. But then

$$f_2(t_{ij}) = \beta_{ij} = \sigma(\alpha_{ij}) = \sigma f_1(t_{ij})$$

By (5.8.2)″ this means that $f_2 = \sigma f_1$. Thus $\operatorname{Ker} f_2 = \operatorname{Ker} f_1$ since σ is injective.

Conversely suppose $\operatorname{Ker} f_1 = \operatorname{Ker} f_2$. Now for i=1,2 $V_M/\operatorname{Ker} f_i \approx f_i(V_M)$, where $f_i(V_M)$ denotes the subring of F_i generated by the image of V_M under f_i, so we deduce that $f_1(V_M) \approx f_2(V_M)$ under an isomorphism σ which maps α_{ij} to β_{ij}. Since for i=1,2, $f_i(V_M)$ contains all the entries of N_i, it follows from (4.16) that F_i is the quotient field of $f_i(V_M)$. Consequently, by the universal property of quotient fields, it follows that σ extends in the natural way to an isomorphism from F_1 onto F_2 . Thus N_1, N_2 are g.p.e. by defn.(4.15).

By (5.24) we have not only provided the third characterization of generalised projective equivalence promised in §4, but we have also reduced the representation problem to a study of Spec V_M and for this we use the sophisticated machinery of commutative algebra. Moreover if we are just interested in representations over finite fields we have :-

(5.25) Corollary The correspondence in (5.9)″ restricts to a bijection between the maximal ideals of V_M and the g.p.e. classes of representations of M over finite fields.

Proof By (5.24) it suffices to prove

1) that if $\underline{m}$ is a maximal ideal of V_M then $V_M/\underline{m}$ is finite

and 2) if N is an F-representation (in p.c.f.) of M where F is finite, then Ker f_N is a maximal ideal of V_M.

1) has already been established in (5.10)″

2) since F is finite, $f_N(V_M)$ is a finite integral domain contained in F. But every finite domain is a field, so because of (4.16) $f_N(V_M) = F$, that is, f_N is surjective and $V_M/\text{Ker } f_N \approx F$. Hence Ker f_N is a maximal ideal of V_M.

In the next theorem we establish the algebraic relationship between the rings V_M, R_M. We shall assume that M has k connected components and hence (by (2.22)) the B-basic c.i. matrix A_B has n-k atomic entries. Let $q = n-k$, and H the free Abelian group on q generators $Z_1,\ldots,Z_q$.

(5.26) Theorem $\quad R_M \approx V_M\langle Z_1,\ldots,Z_q\rangle \quad (= V_M(H))$

Proof Write $S = V_M\langle Z_1,\ldots,Z_q\rangle$. Recalling that $L = [I_r \mid L']^T$ (where $L' = [t_{ij}]_{\substack{r+1\le i\le n\\ i\le j\le r}}$) we shall identify the t_{ij}'s with their natural images in S. By construction the matrix L' has s atomic entries (all equal to 1), so suppose these appear in the $(i_1,j_1),\ldots,(i_q,j_q)$ positions of L'. It can be shown by an argument which is a repetition of the proof of (2.8.1) that we can find elements $f_{r+1},\ldots,f_n$, $g_1,\ldots,g_r \in H$ $(\subset S)$

$$\text{such that} \quad f_{i_k} g_{i_k} = Z_k \quad (\text{for } k=1,\ldots,q)$$

So if we write $y_{ij} = f_i t_{ij} g_j$ and $Y' = [y_{ij}]_{\substack{r+1\le i\le n\\ 1\le j\le r}}$

$$\text{then} \quad Y' = \text{diag}(f_{r+1},\ldots,f_n)\, L'\, \text{diag}(g_1,\ldots,g_r) \qquad (5.26.1)$$

and the k^{th} atomic entry of Y' is equal to Z_k $(k=1,\ldots,q)$.

If we now write $Y = [I_r | Y']^T$, then we will prove the theorem by showing that the pair (S,Y) satisfy the conditions of $(5.15)'$:-

1) Certainly S is reduced since V_M is.

2) By (5.26.1) every $(r\times r)$ subdeterminant of Y has the form $h \det L(U)$ where $h \in H$ and U is an r-subset of E. Every element of H is a unit in S and $\det L(U)$ is either zero or a unit in V_M (hence also in S), so we deduce that every $(r\times r)$ subdeterminant of Y is either zero or a unit in S. Moreover, by construction, $Z_1,\dots,Z_q$ all appear as entries of Y', hence (up to sign) as $(r\times r)$ subdeterminants of Y. Now S is clearly generated as a $\mathbb{Z}$-algebra by V_M together with the elements $Z_1,\dots,Z_q$, $Z_1^{-1},\dots,Z_q^{-1}$. By $(5.8.2)''$ V_M is finitely generated as a $\mathbb{Z}$-algebra by elements of the form $\det L(U)$, $(\det L(U))^{-1}$ (where U is an r-subset of E), and $\det L(U) = h \det Y(U)$ for some $h \in H$. It now follows that S is finitely generated as a $\mathbb{Z}$-algebra by the $(r\times r)$ subdeterminants of Y, together with their inverses.

3) Suppose that $N = [I_r | N']^T$ is a column echelon F-representation of M where $N' = [\alpha_{ij}]_{\substack{r+1\leq i\leq n \\ 1\leq j\leq r}}$. We have to find a homomorphism $h : S \to F$ for which $f(y_{ij}) = \alpha_{ij}$.

By (1.42), N' has its atomic entries in the same corresponding positions as A_B (and hence also L', Y'), that is, the $(i_1,j_1),\dots,(i_q,j_q)$ positions. For ease of notation write

$$\alpha_{i_k j_k} = \gamma_k \qquad (k=1,\dots,q)$$

The elements $f_{r+1},\dots,f_n$, $g_1,\dots,g_r$ are of course 'functions' of $Z_1,\dots,Z_q$ of the form $Z_1^{m_1}\dots Z_q^{m_q}$ $(m_i \in \mathbb{Z})$, so if $f_i = f_i(Z_1,\dots,Z_q)$ and $g_j = g_j(Z_1,\dots,Z_q)$, then in the sense of (4.9) we may define elements $\delta_{r+1},\dots,\delta_n$, $\mu_1,\dots,\mu_r$ of F by

$$\delta_i = f_i(\gamma_1,\ldots,\gamma_q) \qquad i=r+1,\ldots,n$$
$$\mu_j = g_j(\gamma_1,\ldots,\gamma_q) \qquad j=1,\ldots,r \qquad (5.26.2)$$

The δ_i's and μ_j's are all non-zero, and since $f_{i_k} g_{j_k} = Z_k$,

$$\delta_{i_k} \mu_{j_k} = \gamma_k \qquad k=1,\ldots,q \qquad (5.26.3)$$

Consider the matrix

$$N_1 = \operatorname{diag}(\mu_1,\ldots,\mu_r, \delta_{r+1}^{-1},\ldots,\delta_n^{-1})\ N\ \operatorname{diag}(\mu_1^{-1},\ldots,\mu_r^{-1}),$$

so $N_1 = [I_r|N_1']^T$ where $N_1' = [\delta_i^{-1}\alpha_{ij}\mu_j^{-1}]$. The matrices N, N_1 are projectively equivalent so N_1 is an F-representation of M. Moreover, N_1 is in p.c.f. since for each $k=1,\ldots,q$, the k^{th} atomic entry of N_1' is

$$\delta_{i_k}^{-1}\ \alpha_{i_k j_k}\ \mu_{j_k}^{-1} = \delta_{i_k}^{-1}\ \gamma_k\ \mu_{j_k}^{-1} = 1 \quad (\text{by } (5.26.3))$$

Thus, by $(5.8.3)''$ there is a homomorphism $h: V_M \to F$ in which $h(t_{ij}) = \delta_i^{-1}\alpha_{ij}\ \mu_j^{-1}$. Certainly h extends to a homomorphism from S into F if we define $h(Z_k) = \gamma_k$ for $k=1,\ldots,q$.
Now for $i=r+1,\ldots,n$, $j=1,\ldots,r$ we have

$$\begin{aligned} h(y_{ij}) = h(f_i t_{ij} g_j) &= h(f_i)\ h(t_{ij})\ h(g_j) \\ &= h(f_i)\ h(g_j)\ \delta_i^{-1}\alpha_{ij}\ \mu_j^{-1} \\ &= h(f_i(Z_1,\ldots,Z_q))\ h(g_j(Z_1,\ldots,Z_q))\ \delta_i^{-1}\alpha_{ij}\ \mu_j^{-1} \\ &= f_i(\gamma_1,\ldots,\gamma_q)\ g_j(\gamma_1,\ldots,\gamma_q)\ \delta_i^{-1}\alpha_{ij}\ \mu_j^{-1} \\ &= \delta_i\ \mu_j\ \delta_i^{-1}\alpha_{ij}\ \mu_j^{-1} \qquad (\text{by } (5.26.2)) \\ &= \alpha_{ij} \qquad \text{as required.} \end{aligned}$$

4) Suppose $h: S \to F$ is a homomorphism in which $h(y_{ij}) = \alpha_{ij}$ say. Write $N' = [\alpha_{ij}]$ and $N = [I_r|N']^T$. We have to show that N is an F-representation of M.

For $k=1,\ldots,q$ write $\alpha_{i_k j_k} = \gamma_k$ so then $h(Z_k) = \gamma_k$, which is non-zero since Z_k is a unit in S. Let δ_i, μ_j be defined as in (5.26.2).

Now $h(f_i t_{ij} g_j) = h(y_{ij}) = \alpha_{ij}$, that is,

$$\begin{aligned}\alpha_{ij} = h(f_i t_{ij} g_j) &= h(t_{ij})\, h(f_i)\, h(g_j)\\ &= h(t_{ij})\, h(f_i(Z_1,\ldots,Z_q))\, h(g_j(Z_1,\ldots,Z_q))\\ &= h(t_{ij})\, f_i(\gamma_1,\ldots,\gamma_q)\, g_j(\gamma_1,\ldots,\gamma_q)\\ &= h(t_{ij})\, \delta_i\, \mu_j\end{aligned}$$

Hence $h(t_{ij}) = \delta_i^{-1} \alpha_{ij}\, \mu_j^{-1}$. Thus, by considering the restriction of h to V_M we deduce from $(5.8.4)''$ that the matrix $N_1 = [I_r | N_1']^T$, where $N_1' = [\delta_i^{-1} \alpha_{ij}\, \mu_j^{-1}]$, is an F-representation of M. But N is projectively equivalent to N_1 so N is an F-representation of M as required.

The theorem now follows from $(5.15)'$.

(5.27) Remark We have shown that both the rings A_M and R_M are independent of the ordering of M. We obviously hope now to establish the same result result for V_M , that is, if V_M' is the canonical Vámos ring defined with respect to a different ordering of E, then

$$V_M \approx V_{M'} \qquad (5.27.1)$$

In [29] , Sehgal conjectured that for any commutative, Noetherian rings R, S,

$$R\langle Y\rangle \approx S\langle Y\rangle \quad \text{implies} \quad R \approx S.$$

If this conjecture were true then (5.27.1) would follow immediately from (5.18) and (5.26). However in [22] , Krempa has provided a counter-example, so it seems that we may not be able to deduce (5.27.1) from (5.26) and the general theory of group rings as I had first expected. I believe however that a proof of (5.27.1) could be constructed along the same lines as (5.18), using (5.15)". Until all the extremely labourious and technical details of such a proof are checked, (5.27.1) will have to remain a (very strong) conjecture. It should be noted that all the examples of V_M given at the end of this section are certainly independent of the ordering of E.

Until (5.27.1) can be proved, the analagous results to (5.19),(5.20),(5.21) for V_M will only hold with respect to certain orderings of E. However, since these are very significant results modulo (5.27.1) we state them below. Only (5.19)$'$ now requires any additional justification.

(5.20)$'$ With respect to the orderings of E given in (5.20), $V_M \approx V_{M_0}$.

(5.21)$'$ Suppose $M = M_1(E_1) \oplus M(E_2)$. Then with respect to the orderings of E, E_1, E_2 given in (5.21),

$$V_M \approx \frac{V_{M_1} \otimes_Z V_{M_2}}{N(V_{M_1} \otimes_Z V_{M_2})}$$

(5.19)$'$ There are orderings of E for which $V_M \approx V_{M^*}$.

Proof By (2.25) there is an ordering of E with respect to which the matrix A_B is in step diagonal form. Suppose this ordering is $e_1,\dots,e_n$. Now suppose $A = [I_r|A_1]^T$ is an F-representation of M with respect to this ordering which is in p.c.f. By (2.26) every atomic entry of A_1^T is equal to 1, since by (1.42) A_1 is in s.d.f. Thus $[I_{n-r}|A_1^T]^T$ is also in p.c.f. With this consideration, the proof of (5.19) carries through in this case if V_M is defined with respect to $e_1,\dots,e_n$ and V_{M^*} is defined with respect to $e_{r+1},\dots,e_n, e_1,\dots,e_r$.

(5.28) Examples

1) Suppose M is the uniform matroid $U_{2,k}$ for $k \geq 4$. Write $m = k-3$.

$$\text{Then } D = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & X_1 \\ \vdots & \vdots \\ 1 & X_m \end{bmatrix} \qquad T = \mathbb{Z}[X_1,\ldots,X_m]$$

In this case $\underline{b} = 0$, and $a = (\prod_{i=1}^{m} X_i)(\prod_{i=1}^{m}(1-X_i))(\prod_{i<j}^{m}(X_i-X_j))$

Hence $V_M = \mathbb{Z}[X_1,\ldots,X_m]_{(a)}$ in this case. Since a is a unit in V_M it is now easily deduced that M is representable over F if and only if $|F| \geq m+2$.

2) The matroid M is regular if and only if $V_M \approx \mathbb{Z}$

Proof First suppose $V_M \approx \mathbb{Z}$. For any field F there is a homomorphism $f: \mathbb{Z} \to F$ defined by $f(n) = n.1_F$, so by (5.8.4)″ M is F-representable for every field F, that is, M is regular.

Conversely suppose M is regular. Then by (2.13) there is a (0,1,-1)-matrix A such that for any field F, any F-representation of M is projectively rquivalent to A. It is now routine to check that the pair $(\mathbb{Z},A)$ satisfy the four conditions of (5.15)″.

3) Suppose M is binary. Then $V_M \approx GF(2)$ if and only if M is not regular.

Proof If $V_M \approx GF(2)$ it is immediate from (5.8.4)″ that $c(M)=\{2\}$, so M is certainly not binary.

Conversely M binary and not regular implies by (1.43) and (2.13) that every representation of M is projectively equivalent to the matrix $A = [I_r | A_B]^T$. It is now routine to check that the pair $(GF(2), A)$ satisfy (5.15)″.

We may illustrate this example in the special case when M is the Fano matroid whose planar representation is given in (5.23). The matrix D is also given in (5.23). Now M has 7 non-bases, of which only $\{3,4,5\}$, $\{1,4,6\}$, $\{2,4,7\}$, $\{5,6,7\}$ yield non-zero subdeterminants. In particular

$\det D(\{3,4,5\}) = X_1 - 1$, $\det D(\{1,4,6\}) = X_2 - 1$,

$\det D(\{2,4,7\}) = X_3 - 1$,

hence the images of X_1, X_2, X_3 in V_M are all equal to 1. We may as well assume then that

$$D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad \text{and} \quad T = \mathbb{Z}$$

in which case the only non-basis yielding a non-zero subdeterminant is $\{5,6,7\}$, and $\det D(\{5,6,7\}) = 2$.

Thus $\underline{b} = \sqrt{(2)} = (2)$, and it is easily checked that $a = 1$.

Thus $V_M = \mathbb{Z}/(2) = GF(2)$.

We also note here that if we remove the line $(5,6,7)$ from M we obtain the non-Fano matroid M' ; by the same argument as above in calculating $V_{M'}$ we may assume that D is given as above. In this case $\underline{b} = 0$ and $a = 2$ since $\{5,6,7\}$ is a non-basis, so that $V_{M'} = \mathbb{Z}_{(2)}$. By (5.8.4)″, 2 is the only prime (or zero) not in $c(M')$.

4) A weak generalisation of (5.28.3) for arbitrary finite fields is the following result . We assume $F = GF(p^m)$

<u>T.F.A.E.</u> 1) <u>M is representable only over fields isomorphic to F, and any two representations are g.p.e.</u>

2) <u>$V_M \approx F$.</u>

(Note :- by (2.13) this reduces to (5.28.3) for F=GF(2))

Proof 1) implies 2) Let A be an F-representation of M in p.c.f. Then it is clear that the pair (F,A) satisfy $(5.15)''$.

2) implies 1) is immediate from (5.24).

5) In (4.14.1) we constructed, for each prime p, matroids M, M' having respective characteristic sets $\{p\}$ and $P\backslash\{p' \leq p\}$. For either matroid, any representation is projectively equivalent to the matrix A given in the example. Using this matrix, it is routine to check (using $(5.15)''$) that

$$\underline{V}_M = \mathbb{Z}/(p) \ (=GF(p)) \quad \text{and} \quad \underline{V}_{M'} = \mathbb{Z}_{(a)} \quad \text{where}$$
$$a = \Pi\{p' \text{ prime} \leq p\}$$

6) <u>If $M = PG(r,F)$</u> (viewed as a matroid in the usual sense) <u>where F is a finite field, then $\underline{V}_M \approx F$.</u>

Proof Let A be the natural representation matrix of M described in §4. Using (4.17) it is now routine to check that the pair (M,A) satisfy the conditions of $(5.15)''$.

7) By the previous examples we have seen that $\mathbb{Z}$, $\mathbb{Z}_{(a)}$ (where a is the product of the first t primes, for any t) and <u>any finite field all occur as the Vámos rings of matroids.</u> These are of course special examples and we would like to know in general which rings can occur. A partial solution is :-

<u>If $f(X)$ is an irreducible polynomial in $\mathbb{Z}[X]$, then there is a matroid M for which</u>

$$\underline{V_M = (\mathbb{Z}[X]/(f(X)))_{(\overline{g(X)})}} \quad \text{for some } g(X) \in \mathbb{Z}[X]$$

Proof We use the same notation as (4.10)-(4.12). Let K be the quotient field of $\mathbb{Z}[X]/(f(X))$ and x the natural image of X in K. We recall that the construction of $(1,0,f(x))$ in

PG(3,K) (described in (4.12)) induces two matroids, $M_{f(x)}$ and $M'_{f(x)}$, the latter being the actual configuration of the construction (without any extra lines of PG(3,K) added). For ease of notation write $M = M'_{f(x)}$. If A is the natural matrix corresponding to the points of the construction, we have seen in (4.10) that the collinear triples force each entry of A to have the form $g_{ij}(x)$ for some $g_{ij}(X) \in \mathbb{Z}[X]$. (note that A is by construction a representation of $M_{f(x)}$ but not necessarily of M). For exactly the same reasons we may assume that the matrix D used to define V_M is precisely $D = [g_{ij}(X)]$ over $T = \mathbb{Z}[X]$. In this case all the non-bases of M have zero determinant in D except for one, namely that corresponding to the triple B, P_0, Q_1, and this has determinant f(X). Thus $\sqrt{\underline{b}} = \underline{b} = (f(X))$ (since the latter is prime) and $V_M = (\mathbb{Z}[X]/(f(X))_{\overline{g(X)}}$ where $g(X) = \Pi\{\det D(U);\ U \text{ basis of } M\}$.

By (4.13) and a similar argument this result generalises to :-

<u>Corollary</u> <u>If</u> $f_1,\ldots,f_s$ <u>is any family of polynomials in</u> $\mathbb{Z}[X_1,\ldots,X_t]$ <u>which generate an ideal</u> $\underline{b}$ <u>whose radical is prime.</u> <u>Then there is a matroid M for which</u>

$$V_M = (\mathbb{Z}[X_1,\ldots,X_t]/\sqrt{\underline{b}})_{(\bar{g})} \quad \underline{\text{for some } g} \in \mathbb{Z}[X_1,\ldots,X_t]$$

8) In every one of the preceding examples the ring V_M is an integral domain. For examples of non-domain Vámos rings we consider the matroids of (4.13.2) and (4.13.3). In both cases $|c(M)| = 2$, so the desired examples follow from (5.14). In fact using (4.10) and (5.15)'' (with the respective natural representation matrices) it is easily seen that the canonical Vámos rings of these matroids are respectively

$$(\mathbb{Z}/(1103.\ 2809))_{(\bar{a})},\quad (\mathbb{Z}/(13.19))_{(\bar{a}')}$$

where a, a' are the products of the non-zero (3×3) subdeterminants of the respective natural representation matrices.

9) We now exhibit an example of <u>a matroid M for which $|c(M)| = 1$</u> <u>and yet V_M is not a domain</u>:-

Let M_1, M_2 be copies of the matroid $PG(3,4)$. By (5.28.6) $V_{M_i} \approx GF(4)$ (for $i=1,2$). By Theorem 39 in [42], the tensor product of finite fields is a reduced ring, so $N(GF(4) \otimes_{\mathbb{Z}} GF(4)) = 0$. Thus by $(5.21)'$, if $M = M_1 \oplus M_2$ it follows that

$$V_M \approx GF(4) \otimes_{\mathbb{Z}} GF(4) \quad (\approx GF(4) \otimes_{GF(2)} GF(4)).$$

We claim that the latter is a non-domain. For, write $GF(4) = \{0,1,\varepsilon,\varepsilon^2\}$ where ε is a primitive cube root of unity. Then $\{1,\varepsilon\}$ is a basis for $GF(4)$ over $GF(2)$. Thus if we write

$$a_1 = 1\otimes 1\ , \quad a_2 = 1\otimes\varepsilon\ , \quad a_3 = \varepsilon\otimes 1\ , \quad a_4 = \varepsilon\otimes\varepsilon\ ,$$

then $\{a_1,a_2,a_3,a_4\}$ is a basis for V_M over $GF(2)$, so V_M consists of 16 elements of the the form $\sum_{i=1}^{4} \alpha_i a_i$ where $\alpha_i = 0,1$

Now write $\qquad x = a_1+ a_3+ a_4 \quad , \quad y = a_2+ a_3+ a_4$

Certainly $x, y \neq 0$. However since $\varepsilon^2+\varepsilon = 1$, and $2=0$, we have:-

$$\begin{aligned} xy &= (1\otimes\varepsilon)+(\varepsilon\otimes 1) + (\varepsilon\otimes\varepsilon) + (\varepsilon\otimes\varepsilon) + (\varepsilon^2\otimes 1) \ (\varepsilon^2\otimes\varepsilon) + \\ &\qquad (\varepsilon\otimes\varepsilon^2) + (\varepsilon^2\otimes\varepsilon) + (\varepsilon^2\otimes\varepsilon^2) \\ &= (1\otimes\varepsilon) + (\varepsilon\otimes 1) + (\varepsilon^2\otimes 1) + (\varepsilon\otimes\varepsilon^2) + (\varepsilon^2\otimes\varepsilon^2) \\ &= (1\otimes\varepsilon) + (\varepsilon\otimes 1) + (\varepsilon\otimes 1) + (1\otimes 1) + (\varepsilon\otimes 1) + (\varepsilon\otimes\varepsilon) + \\ &\qquad (1\otimes 1) + (1\otimes\varepsilon) + (\varepsilon\otimes 1) + (\varepsilon\otimes\varepsilon) \quad = 0 \end{aligned}$$

Thus V_M is a non-domain. In this example M is disconnected, but we can define a matroid M' as that being induced by the matrix

$$A = \left[\begin{array}{ccc|ccc} & & I_6 & & & \\ \hline & N & & & 0 & \\ \hline & 0 & & & N & \\ \hline 1 & 0 & 0 & 1 & 0 & 0 \end{array}\right]$$

over GF(4) where $\left[\frac{I_4}{N}\right]$ is the natural representation matrix for PG(3,4). By (1.45) M' is a connected matroid (which differs from M only by the addition of the last line of A). Since both non-zero entries in the last line are atomic it follows from (4.17) that M' is uniquely representable by the matrix A, and hence it is routine to check that the pair (V_M, A) satisfy (5.15)″ for the ring $V_{M'}$. Thus $V_{M'} \approx V_M$ which is a non-domain.

10) We now show how (5.5)″ can be used to prove that the well-known Vámos matroid is not representable. This matroid M is usually defined as the matroid on $E = \{1,\ldots,8\}$ with bases all 4-sets except $\{1,2,3,4\}$, $\{1,2,5,6\}$, $\{1,2,7,8\}$, $\{3,4,5,6\}$, $\{3,4,7,8\}$. After a suitable relabelling of the elements it will also be correct (and more convenient in our case) to assume that the non-bases are $U_1 = \{2,3,4,8\}$, $U_2 = \{1,2,7,8\}$, $U_3 = \{1,3,4,7\}$, $U_4 = \{3,4,5,6\}$, $U_5 = \{1,5,6,7\}$. With respect to the ordering $1,\ldots,8$, the matrix D becomes

$$D = \begin{bmatrix} & I_4 & & \\ \hline 1 & 1 & 1 & 1 \\ 1 & X_7 & X_1 & X_2 \\ 1 & 0 & X_3 & X_4 \\ 0 & 1 & X_5 & X_6 \end{bmatrix}$$

Now $\det D(U_4) = 1-X_7$, so the natural image of X_7 in V_M will be equal to 1. We may thus assume that $X_7 = 1$ in D and that $T = \mathbb{Z}[X_1,\ldots,X_6]$. In this case

$$\det D(U_1) = 0\ ,\ \det D(U_2) = X_3X_6 - X_4X_5\ ,\ \det D(U_3) = 0\ ,$$
$$\det D(U_4) = 0\ ,\ \det D(U_5) = X_1X_4 - X_2X_3 - X_4 + X_3$$

Write $g_1 = X_3X_6 - X_4X_5 \qquad g_2 = X_1X_4 - X_2X_3 - X_4 + X_3$

Then $\underline{b} = (g_1, g_2)$. We note that the sets $U_6 = \{1,2,4,7\}$ and $U_7 = \{2,5,6,8\}$ are bases, and

$\det D(U_6) = X_3$, $\det D(U_7) = X_1X_6 - X_2X_5 - X_6 + X_5$

But then the polynomial $g = X_3(X_1X_6 - X_2X_5 - X_6 + X_5)$ divides a. Now,

$$g = X_5g_2 + (1-X_1)g_1 \in \underline{b} \subset \sqrt{\underline{b}}$$

Thus g divides a implies $a \in \sqrt{\underline{b}}$ and by (5.5)″, M is non-representable.

Relationship to White's bracket ring

An alternative approach to reducing the representation problem to a ring-theoretical one has been made by White in [38,39,40,41]. The ring B_M (called the bracket ring) which White associates with each matroid M is a ring of generalised determinants, and which is also ,in a weaker sense than ours, a 'universal representation object for M'. We now determine a relationship between the bracket ring and the Vámos ring.

Let the matroid M on E be of rank r as usual. The bracket ring is defined in the following way :-

To every ordered r-tuple $U=(u_1,\ldots,u_r)$ of elements of E, associate a symbol $[u_1,\ldots,u_r]$, or simply $[U]$, called a bracket. Let S_M be the polynomial ring over $\mathbb{Z}$ generated by the indeterminates $\{[U];\ U \in E^r\}$. Let $\underline{a}$ be the ideal of S_M generated by all elements of the following three types

1) $[U]$, if U contains repeated elements or is dependent in M.
2) $[U] - (\operatorname{sgn}\sigma)[\sigma(U)]$ for any permutation σ of U
3) $[u_1,\ldots,u_r][v_1,\ldots,v_r] - \sum_{i=1}^{r}[v_i,u_2,\ldots,u_r][v_1,\ldots,v_{i-1},u_1,v_{i+1},\ldots,v_r]$

The syzygies are any relations in this ideal. The bracket ring B_M is now defined by $B_M = S_M/\underline{a}$.

We now suppose that $B = \{e_1,\ldots,e_r\}$ is a basis of M as usual.

Now write $\underline{a}'$ for the ideal of S_M generated by the ideal $\underline{a}$ together with the additional element $[B] - 1$, and write $B'_M = S_M/\underline{a}'$ (so if z is the natural image of the element $[B] - 1$ in B_M, then $B'_M = B_M/(z)$). If now the ring T and ideal $\underline{b}$ of T are defined as in the construction of the simplified Vámos ring R_M then the bracket ring and Vámos ring are related by :-

(5.29) Theorem With the notation above, $B'_M \approx T/\underline{b}$

Proof It suffices to find homomorphisms $\gamma: B'_M \to T/\underline{b}$ and $\psi: T/\underline{b} \to B'_M$ for which $\gamma\psi$ and $\psi\gamma$ are the identity mappings respectively on $T/\underline{b}$ and B'_M. For ease of notation we shall write i for e_i in E $(i=1,\ldots,n)$ and for $1 \leq j \leq r$, $r+1 \leq i \leq n$, U_{ij} for the r-tuple $(1,\ldots,j-1,i,j+1,\ldots,r)$. We recall that T, $\underline{b}$ are defined with respect to the matrix

$$X = \begin{bmatrix} & I_r & \\ \hline X_{r+1,1} & \cdots & X_{r+1,r} \\ \vdots & & \vdots \\ X_{n,1} & \cdots & X_{n,r} \end{bmatrix}$$

and for each $U \subset E^r$ we now define $\det X(U)$ as previously, but noting that we have to respect the ordering of U. In particular $\det X(U_{ij}) = \pm X_{ij}$.

Now let $\gamma: S_M \to T$ be the homomorphism induced by mapping $\gamma([U]) = \det X(U)$ for each bracket $[U]$. By elementary properties of determinants (including the Laplace expansion) and the definition of $\underline{b}$ in T, it follows that $\gamma(\underline{a}') \subset \underline{b}$. Thus γ induces (in the natural way) a homomorphism $\gamma: B'_M \to T/\underline{b}$.

Conversely, let $\psi: T \to S_M$ be the homomorphism induced by $\psi(X_{ij}) = U_{ij}$. This induces (via the natural homomorphism $S_M \to B'_M$) a homomorphism $\psi: T \to B'_M$. We wish to show that $\underline{b} \subset \operatorname{Ker} \psi$, and for this we will have to prove :-

$$\begin{aligned}&\text{For any } r\text{-subset } U \subset E \text{ with } |E\setminus U| = s \geq 1\\ &\psi(\det X(U)) = \pm [B]^{s-1}[U] \quad \text{in } B'_M\end{aligned} \tag{5.29.1}$$

We prove (5.29.1) by induction on s. If s=1, then $U = U_{ij}$ for some $r+1 \leq i \leq n$, $1 \leq j \leq r$, and the result is clear since $\psi(\det X(U_{ij})) = [U_{ij}]$. Next assume $s \geq 2$ and that the result holds for r-sets U' with $|B\setminus U'| < s$. Without loss of generality, assume that $U\setminus B = \{i_1,\ldots,i_s\}$ and that $B\setminus U = \{1,\ldots,s\}$ (that is, $U = \{s+1,\ldots,r, i_1,\ldots,i_s\}$). Then expanding along the first row we get

$\det X(U) =$

$$\begin{vmatrix} X_{i_1 1} \cdots X_{i_1 s} \\ \vdots \\ X_{i_s 1} \cdots X_{i_s s}\end{vmatrix} = X_{i_1 1}\cdot \begin{vmatrix} X_{i_2 2} \cdots X_{i_2 s} \\ \vdots \quad\quad \vdots \\ X_{i_s 2} \cdots X_{i_s s}\end{vmatrix} - X_{i_2 2}\cdot\begin{vmatrix} X_{i_2 1} & X_{i_2 3}\cdots X_{i_2 s} \\ \vdots & \vdots \\ X_{i_s 1} & X_{i_s 3}\cdots X_{i_s s}\end{vmatrix}$$

$$\cdots + (-1)^{s-1} X_{i_1 s}\cdot \begin{vmatrix} X_{i_2 1} \cdots X_{i_s s-1} \\ \vdots \quad\quad \vdots \\ X_{i_s 1} \cdots X_{i_s s-1}\end{vmatrix} \tag{5.29.2}$$

But by the inductive hypothesis, for each $j=1,\ldots,s$,

$$\psi\left(\begin{vmatrix} X_{i_2 1} \cdots X_{i_2 j-1} & X_{i_2 j+1} \cdots X_{i_2 s} \\ \vdots & \vdots \\ X_{i_s 1} \cdots X_{i_s j-1} & X_{i_s j+1} \cdots X_{i_s s}\end{vmatrix}\right) = [B]^{s-2}[j,s+1,\ldots,r,\ i_2,\ldots,i_s]$$

Thus, if we apply ψ to (5.29.2) we obtain

$$\begin{aligned}\psi(\det X(U)) = [B]^{s-2}\big(&[U_{i_1 1}][1,s+1,\ldots,r,i_2,\ldots,i_s] \cdots \\ &\cdots + (-1)^{s-1}[U_{i_1 s}][s,s+1,\ldots,r,i_2,\ldots,i_s]\big)\end{aligned} \tag{5.29.3}$$

Now, because of the syzygies of type (3) in $\underline{a}$, it follows that in B'_M ,

$$\begin{aligned}[B][U] = [1,\ldots,r][i_1,s+1,\ldots,r,\ i_2,\ldots i_s] &= \\ &[i_1,2,\ldots,r][1,s+1,\ldots,r,i_2,\ldots,i_s] \\ &+ [1,i_1,3,\ldots,r][2,s+1,\ldots,r,i_2,\ldots,i_s] + \cdots \\ &\cdots + [1,\ldots,s-1,i_1,s+1,\ldots,r][s,s+1,\ldots,r,i_2,\ldots,i_s]\end{aligned}$$

Now, because of the syzygies of type (2) in $\underline{a}$, it follows that (up to sign) in B'_M, $[B][U]$ is equal to the expression in brackets in (5.29.3). Thus, up to sign,

$$\psi(\det X(U)) = [B]^{s-2}([B][U]) = [B]^{s-1}[U]$$

which proves (5.29.1) by induction.

So if now U is a non-basis of M, it follows from the syzygies of type (1) in $\underline{a}$, that $[U] = 0$ in B'_M and hence by (5.29.1) that $\psi(\det(U)) = 0$ in B'_M. Thus $\underline{b} \subset \operatorname{Ker}\psi$ and ψ induces a homomorphism $\psi: T/\underline{b} \to B'_M$ in the natural way.

Finally we have to show that the mappings γ, ψ defined above satisfy $\gamma\psi = id_{T/\underline{b}}$ and $\psi\gamma = id_{B'_M}$:-

Certainly $\gamma\psi(X_{ij}) = \gamma([U_{ij}]) = X_{ij}$ and since T is generated over $\mathbb{Z}$ by the indeterminates X_{ij} it follows that $\gamma\psi = id_{T/\underline{b}}$

Conversely B'_M is generated over $\mathbb{Z}$ by the brackets $[U]$, and by (5.29.1) we have,

$$\psi\gamma([U]) = \psi(\det X(U)) = [B]^{s-1}[U]$$

But, in B'_M, $[B] = 1$ (since $[B] - 1 \in \underline{a}'$), and so $\psi\gamma([U]) = [U]$ in B'_M and $\psi\gamma = id_{B'_M}$ as required.

BIBLIOGRAPHY

[1] Aigner,M. : 'Combinatorial Theory' Springer Verlag, 1979.

[2] Attiyah,M.F. and McDonald I.G. : 'Introduction to Commutative Algebra' Addison Wesley, 1969.

[3] Bear,R. : 'Linear Algebra and Projective geometry' Academic Press Inc., N.Y., 1952.

[4] Bixby,R.E. : On Reid's Characterization of the Ternary Matroids, J.Comb. Theory Ser B. 26 (1979) 174-204.

[5] Bondy,J.A. : Transversal matroids, base orderable matroids and graphs, Quart.J.Math (Oxford) 23 (1972) 81-89.

[6] Bondy,J.A. and Welsh,D.J.A. : Some results on transversal matroids and constructions for identically self-dual matroids, Quart.J.Math (Oxford) 22 (1971) 435-451.

[7] Bose,R.C. : Mathematical theory of the symmetrical factorial design, Sankhyā 8 (1947) 107-166.

[8] Bourbaki,N : 'Commutative Algebra' Addison Wesley

[9] Brualdi,R. : On Fundamental Transversal matroids, Proc.Amer.Math.Soc. 45 (1974) 151-156.

[10] Bryant V. and Perfect H. : ,'Independence Theory in Combinatorics' Chapman and Hall, 1980.

[11] Brylawski,T.H.: A note on Tutte's Unimodular Representation Theorem, Trans.Amer.Math.Soc. 171 (1975) 499-502.

[12] Brylawski,T.H. and Lucas D. : 'Uniquely Representable Combinatorial Geometries' in Proc.Internat.Colloq. on Comb. Theory, Rome, Italy, 1973, 83-104.

[13] Casse,L.R.A. : A solution to Segre's 'Problem $I_{r,q}$' for q even, Atti. Accad.Naz. Lincei Rend. 46 (1969) 13-20.

[14] Cohn,P.M. : 'Algebra', Vols. I,II, J.Wiley and Sons Ltd.,1977.

[15] Crapo,H. and Rota G-C. : 'Combinatorial Geometries', M.I.T. Press, Cambridge, Mass., 1970.

[16] De Sousa,J. and Welsh,D.J.A. : A characterization of binary transversal matroids, J.Math Analysis Appl. 40(1) 1972, 55-59.

[17] Harary,F : 'Graph Theory', Addison Wesley ,1969.

[18] Hirschfeld,J.W.P. : 'Projective Geometries over finite fields', Vol I , Oxford Univ. Press, 1979.

[19] Hirschfeld,J.W.P. : 'Projective Geometries over finite fields', Vol II, to appear.

[20] Ingleton,A.W. : Representations of Matroids, in 'Combinatorial Mathematics and its Applications',149-167, Academic Press,1971.

[21] Ingleton,A.W. : Matroids with two characteristics, preprint,1981.

[22] Krempa,J. : Isomorphic Group Rings with non-isomorphic commutative coefficients, preprint 1980.

[23] Mason,J.H. : 'Matroids as the study of Geometrical Configurations', in Higher Combinatorics, D.Reidel Publishing Co., Dordrecht, Holland, 1977, 333-376.

[24] Mihalek,R.J. : 'Projective Geometry and Algebraic structures', Academic Press, 1970.

[25] Pedoe,D. : 'An Introduction to Projective Geometry', Pergamon Press, 1963.

[26] Qvist B. : Some remarks concerning curves of the second degree in a finite plane, Ann.Accad. Sci. Fenn. Ser A 134 ,1952.

[27] Rowen,L.H. : 'Polynomial Identities in Ring Theory', Academic Press, 1980.

[28] Segre B. : Curve razionali normali e k-archi negli spazi finiti, Ann. Mat. Pura 39, 1955, 357-379.

[29] Sehgal,S.K: 'Topics in Group Rings', Marcel Dekker, 1978.

[30] Seymour,P.D. : Matroid representation over GF(3), J.Comb. Theory Ser.B 26(2),1979, 159-173.

[31] Thas,J.A. : Normal rational curves and k-arcs in Galois spaces, Rend. Mat. 1 ,1968, 331-334.

[32] Thas,J.A. : Connection between the Grassmannian $G_{k-1,n}$ and the set of k-arcs of the Galois space $S_{n,q}$, Rend.Mat.2,1969,121-134.

[33] Thas,J.A. : Normal rational curves and (q+2)-arcs in a Galois space $S_{q-2,q}$ $(q=2^n)$, Atti.Accad. Naz. Lincei Rend.49,1969,249-252.

[34] Tutte,W.T. : Lectures on Matroids, J.Res. Nat. Bur. Standards Sect.B 69, 1965.

[35] Vámos,P. : A necessary and sufficient condition for a matroid to be linear, Mobius Algebras (Proc. Conf. Univ. Waterloo, Ont.,1971) 162-169.

[36] Vámos,P. : Linearity of matroids over division rings, preprint.

[37] Welsh,D.J.A. : 'Matroid Theory', Academic Press, 1976.

[38] White,N.L. : The bracket ring of a combinatorial geometry I, Trans. Amer. Math. Soc. 202, 1975, 79-95.

[39] White,N.L. : The bracket ring of a combinatorial geometry II, Trans. Amer. Math. Soc. 214, 1975, 233-248.

[40] White,N.L. : The basis Monomial ring of a matroid, Advances in Math. 24(3), 1977, 292-297.

[41] White,N.L. : The transcendence degree of a coordinatization of a Combinatorial Geometry, J.Comb.Theory,B 29(2),1980, 168-175.

[42] Zariski and Samuel : 'Commutative Algebra', Vol.I, Van Nostrand, Princeton, N.J. ,1957.