*On leave from Centre National de la Recherche Scientifique.

**This research was partially supported by the National Science Foundation, Grant # GP-42325.

STABLE MODULES **

by

P. Camion*

Department of Statistics
University of North Carolina at Chapel Hill

Institute of Statistics Mimeo Series No. 921
May, 1974

1. Stable modules. Definition and main properties

1.1 Subsets of an R-module G verifying four axioms

Let G be an R-module where R is any commutative ring. Let S be a stable set $SS \subset S$ of nonzero divisors of R, containing -1 and verifying the prefix condition, i.e. $ab \in S \;\&\; b \in S, \Rightarrow a \in S$. Finally let A be a set of subsets of G verifying

I_1: $X \in A \Rightarrow \alpha X \in A \;, \forall\; \alpha \in S$

I_2: $X \in A \;\&\; Y \in A \Rightarrow X + Y \in A$

I_3: $x \in X \;\&\; X \in A \Rightarrow \{x\} \in A$.

I_4: Let F be any finite subset of A, then

$$\bigcap_{X \in F} X = \phi \Rightarrow \exists\; X,Z \in F \text{ with } X \cap Z = \phi \;.$$

I_4 is referred to as the "finite intersection property", or briefly f.i.p.

1.2 Examples

1.2.1 Examples in ordered modules

These examples are recalled from [1] without proofs. G is an R-module (we suppose $\lambda g = 0 \;\forall\; g \in G \Rightarrow \lambda = 0$). If the subjacent group of G is ordered with P as set of positives and if R is an ordered ring with Q as set of positives, we say that G is an ordered S-module if $QP \subset P$. For these examples R will be the group of units of R which will be a totally ordered ring. So, for every $\alpha \in S$, αP equals P or $-P$ according to the fact that α is in Q or in $-Q$.

1.2.1.1 The set A of intervals with the form $[g',g'']$, $[-\infty,g]$, $[g, +\infty]$, $R = [-\infty, +\infty]$ verifies I_i , $i = 1,2,3,4$. Where, by definition, $[g',g''] = (g' + P) \cap (g'' - P)$.

1.2.1.2. If G is totally ordered, A can be the set of *all intervals* in G:

$X \in A$ iff $\forall\, x,y,z \in G$, $x \leq y \leq z$, and $x,z \in X$, then $y \in X$.

1.2.2. Example in modules over Prüfer domains

A is the set of all cosets of all submodules of G with the form hG, where h is a finitely generated ideal of a Prüfer domain R . Here $S = R\setminus\{0\}$ We suppose $G \xrightarrow{\alpha} \alpha G$ is an injective mapping for every $\alpha \neq 0$.

I_1: $X = x + hG$; $\alpha X = \alpha x + \alpha hG = \alpha x + h'G$

I_2: $X = x + hG$; $Y = y + h'G$, $X + Y = x + y + (h + h')G$,

since $(h + h')G \supset hG$, $h'G$ and thus $(h + h')\, G = hG + h'G$

I_3: $\forall\ x \in G$, $\{x\} = x + \{o\} \in A$.

I_4: This is a consequence of Theorem 6 of [2] of which we state a corollar that we need here. *Consider a distributive lattice, under addition and intersection, of subgroups of an additive group G . If A is the set of all cosets of these subgroups, it has the f.i.p.*

So, all we have to verify is that the submodules h G , where h runs over all finitely generated ideals of R form a distributive lattice. We solve this exercise in order that this paper be self contained.

Since every ideal ℓ in a Priifer ring has an inverse $\overline{\ell}$, that is, $\overline{\ell}\ell = (\alpha)$, principal ideal, one has:

(1) $\ell hG = \ell h'G \Rightarrow \alpha hG = \alpha h'G \Rightarrow hG = h'G$

and

(2) $\ell hG \supset \ell h'G \Rightarrow hG \supset h'G$.

We have obviously

(3) $hG \cap h'G \supset (h \cap h')G$,

and we must prove equality of the two members of (3). Since $h \supset h \cap h'$, there exist ideals ℓ and k , in S such that

(4) $\ell h = h \cap h'$

$kh' = h \cap h'$.

But

$$hh' = (h \cap h')(h + h') = (h \cap h')h + (h \cap h')h'$$

$$= kh'h + \ell hh' = (k + \ell)hh' .$$

Thus

(5) $k + \ell = R$.

Now

(6) $\ell(hG \cap h'G) = \ell hG \cap \ell h'G \subset (h \cap h')G$

(7) $k(hG \cap h'G) = khG \cap kh'G \subset (h \cap h')G$

By summing (6) and (7) and applying (5):

(8) $hG \cap h'G \subset (h \cap h')G$.

From (3) and (8), we have equality of both sides.

We have proved that the considered modules form a sublattice of the lattice of submodules of G . We have now to check out the law of distributivity, which, as we know it, holds for the lattice of finitely generated ideals of a Prüfer ring (See [3] for a proof without the use of maximal ideals).

$$hG \cap (h'G + h''G) = hG \cap (h' + h'')G$$

$$= (h \cap (h' + h''))G = (h \cap h' + h \cap h'')G$$

$$= (h \cap h')G + (h \cap h'')G = hG \cap h'G + hG \cap h''G \ .$$

1.3 Definition and main properties of stable modules

1.3.1 Totally S-stable-matrix

We suppose that the R-module G verifies

$$\phi_\alpha : G \to \alpha G \tag{9}$$

is an injective mapping for every $\alpha \in S$. This is true, for example for G a subgroup of R^E , E being any set, since we have supposed all $\alpha \in S$ were non-zero divisors.

Definition. An $n \times m$ matrix A with entries in R is called *totally S-stable* if every non-zero subdeterminant of A is in S .

The G-rank of any matrix B is, by McCoy's definition, slightly extended in [2], the largest integer r such that there is no g in G annihilating all $r \times r$ subdeterminants of B . Here, clearly, the rank of A is the largest r for which one $r \times r$ subdeterminant of A is not zero.

1.3.2. Primitive elements in R^m, S-stable-modules

The rows of A span a submodule of R^m . R^m may be considered the module of functions with domain $[1,m]$ and range R . So, we call *support* $s(x)$ of $x \in R^m$:

$$s(x) = \{ j / j \in [1,m] \ , \ s_j \neq 0 \} \ . \tag{10}$$

We consider the finite set S of minimal supports:

(11) $s(x) \in S$ for $x \in M$ iff $\forall\, y \in M, (s(y) \subset s(x) \;\&\; y \neq 0) \Rightarrow s(y) = s(x)$.

1.3.2.1. Definition We first consider submodules of R^m .

A submodule M of R^m is S-stable when for every minimal support $s(x)$ of S there exists a $u \in M$ with every non-zero componant in S such that $s(u) = s($

We call such u a *primitive* of M . A special case is the one where S is the group of units of R . *We called those modules "unimodular modules".* Since S is a stable set of non-zero divisors, it is clear that if $\bar{R}$ is the ring of fractions of R with denominators in S , then a S-stable module is unimodular over $\bar{R}$. But the converse is not true, that is if $\bar{M}$ is unimodular in R^m , the R-module $\bar{M} \cap R^m$ is not necessarily S-stable in R^m . S contai -1 (thus 1) by definition, but it does not necessarily contain all units of R. The following theorem has been proved for unimodular module [1] , that is for S the group of units of R .

1.3.2.2. Theorem 1

The orthogonal module $M^\perp$ of M in the dual of R^m is itself S-stable.

Before going to the proof, let us observe on an example what is the meaning of the theorem. Take $R = \mathbb{Z}^m$, the ring of rational integers, and let M be a direct factor of $\mathbb{Z}^m$. For each minimal support in M we have one (since M is a direct factor) and only one primitive with greatest common divisor of all non-zero componants equal to 1 . (For if u and v are such primitives and $u_i \neq 0$, then $v_i u - u_i v = 0$. v_i divises $u_i v_j$ for every $v_j \neq 0$ and must divise u_i . Also $u_i | v_i$ and $u_i = v_i$.) Hence there is a finite number of su primitives and their non-zero componants generate with -1 and their divisors a stable set S . Now the theorem teaches us that for every minimal

support in $M^{\perp}$, there exists a $u \in M^{\perp}$ having this support with all non-zero componants in S. If $s(u) = s(v)$ and $\sum_{1 \le j \le m} (v_j) = \mathbb{Z}$, then v_j divides some element in S, and is consequently in S, by the prefix condition.

1.3.2.3. Numerical example

Primitives in M	Primitives in $M^{\perp}$
(0,6,7,-5)	(0,13,-9,3)
(3,0,2,6)	(52,0,-15,-21)
(-21,12,0,-52)	(12,-5,0,-6)
(15,36,52,0)	(4,7,-6,0)

We see that every integer in the first array divises a product in the second array and conversely:

1.3.2.4. Proof of Theorem 1.

It is sufficient to prove Theorem 1 in the case where S is a group. For, if S is not a group let $\overline{R}$ be the ring of fractions of R with denominators in S. The set of elements α/β with $\alpha, \beta \in S$ form a multiplicative group $\overline{S}$ in $\overline{R}$. If M is S-stable then $\overline{M} = \overline{R}M$ is $\overline{S}$-stable and the orthogonal $\overline{M}^{\perp}$ of $\overline{M}$ is $\overline{S}$-stable. Now $\overline{M}^{\perp} \cap R^m \subset M^{\perp}$ and if $x \in M^{\perp}$ and $y \in \overline{M}$, there exists a non-zero divisor α such that $\alpha y \in M$, so

$$\alpha \langle x,y \rangle = \langle x, \alpha y \rangle = 0$$

and $\langle x,y \rangle = 0$, thus $x \in \overline{M}^{\perp}$, $M^{\perp} = \overline{M}^{\perp} \cap R^m$; $\overline{M}^{\perp} = \overline{\overline{R}M}^{\perp}$. If x has minimal support in $M^{\perp}$, it has also minimal support in $\overline{M}^{\perp}$ since to every y in $\overline{M}^{\perp}$ correspond an αy in M with $s(y) = s(\alpha y)$. Thus there exists a

$u \in \overline{M}^{\perp}$, $s(u) = s(x)$, with all non-zero componants in $\overline{S}$. The product α of all denominators of u_j , $j \in \{1, \ldots, m\}$ is in S as well as every numerator of the u_j , by the prefix condition. Hence $\alpha u \in M^{\perp}$ has all non-zero componants in S . This will achieve the proof.

Notations and definitions.

An $n \times m$ matrix has its rows labeled by the ordered set $[1,n]$ and its columns labeled by the ordered set $[1,m]$. A_I^J is the submatrix of A whose rows are labeled by the ordered subset I of $[1,n]$ and whose columns are labeled by the ordered subset J of $[1,m]$. An *echelon matrix* A is an $n \times m$ matrix with A^J the identity matrix for some $J \subset [1,m]$. For the following Properties 1,2,3,4,5,6, S will be a subgroup of the group of units of R ccntaining -1 .

Property 1. *Let A be an $n \times m$ matrix, totally S-stable (i.e. every non-zero subdeterminant is in S). If A^J is a non-singular $n \times m$ submatrix of A , then $(A^J)^{-1}A$ is a totally S-stable echelon matrix.*

$(A^J)^{-1}A^J = I$, so $B = (A^J)^{-1}A$ is an echelon matrix. If B_L^K is any square submatrix of B , there exists a $J' \subset J$ such that $\text{Det } B^{J' \cup K} = \pm \text{Det } B_L^K$ But $\text{Det } B^{J' \cup K} = \text{Det } (A^J)^{-1} \text{Det } A^{J' \cup K}$. Since $-1 \in S$, $\text{Det } B_L^K \in S$.

Property 2. *If an S-stable-module M is spanned by the rows of an echelon matrix B , with B^J the identity matrix, then any non-empty support $s(x)$, $x \in M$, meets J and any row of B has minimal support.*

$s(x)$ meets J , obviously. Let b be a row of B and $s(y) \subset s(b)$ for some non-zero $y \in M$. By hypothesis there exists a primitive $u \in M$ with $s(u) \subset s(y) \subset s(b)$. Necessarily $u = \alpha b$ for some $\alpha \in S$ and since α is not a zero divisor $s(u) = s(b)$.

Property 3. *If x has minimal support in an S-stable module M and if one of its componants is in S, every non-zero componant of x is in S.*

By definition there exists a $u \in M$ with $s(u) = s(x)$ and $u_j \in S \cup \{o\}$, $\forall\, j \in [1,m]$. Let $x_s \in S$, then $x - x_s u_s^{-1} u = 0$, and $x_j = x_s u_s^{-1} u_j \in S \cup \{o\}$, $\forall\, j \in [1,m]$.

Property 4. *Let B be an echelon matrix with a maximum number of rows, all of them in a S-stable module M. Then these rows form a basis of M.*

Let $B^J = I$ and let x be any element in M. If $tB^J = x_j$, $s(tB - x) \subset \overline{J} = [1,m]/J$. Now $s(tB - x)$ is empty. For, if it were not, there would exist a $u \in M$ with $u_j = 1$ for some $j \in \overline{J}$. Replacing every row b of B by $b - b_j u$, B would be replaced by an echelon matrix which could be extended to an echelon matrix with u. This is impossible.

Property 5. *The matrix B of Property 4 is totally S-stable.*

By the argument of proof of Property 1, it suffices to show that every square non-singular B^J has determinant in S. Let $A = (B^K)^{-1}B$ with $\mathrm{Det}B^K \in S$, where B^K has the largest possible numbers of columns in B^J. A is an echelon matrix and by 4,2 and 3, every entry of A is in S. Suppose $J\backslash K \neq \phi$ and let $j \in J\backslash K$. Now there must be a $k \in K\backslash J$ and let $A^k = \ell_i$, the i^{th} unit vector. If $A_i^j \neq 0$ we replace, in the identity matrix, the i^{th} column by A^j, obtaining a matrix T with $\mathrm{Det}\, T \in S$. Denote by L the set $\{j\} \cup K\backslash\{k\}$. Then A^L has determinant in S. But $A^L = (B^K)^{-1}B^L$. This shows B^L has determinant in S which is impossible since B^L has one more column that B^K in B^J. Hence $A_i^j = 0$ for every $j \in J/K$. But $A_i^j = 0\ \forall\, j \in J \cap K$. This means A^J is singular and since $A^J = (B^K)^{-1}B^J$, this is impossible.

Property 6. *If M is a submodule of R^m spanned by the rows of a totally S-stable matrix A, every x in M with minimal support is homothetic to a row of some echelon matrix B whose rows span M. To every $x_j \neq 0$ corresponds such a B with $s(x) \cap J = \{j\}$, where B^J is the identity matrix. M is an S-stable module.*

Consider an $x \in M$ with minimal support $s(x)$. Now we may suppose A is $n \times m$ with rank n and let $\text{Det } A^J \neq 0$ such that $\text{Card}(J \cap s(x))$ is minimum. Let $k \in J \cap s(x)$. Then $B^k = (A^J)^{-1}A^k = \ell_i$, the i^{th} unit vector. Now we show that $B_i^j = 0 \ \forall\ j \in \overline{s(x)} = [1,m]/s(x)$. If $B_i^j \neq 0$ we could build up an invertible matrix T by changing ℓ_i to B^j in the unit matrix. If $K = \{j\} \cup J/\{k\}$, $B^K = (A^J)^{-1}A^K$ would then be invertible and so would be A^K with $\text{Card}(K \cap s(x)) < \text{Card}(J \cap s(x))$ which is impossible. Then $s(B_i) \subset s(x)$ and $x = \alpha B_i$. Finally since B_i belongs to M and $B_i^j \in S$, $\forall\ j \in \{1, \ldots, m\}$, $u = B_i$ is a primitive with $s(u) = s(x)$. We observe that J may have been chosen in order that $J \cap s(x) = \{j\}$ for any j with $x_j \neq 0$.

In conclusion, if M is S-stable, there exists a totally S-stable matrix, let us say, $[I,A]$ whose rows span M. Then $[A^T,-I]$, which is itself totally S-stable, span $M^\perp$. By Property 6, $M^\perp$ is then S-stable, which was to be proved.

1.3.2.5. Some consequences

Remark. It is easy to verify that if a S-stable module M is a direct factor of R^m (S being now a general stable semi-group of non-zero divisors with the prefix property) then $(M^\perp)^\perp = M$. Also if R is a principal ideal ring and if $(M^\perp)^\perp = M$, then M is a direct factor of R^m. Notice that if M has a basis, it may not have a basis of primitives. We also have

Corollary 1. *If a module M is spanned by the rows of an $n \times m$ matrix A with rank n, a sufficient condition that it be S-stable is that Det $A^J \in S$, for every $n \times m$ matrix A^J.*

With the notations of 1.3.2.4, Det A^J is invertible in $\bar{S}$. Then $(A^J)^{-1}A$ has all its entries in $\bar{S}$ and, moreover, it totally $\bar{S}$-stable. Now by Property 6 every x with minimal support will be found proportional to some row of some $(A^J)^{-1}A$. Multiplying this row by Det A^J, we find a primitive with componants in S.

Corollary 2. *Let $\bar{M} = \bar{R}M$ with $\bar{M}, \bar{R}$ defined as in 1.3.2.4 and, denote again by $\bar{S}$ the group generated by S in $\bar{R}$. Then M is S-stable iff $\bar{M}$ is spanned by the rows of an $n \times m$ matrix A with rank n and with Det $A^J \in \bar{S}$ for every non-singular $n \times m$ A^J.*

By Properties 4,5, if $\bar{M}$ is stable such a basis always exists. By Corollary 1 the converse is true. Finally we have seen in 1.3.2.4 that M is S-stable iff $\bar{M} = \bar{R}M$ is $\bar{S}$-stable.

Corollary 3. *To every S-stable module M of Z^m, where S is the set of odd integers corresponds a unimodular module.*

Let the rows of A be a basis of M. Let us first show that (Det $A^J \in (2) \Rightarrow$ Det $A^J = 0$). Suppose Det A^J is even. Then among all possible linear combinations tA^J such that $s(tA^J)$ reduces to one element there must be one such that the only componant of tA^J is even with $\sum_{1 \le i \le n} (t_i) = \mathbb{Z}$. But then tA is a primitive, by Property 2 and since the greatest common divisor of its componants divides that one of any other primitive with the same support, M would not be S-stable. Now consider A modulo 4. For some invertible

$A^J,_B=(A^J)^{-1}A$ has all its subdeterminants 1,-1 or zero mod 4. Consider now that matrix B as a matrix over the integers. Every subdeterminant is 0,1 or -1 mod 4. But it is known that an echelon matrix with entries 0,1,-1 cannot have a subdeterminant greater than 1 without having another equal to ±2 .* Hence the obtained matrix is totally unimodular and its rows span a unimodular Z-module.

1.3.2. A more general definition for stable modules

Definition. A submodule of G^m , where G , defined in 1.3.1, is an R-module, is S-stable if it is the smallest submodule of G^m containing $xg = (x_j g)_{1\leq j\leq m}$ for every g in G and for every x in a S-stable submodule M of R^m . Such a module is denoted by (M . G) . The *primitives* of (M . G) will be, by definition the primitives of M .

By 1.3 (9) , if u is a primitive of M , s(u) = s(ug) for every non-zero g in G .

Representatives. A set of representatives is a finite set of primitives of (M . G) , one for every minimal support.

Property 7. *If x has minimal support in (M . G) , $\exists a \in S$ such that $ax = ug$ for a primitive u and some $g \in G$.*

Let A be an echelon matrix, totally $\bar{S}$-stable and whose rows span $\bar{M}$ over $\bar{R}$. We choose it in order that $A^J = I$ for a set J with Card(J ($\bar{}$) s(x minimum. We know that there exists an echelon matrix B with $B^{\bar{J}} = I$, $\bar{J} = [1,m]/J$, whose rows span $\bar{M}^{\perp}$ over $\bar{S}$. x being orthogonal to each row

*This property is not verified if all entries are not in {0,1,-1} . A totally unimodular matrix in which 4 is added to any entry is a counterexample. (See for example [4].)

of B , it is impossible that $s(x) \subset \overline{J}$. Let $j \in s(x) \cap J$. By the argument used for the proof of Property 6, the row A_i of A with $A_i^j = 1$ has its support contained in $s(x)$ and it follows from hypothesis that $s(A_i) = s(x)$. Now $x - A_i x_j$ has its support contained in $\overline{J}$. Thus $x - A_i x_j = 0$. Multiplying by suitable $\alpha \in S$, we find $\alpha x = ug$ with $u = \alpha A_i \in M$ and $g \in G$.

Property 8. *Let $(M.G)$ be an S-stable module and U a set of representatives of $(M.G)$. Then to every $x \in (M.G)$ corresponds a $\beta \in S$ such that*

$$\beta x = \sum_{u \in U} u g_u \ , \ g_u \in G \ , \ g_u = 0 \ \text{ if } \ s(u) \not\subset s(x) \ , \ \forall \ u \in U \ .$$

Write $y = \beta x - \sum_{u \in U} u g_u$, choosing β in S and $g_u \neq 0$ only if $s(u) \subset s(x$ and such that $s(y)$ be minimal. We show $s(y) = \phi$, that is, $y = 0$. Suppose $s(y) \neq \phi$. Then, by Property 7, there exists a $v \in U$ with $s(v) \subset s(y)$. Le $v_j \neq 0$. Then $s(v_j y - v y_j)$ is properly contained in $s(y)$. But this is impossible, since

$$v_j \beta x - \sum_{u \in U} u v_j g_u - v y_j = \beta' x - \sum_{u \in U} u g'_u \ ,$$

with $\beta' \in S$ and $g'_u \in G$, $\forall \ u \in U$.

Let K be any subset of $[1,m]$, and $\overline{K} = [1,m] \backslash K$. The projection $\Pi_{\overline{K}}$ of G^m onto $G^{\overline{K}}$ is the linear mapping $x \rightsquigarrow x^{\overline{K}}$, where the componants of $x^{\overline{K}}$ are labeled in $\overline{K}$ and $x_j^{\overline{K}} = x_j$, $\forall \ j \in \overline{K}$. We denote by the same symbol $\Pi_{\overline{K}}$ the restriction of $\Pi_{\overline{K}}$ at M , submodule of G^m . $\mathrm{Ker}\Pi_{\overline{K}}$ is then the submodule of all x in M with $x_j = 0$, $\forall \ j \in \overline{K}$. We denote by Δ_K the operator $\mathrm{Ker}\Pi_{\overline{K}}$: we suppose now *S is a group.*

Property 9. *For every subset K of $[1,m]$, $\Delta_K(M.G)$ is an S-stable module i. M is S-stable. If U is a set of representatives of M , then $U \cap \Delta_K M$ is*

a set of representatives of $\Delta_K(M.G)$.

We have $((\Delta_K M).G) \subset \Delta_K(M.G)$. Now by Property 8, since $\beta^{-1}u \in \Delta_K M$ if $u \in \Delta_K M$, the converse inclusion is verified. The last assertion follows.

Remark. If M is a S-stable module of R^m , it is clear that $\Delta_K M$ is also a S-stable module. Now we have

Property 10. *If* R *is a principal ideal ring,* $\Delta_K M$ *is a direct factor of* M *for every* $K \subset [1,m]$ *iff* M *is a direct factor of* R^m . *Every* x *in* M *is a linear combination of primitives with supports contained in* $s(x)$ *if* M *is a direct factor of* R^m .

If R is a principal ideal ring, it is true that M is a direct factor if $\alpha x \in M$, $\alpha \in S \Rightarrow x \in M$. For, if $M \oplus N = R^m$ and p is a projector of R^m onto M , $p(x) \in M$, $(1-p)(x) \in N$. But $0 = (1 - p)(\alpha x) = \alpha(1-p)(x)$. Since α is not a zero divisor, $x = p(x) \in M$.

Now the condition is sufficient since it means that the invariant factors of M are all equal to (1) and this means M is a direct factor.

Now if $\alpha x \in \Delta_K M$, since $s(x) \subset s(\alpha x)$, α being a non-zero divisor, $x \in \Delta_K M$ and consequently, $\Delta_K M$ is a direct factor.

Before proving the last assertion, we first observe that it may not be true if M were not a direct factor.

Example:

$$(1,1,5)$$

$$(1,-1,3)$$

If M is the module over $\mathbb{Z}$ spanned by those two elements, its primitives are scalar multiples of $(2,0,8),(0,2,2)$ and $(2,-8,0)$, then obviously the primitives span a proper submodule of M .

We prove the last assertion by recurrence on the cardinality of $s(x)$. If the rows of A form a basis of $\Delta_{s(x)}M$ we built up a set U , one $u \in U$ for each minimal support, as follows. To every $k \times k$ matrix A^J corresponds an adjoint $(A^J)^*$ and the rows of $(A^J)^*A = B$ have minimal supports. U will be the union of the rows of such B's . Notice that every componant of a row of a B is the determinant of some A^J and that every $\mathrm{Det}A^J$ appears as a componant of some element in U .

Now let $U^{(j)}$ be the subset of $u \in U$ with $u_j \neq 0$. Denote by y the element $u_j x - x_j u$ of $\Delta_{s(x)}M$. $y_j = 0$ and so $s(y)$ is properly contained in $s(x)$. By recurrence, $y = \sum_{u\in U} \alpha_u u$, and $u_j x = \sum_{u\in U} \alpha'_u u$. Let β_j be the greatest common divisor of the u_j , u running over $U^{(j)}$. Then

$\beta_j x = \sum_{u\in U} \beta_u u$. Now $\sum_{j\in s(x)} (\beta_j) = R$ since, as we have just seen,

$\sum_{j\in s(x)} (\beta_j) = \sum_{\mathrm{Card}J=k} (\mathrm{Det}\, A^J)$ and $\Delta_{s(x)}M$ is a direct factor of R^m . Hence, by suitable linear combination of the $\beta_j x$, $j \in s(x)$, we get the result.

Proposition 1. *Let R be a Dedekind domain and let M be a direct factor of R^m . Then every x in M is a linear combination of primitives with supports contained in $s(x)$.*

We denote by p a maximal ideal of R . We make $K = s(x)$ and we denote $\Delta_K M$ by M' . R_p, M_p, M'_p will denote respectively the localization of R, M, M' at p . Let P be the set of maximal ideals of R . If u is a primitive in M' , u has minimal support in M'_p and thus conversely, if $u^{(p)}$ has minimal support in M'_p , for every $\alpha \notin p$ such that $\alpha u^{(p)} \in M'$, $\alpha u^{(p)}$ is a primitive in M' . Now R_p is a principal ideal ring and by Property 10 we can write for every $p \in P$

(12) $$\frac{x}{I} = \sum \alpha_u^{(p)} u^{(p)}$$

where $\alpha_u^{(p)} \neq 0$ implies $u^{(p)}$ is in M'_p and has minimal support. Then there exists a $\gamma^{(p)} \notin p$ such that $\gamma^{(p)} u^{(p)}$ is a primitive of M' for every $\alpha_u^{(p)} \neq 0$, and we know that we can find a finite set E of $p \in P$ such that

(13) $$\sum_{p \in E} \gamma^{(p)} \delta^{(p)} = 1$$

with suitable $\delta^{(p)} \in R$. Consequently (12) and (13) will entail in R^m

(14) $$x = \sum_{p \in E} \sum \delta^{(p)} \alpha_u^{(p)} \gamma^{(p)} u^{(p)}$$

where all $\gamma^{(p)} u^{(p)}$ are primitives in M' with supports in $s(x)$.

1.4 The particular case of unimodular modules

Unimodular modules defined in [1] appear as a particular case for S-stable modules, that is the case where S is the whole group of units of R. A conversation with L. Geissinger during seminar lectures on unimodular modules at th University of North Carolina lead us to do the following characterization of unimodular R-modules, for R a domain. Let Π_K be the mapping $x \rightsquigarrow (x_j)_{j \in K}$, $\forall\, x \in M$.

Theorem 2. *A submodule M of R^m, R a domain, is unimodular iff for every $\phi \neq K \subset [1,m]$, the annihilator $A(x)$ of every $x \in R^K/\Pi_K M$ is either $\{o\}$ or R.*

We have to prove that for every minimal support J, there exists a $u \in M$, with $s(u) = J$ such that u_j is a unit of R, $\forall\, j \in J$. The hypothesis is

that $\forall K \subset [1,m]$ if $\alpha\Pi_K x \in \Pi_K M$, $\alpha \neq 0$, then $\Pi_K x \in \Pi_K M$, that is, there exist some y in M whose projection in R^K is $\Pi_K x$. Indeed, if this occurs the annihilator of $\Pi_K x$ is not $\{o\}$ and then contains 1.

Now, let $K = \{j\} \cup \bar{J}$, $j \in J$, with $s(x) = J$, minimal support. Since $x_j(1,0, \ldots ,0) = (x_j,0, \ldots ,0) \in \Pi_K M$, $(1,0, \ldots ,0) \in \Pi_K M$, $(1,0, \ldots ,0) = \Pi_K u$, $u \in M$, but such a u is in $\Delta_J M$. Now if k is any other element in J, a v is found in $\Delta_J M$ with $v_k = 1$. Since $s(v) = s(u) = J$, $v_j u - v = 0$ $v_j u_k = 1$, hence u_k is a unit as it was to be shown.

Conversely, if M is unimodular, it is spanned by the rows of a totally unimodular matrix. Then $\Pi_J M$ is a unimodular module of R^J, $\forall J \subset [1,m]$. Now $\Pi_J M$ is spanned by the rows of an echelon matrix A with A^K the unit matrix; Card $K \geq 1$. Then obviously, $\Pi_J M \oplus R^{J\setminus K} \times \{o\}^K = R^J$. Let $\alpha x \in \Pi_J M$, $x \in R^J$. We write $v = y + z$, $y \in \Pi_J M$, $z \in R^{J\setminus K} \times \{o\}^K$. $\alpha x = \alpha y + \alpha z$, thus $\alpha z = 0$. Since R is a domain, $z = 0$ if $\alpha \neq 0$, $x = y \in \Pi_J M$.

Another characterization is the following (again R is a domain).

Theorem 3. *A submodule M of R^m, R a domain, is unimodular, iff for every $\phi \neq K \subset [1,m]$, $\Pi_K M$ is a direct factor of R^K.*

Let $s(x) = J$ be a minimal support. We make $K = \{j\} \cup \bar{J}$, when $j \in J$. Then $(x_j,0, \ldots ,0) \in \Pi_K M$. Let us denote $(1,0, \ldots ,0)$ by ℓ_j. Since $\Pi_K M \otimes N = R^K$,

$$\ell_j = y + z \ , \ y \in \Pi_K M \ , \ z \in N \ .$$

$$x_j \ell_j = x_j y + x_j z$$

Since $x_j \ell_j$ is in $\Pi_K M$ and $x_j \neq 0$ is not a zero divisor, $\ell_j = y \in \Pi_K M$. The proof now follows with the same argument as for the previous theorem.

2. The Theorem of Compatibility

2.1 Property 11. *Let M an S-stable module with a n-basis. Denote by μ the cannonical R-isomorphism of R^n onto M and let $t^{(a)} = \mu^{-1} a$, $\forall\ a \in M$. Denote by U a set of representatives of M and by K any subset of $[1,m]$, an $x \in G^m$ verifies*

$$\sum_{1 \leq j \leq m} a_j x_j = \sum_{1 \leq i \leq n} t_i^{(a)} b_i \ , \ b \in G^n \ , \forall\ a \in \Delta_K M \text{ iff}$$

$$(1) \qquad \sum_{1 \leq j \leq m} u_j x_j = \sum_{1 \leq i \leq n} t_i^{(u)} b_i \ , \forall\ u \in U \cap \Delta_K M \ .$$

If (1) is verified, we have, by Property 8, if $a \in \Delta_K M$,

$$(2) \qquad \beta a = \sum_{u \in U \cap \Delta_K M} u \alpha_u \ ,$$

$$\beta \sum_{1 \leq j \leq m} a_j x_j = \sum_{u \in U \cap \Delta_K M} \alpha_u \sum_{1 \leq j \leq m} u_j x_j = \sum_{u \in U \cap \Delta_K M} \alpha_u \sum_{1 \leq i \leq n} t_i^{(u)} b_i$$

$$= \sum_{u \in U \cap \Delta_K M} b_i \sum_{1 \leq i \leq n} \alpha_u t_i^{(u)} = < b \ , \ \sum_{u \in U \cap \Delta_K M} \alpha_u t^{(u)} >$$

But, applying μ^{-1} to (2),

$$(3) \qquad \beta t^{(a)} = \sum_{u \in U \cap \Delta_K M} \alpha_u t^{(u)} \ ,$$

Hence

$$\beta \sum_{1 \leq j \leq m} a_j x_j = < b \ , \ \beta t^{(a)} > = \beta < b \ , \ t^{(a)} > \ ,$$

and since $\beta : G \to \beta G$ is injective,

$$\sum_{1\le j\le m} a_j x_j = \sum_{1\le i\le n} t_i^{(a)} b_i \ .$$

2.2 First statement and proof

Let $(\Gamma_j)_{j \in [1,m]}$ be a family of subsets belonging to A (defined in 1.1) relative to a stable set S of R. Let also $\{b_i\} \in A$, $i \in [1,n]$. Finally let $A = (a_i^j)$ be an $n \times m$ matrix with rank n whose rows span a S-stable module M with representative set U. We have

Theorem 4. *The linear system*

$$(4) \qquad \sum_{1\le j\le m} a_i^j x_j = b_i \ , \ i = 1, \ \dots \ ,n \ .$$

has a solution $(x_j)_{1\le j\le m} = x \in \Gamma = (\Gamma_j)_{1\le j\le m}$ *iff for every* $u = t^{(u)}A$ *in* U

$$(5) \qquad \sum_{1\le i\le n} t_i^{(u)} b_i \in \sum_{1\le j\le m} u_j \Gamma_j$$

We prove that if (5) entails existence of an $x^{(K)} \in \Gamma$ such that $\forall\ c \in \Delta_K M$, $\sum_{1\le j\le m} c_j x_j^{(K)} = \sum_{1\le i\le n} t_i^{(c)} b_i$ (see Property 11 for notations) for every $K \subset [1,m]$ with Card $K < r$, then (5) also entails existence of such an $x^{(K')}$ for any $K' \subset [1,m]$ with Card $K' = r$. This will prove that for $K = [1,m]$ there exists an $x \in \Gamma$ as claimed. Let s be any element in K' and write $K' = K \cup \{s\}$. Let U be the subset of all representatives of M with support in K'. $U = U_1 \cup U_2$ where U_2 is the set of all representatives of M with

supports in K. By Property 11, we have to show that there exists a $x^{(K')} \in \Gamma$ such that for every $u \in U$:

$$(6) \qquad \sum_{1 \le j \le m} u_j x_j^{(K')} = \sum_{1 \le i \le n} t_i^{(u)} b_i \ .$$

$x^{(K')}$ will be constructed as follows. We show that Γ_s may be reduced to one point $\{x_s^{(K')}\} = \Gamma_s'$ and that the hypothesis (5) is still verified for every $u \in U^{(K')}$ with that new set of Γ_j's. We will then consider another s in K' and change again the Γ_j's. The set of Γ_j's that we finally obtain is the set of $\{x_j^{(K')}\}$ for which (5) is then verified. We first observe that whatever it will be, the new Γ_s' will verify (5) for every $u \in U_2$ together with the old Γ_j, $j \neq s$, since $u_s = 0$, $\forall\, u \in U_2$. We have thus only to consider the u's in U_1. Let us define some notations,

$$(7) \qquad \beta_u = \prod_{\substack{v \in U_1 \\ v \neq u}} v_s \ ; \ u' = \beta_u u \ , \ \forall\, u \in U_1 \ .$$

Then, $u'_s = \alpha, \alpha$ a constant, for every $u \in U_1$. Notice that the β_u's and α are in S. We have

$$(8) \qquad \sum_{1 \le i \le n} t_i^{(u')} b_i \in \sum_{\substack{1 \le j \le m \\ j \neq s}} u_j' \Gamma_j + \alpha \Gamma_s \ , \ \forall\, u \in U_1 \ .$$

which means that $\alpha\Gamma_s$ meets $\sum_{1 \le i \le n} t_i^{(u')} - \sum_{\substack{1 \le u \le m \\ j \neq s}} u_j' \Gamma_j$, for every u in U_1.

If we could prove that

$$(9) \qquad E = \bigcap_{u \in U_1} \Big(\sum_{1 \le i \le n} t_i^{(u')} b_i - \sum_{\substack{1 \le j \le m \\ j \neq s}} u_j' \Gamma_j \Big) \neq \phi \ ,$$

by the finite intersection property, we would have

(10) $$\alpha\, x_s^{(K')} \in \alpha\Gamma_s \cap E$$

and, α being a non zero divisor verifying 1.2 (9), $\Gamma'_s = \{x_s^{(K')}\}$ would meet our requirement.

Now, by recurrence, we know that there exists a $x^{(K)}$, $x_j^{(K)} \in \Gamma_j$, $j \in K$, verifying

(11) $$\sum_{1\le i\le m} t_i^{(u)} b_i = \sum_{1\le u\le m} u_j x_j^{(K)} \quad , \forall\ u \in U_2 \ .$$

Notice that the componants $x_j^{(K)}$ for $u \notin K$ are irrelevant.

Let us consider $x_s^{(K)}$ in $\overline{SG}$ verifying

(12) $$v_s x_s^{(K)} = \sum_{j\in K} v_j x_j^{(K)} - \sum_{1\le i\le n} t_i^{(v)} b_i$$

for some v picked up in U_1 .

Now for any $u \in U$,

(13) $$v_s u - u_s v \in \Delta_K M \ ,$$

and, by (11), from Property (11)

(14) $$\sum_{j\in K} (v_s u_j - u_s v_j)\, x_j^{(K)} = \sum_{1\le i\le n} (v_s t_i^{(u)} - u_s t_i^{(v)})\, b_i \ ,$$

which means that

(15) $$v_s u_s x_s^{(K)} = v_s \sum_{j\in K} u_j x_j^{(K)} - v_s \sum_{1\le i\le n} t_i^{(v)} b_i \ .$$

v_s is in S and we may conclude that

(16) $$u_s x_s^{(K)} \in \sum_{j\in K} u_j \Gamma_j - \sum_{1\le i\le n} t_i^{(u)} b_i \ , \forall\ u \in U_1 \ .$$

Multiplying both members of (15) by β_u , we obtain (9).

(For clarity, we point out that $x_s^{(K')}$ of (10) is not necessarily the same as $x_s^{(K)}$, since $x_s^{(K)}$, which allowed the proof of (9) is not required to be in Γ_s , since it is even not required to be in G but in $\overline{SG}$. However, $\alpha x_s^{(K)}$ is in G .)

2.3 A more general statement

In 2.2, we have considered a problem concerning an S-stable module M with a basis. An S-stable module has not necessarily a basis since a submodule of R^m for R a domain, has not necessarily a basis.

Let $R^{(M)}$ be the set of almost zero $t = (t_a)_{a\in M}$, $t_a \in R$, $\forall\, a \in M$. N is the submodule of $R^{(M)}$ consisting of all t such that $\sum_{a\in M} t_a a = 0$. As for Property 11, there is still a R-isomorphism μ of the quotient module $R^{(M)}/N$ onto M :

$$\mu t^{(c)} = \sum_{a\in M} t_a^{(c)} a = c \in M . \tag{17}$$

Now, if $b = (b_a)_{a\in M} \in G^M$, and $\sum_{a\in M} t_a b_a = 0$, for every $t \in N$, then

$$\sum_{a\in M} t_a^{(c)} b_a \tag{18}$$

is also defined for every $t^{(c)}$ in $R^{(M)}/N$. The arguments of proof of Propert 11 and of Theorem 4 hold for proving

Theorem 5 . *Let M be an S-stable module of R^M and N and b defined as here above. Then if $\Gamma_j \in A$, $\forall\ j \in [1,m]$, if $\{b_a\} \in A$, $\forall\ a \in M$, there exists an $x = (x_j)_{1\le j\le m} \in (\Gamma_j)_{1\le j\le m}$ with*

(19) $$\sum_{1\le j\le m} a_j x_j = b_a \quad \forall\ a \in M$$

iff for every $u = \sum_{a\in M} t_a^{(u)} a$ *in a finite set* U *of representatives of* M ,

(20) $$\sum_{a\in M} t_a^{(u)} b_a \in \sum_{1\le j\le m} u_j \Gamma_j \ .$$

Theorem 6. *Let* M *be an S-stable module spanned by the rows of a* $n \times m$ *matrix* A . *Let* $\Gamma_j \in A$, *for all* j , *and* $\{g\} \in A$, $\forall\ g \in G$. *Let* U *be a set of representatives of* M *and* T_1 *any set of* t*'s for which* $U = \{u \mid tA = u\ ,\ t \in T_1\}$, *let* $b \in G^n$; *then there exists a finite set* $T_2 \subset R^n = R^A$ *such that*

(21) $$Ax = b\ ,\ x \in \Gamma = (\Gamma_j)_{j\in[1,m]}$$

has a solution iff

(22) $$tA = \sum_{i\in[1,n]} t_i b_i = 0\ ,\ \forall\ t \in T_2$$

and

(23) $$\sum t_i b_i \in \sum u_j \Gamma_j\ ,\ \forall\ t \in T_1 \ .$$

Since the rows of A form a set of generators of M , we may replace (20) in the statement of Theorem 5 by

(24) $$\sum_{a\in A} t_a^{(u)} b_a \in \sum_{1\le j\le m} u_j \Gamma_j \ .$$

($a \in A$ means a runs over the set of rows of A). We first show that there exists a finite set $T_2 \subset R^A$ spanning over R the module L_1 of t's verifyi

(25) $$\sum_{a\in A} t_a a = 0 .$$

If this is proved, we will have

(26) $$\left(\sum_{a\in A} t_a b_a = 0 , \forall\, t \in L_1\right) \Longleftrightarrow \left(\sum_{a\in A} t_a b_a = 0 \;\forall\; t \in T_2\right) ,$$

since the denominators in $\bar{R}$ are non zero divisors (1.324). Furthermore, we will have $\sum_{a\in M} t_a b_a = 0$ for every $t \in N$, N defined in Theorem 5, with

(27) $$b_c = \sum_{a\in A} \alpha_a b_a \text{ , whenever } \sum_{a\in A} \alpha_a a = c$$

and the sufficient condition for Theorem 6 will follow.

By corollary 2 in #1, we know that $\bar{M} = \bar{R}M$ is spanned by the rows of an echelon matrix B with $B^J = I$. Since every support $s(x)$, $x \in M\backslash\{0\}$ meets J, $\sum_{a\in A} t_a a = 0$ iff $\sum_{a\in A} t_a a_j = 0$, $j \in J$. Let L_2 be the R-module spanned by the columns of A in R^n with indexes in J. We have just seen that $t \in L_1$ iff $t \in L_2^{\perp}$. Then $L_1 = L_2^{\perp}$. Since $B^J = I$, there exists a $\bar{R}$-homomorphism μ of $\bar{R}^n$ onto $\bar{R}^k$, k the dimension of $\bar{M}$ whose restriction ν at $\bar{R}L_2$ is an isomorphism. Then $p = \nu^{-1}o\mu$ is a projector of $\bar{R}^n$ onto $\bar{R}L_2$ which is a direct factor:

(28) $$\bar{R}L_2 \oplus L_3 = \bar{R}^n .$$

But then

(29) $$(\bar{R}L_2)^{\perp} \oplus L_3^{\perp} = \bar{R}^n .$$

Now, $L_1 = L_2^{\perp}$ means $\bar{R}L_1 = (\bar{R}L_2)^{\perp}$ and if q is the projector of $\bar{R}^n$ onto $\bar{R}L_1$, $\{q(\ell_i)\}_{i\in[1,n]}$ is a set of generators of $\bar{R}L_1$, where $\{\ell_i\}_{i\in[1,n]}$ is

the cannonical basis of $\overline{R}^n$. Finally if α is the product of the denominators met in $\{g(\ell_i)\}_{i\in[1,n]}$, we make $T_2 = \{\alpha q(\ell_i)\}_{i\in[1,n]}$, and (25) is proved.

Remark. We notice that T_2 may be actually constructed:

$$<\ell_i \ , \ (1 - p)\ell_j>$$

is the j^{th} componant of $q(\ell_i)$.

3. Consequences of the Theorem of Compatibility.

Theorem 5 is the theorem of compatibility in its most convenient form for deducing known and new results.

3.1 Consequences through known results.

It generalizes "Le theorème de compatibilité" of [1] from which were deduced the usual theorems of consistancy of systems of linear inequalities, "Le théorc de décomposition pour les groups réticulés" N. Bourbaki [5], and results in Graph Theory.

3.2 The generalized Lemma of Farkas

Let R be a linear ordered domain. Then if S is any stable set in R , the ring $\overline{R}$ of all fractions with denominators in S is a subring of the linear ordered ring of fractions with denominators in $R\backslash\{o\}$. Then the restriction of this order to $\overline{R}$ makes it a linear ordered ring. The set A of all intervals in $\overline{R}$ verifies the axioms I_1, I_2, I_3, I_4 of 1.1, since S is a set of units in $\overline{S}$. We first prove the

3.2.1 Lemma *Let U be a set of representatives of the S-stable module M. We denote $-U \cup U$ by V. Then for any x in M, we may write*

$$(1) \qquad x = \sum_{u \in V} \alpha_u u \ , \ \alpha_u \geq 0 \ , \ \alpha_u \in \overline{R} \ , \ x_j u_j \geq 0 \ , \forall \ j \in [1,m]$$

The denominators of all α_u possibly involved in expressions like (1) are take from a finite subset of S, the set of non zero componants of the u's.

We proof (1) for $x \geq 0$. The lemma will follow since for any set $\{\varepsilon_j\}_{1 \leq j \leq m}$, $\varepsilon_j \in \{1,-1\}$,

$$(2) \qquad (x_j)_{j \in [1,m]} \rightsquigarrow (\varepsilon_j x_j)_{j \in [1,m]}$$

defines a mapping of M onto an S-stable module.

We first show that there exists a $u \geq 0$, $u \in V$, with $s(u) \subset s(x)$. If $s(x)$ is minimal, it is true, since then, there exists a $u \in V$ with $s(u) = s(x)$; thus, $x - u_s^{-1} x_s u = 0$ with $s \in s(u)$, $u_s > 0$. Then for any $j \in s(u)$, $x_j = u_s^{-1} x_s u_j > 0$, consequently, $u_j > 0$. We suppose now the property verified for all $y \geq 0$, $y \neq 0$ with at most k elements in $s(y)$ and we prove that it is still valid for any $x \geq 0$ with Card $s(x) = k'$, where k' is the smalles integer larger than k for which such an x does exist. There exists a v in V with $s(v) \subset s(x)$. Let

$$(3) \qquad J = \{j \mid v_j > 0\} \ .$$

J is not empty since we would have taken $-v$ in V if it occured that $J = \phi$ for v .

Now let $s \in J$ be such that

$$(4) \qquad v_s^{-1} x_s \leq v_j^{-1} x_j \ , \ \forall \ j \in J$$

It is clear that

$$y = x - v_s^{-1} x_s v \geq 0 \ . \tag{5}$$

and since $s(y) \subset s(x)$, $s(y) \neq s(x)$, $\text{Card}\ s(y) \leq k$. Thus a $u \geq 0$, $u \in V$ exists with $s(u) \subset s(y) \subset s(x)$. Knowing the existence of such a u , we prove (1) by recurrence on $\text{Card}\ s(x)$, $x \geq 0$. We consider again $s \in s(u)$ with

$$u_s^{-1} x_s \leq u_j^{-1} x_j \ , \ \forall\ j \in s\ (u) \ . \tag{6}$$

Now

$$y = x - u_s^{-1} x_s u \geq 0 \ , \tag{7}$$

and, by recurrence,

$$y = \sum_{v \in V} \alpha_v v \ , \ \alpha_v \geq 0 \ , \ \alpha_v \in \overline{R} \ , \ \alpha_v v \geq 0 \ . \tag{8}$$

Then, (7) and (2) achieve the proof of (1). Now, to prove the last assertion, observe by (7) that the denominators concerned are taken from the finite set of componants of u's in V .

3.2.2 Notations and definitions

Let A be a finite subset of R^n with rank r . The elements of A form the columns of a matrix that we denote by the same letter A . Now the rows of A span a module $M(A)$ over S that we may consider a S-stable module for suitable S . For example we may build up S as follows if we want a finitely generated S whenever every factorization in R is finite. Let A_I be a set of r independant rows in A and $\{A_I^J\}_{J \in E}$ the set of all non-singular $r \times r$ submatri

of A_I. Denote by E the set of all determinants of all A_I^J's and their opposites while J runs over $\mathcal{E}$. E also contains -1. If $\overline{E}$ is now the multiplicative group generated by E in the field K of fractions of R, we make $S = \overline{E} \cap R$, and clearly S meets the requirements of its definition in 1.1. By multiplying A_I on the left by all adjoints of A_I^J's, $J \in \mathcal{E}$, we obtain a set of rows of matrices which form a set U of representatives of the S-stable module $M(A)$.

Definitions.

We denote by $\hat{C}$ any cone over R, that is any set verifying $\alpha\hat{C} \subset \hat{C}$, $\forall\, \alpha > 0$, $\alpha \in R$ and $\hat{C} + \hat{C} \subset \hat{C}$, $\hat{C}$ being a subset of a R-module.

When $\hat{C} \subset R^n$, the Polar $\hat{C}^*$ of $\hat{C}$ is by definition the cone

$$\hat{C}^* = \{y \mid \forall\, x \in \hat{C},\ \sum_{1\le i\le n} x_i y_i \le 0,\ y \in R^n\} \tag{9}$$

If F is a set of non zero elements in R, we denote by $F^{-1}R$ the set of all fractions with denominators in F. Given a subset C of R^n and a subset $E = ER$ of the field K of fractions of R, we denote by $\hat{C}(E)$ the cone

$$\{x \mid x = \sum_{c\in C} \alpha_c c,\ \alpha_c \in E,\ \alpha_c \ge 0\}\ . \tag{10}$$

We are now ready to state the generalizations of the Lemma of Farkas. K is again the smallest field containing R.

Theorem 7. *Let A be a finite subset of R^n and let S be any suitable set that makes $M(A)$ an S-stable module, then there exists a finite subset F of S such that the polar $\hat{A}^*$ of the cone $\hat{A} = R^n \cap \hat{A}(K)$ has the form $\hat{A}^* = R^n \cap \hat{B}(F^{-1}R)$, B a finite set. Moreover the polar $(\hat{A}^*)^*$ of $\hat{A}^*$ is $\hat{A}$ Moreover $\hat{A} = R^n \cap \hat{A}(F^{-1}R)$.*

Before proving the theorem, let us observe that if R is an ordered field, $\hat{A}$ is the cone hull of A, since $F^{-1}R = R$ and the theorem's meaning in that particular case is that the polar of $\hat{A}$ is a finitely generated cone $\hat{B}$ whose polar is $\hat{A}$ itself. This is the well known lemma of Farkas.

We first define F. When forming a set U of representatives of $M(A)$, each time we have the choice between a $u \leq 0$ and its opposite, we take the $u \leq 0$. F will be the set of non zero componants of elements in U. We first prove: *$\hat{A} = R^n \cap \hat{A}(F^{-1}R)$ is the cone $R^n \cap \hat{A}(K)$ of all elements in R^n which belong to the cone hull of A in K^n.*

If $b \in R^n \cap \hat{A}(K)$, it is well known that there exists an $x \in K^m$, $x \geq 0$, such that, in matrix notations, $Ax = b$, with $s(x) \subset J$, A^J a set of r independant columns of A, where r is the rank of A. Let A_I^J be an $r \times r$ non-singular submatrix of A^J. Multiplying A_I on the left by the adjoint of A_I^J we obtain a matrix B whose rows have minimal supports and may be replaced by elements in U with corresponding supports. The matrix finally obtained is C, with C^J an $r \times r$ diagonal matrix. Now every row c in C has the form $\sum_{1 \leq i \leq n} t_i^{(c)} A_i$, with $t_i^{(c)} \in R$, for all c, for all i. We then have

$$\sum_{j \in J} c_j x_j = \sum_{1 \leq i \leq n} t_i^{(c)} b_i \,. \tag{11}$$

For every row c in C, the second member of (11) is in R and at most one summand in the first member does not vanish. Hence $x_j \in F^{-1}R$, $\forall\, j \in J$, which proves this first assertion. We now come back to the ordered ring $\bar{R}$ defined in the introduction of 3.2 and what we have just proved allows us in particular to consider $\hat{A}$ the cone of all elements in R^n belonging to the cone hull of A over $\bar{R}$. This will allow us to apply Theorem 6 in which S

has to be replaced by the group $\bar{S}$ generated by the S in the present statement and where $\Gamma_j = [0,\infty[\subset \bar{R}$, for all j. A is the set of all intervals in $\bar{R}$. The present U is still a set of representatives for $\bar{R}M(A)$ which will be the module M in theorem 6. Then, we may characterize $\hat{A}$ by saying

(12) if $b \in R^n$ $b \in \hat{A}$ iff $\exists\, x \geq 0$, $x \in \bar{R}^m$, $Ax = b$.

The consequence of Theorem 6 is

(13) if $b \in R^n$, $b \in \hat{A}$ iff $\forall\, t \in -T_2 \cup T_2 \cup T_1'$: $\sum_{1\leq i\leq n} t_i b_i \leq 0$,

where $T_1' \subset T_1$ is the subset of $t^{(u)}$ corresponding to non-positive primitive $u \in U$.

Let $B = -T_2 \cup T_2 \cup T_1'$. As in the proof of Theorem 6, we denote by L_1 the R-module spanned by T_2, that is, the cone hull over R of $-T_2 \cup T_2$. Now $t \in \hat{A}^*$ means $c = tA \leq 0$ and by the lemma, $c = \sum_{u\in U} \alpha_u u$, $\alpha_u u \leq 0$. This means $tA = \sum_{u\in U} \alpha_u t^{(u)}A$, or $t \equiv \sum_{u\in U} \alpha_u t^{(u)} \bmod L_1$, or

$t = \sum_{u\in U} \alpha_u t^{(u)} + \sum_{t\in T_2} \alpha_t t$, with $\alpha_t \in R$, $\forall\, t \in T_2$. Consequently t belongs to $R^n \cap \hat{B}(F^{-1}R)$ since the denominators of the α_u's belong to F and $\alpha_u u \leq 0$. Then $\hat{A}^* \subset R^n \cap \hat{B}(F^{-1}R)$ and the first assertion follows.

By (13) we know that $\hat{A}$ is the set of b's for which $\sum_{1\leq i\leq n} t_i b_i \leq 0$, for all t in $\hat{A}^*$; hence $(\hat{A}^*)^* = \hat{A}$. A *pointed cone* (or *proper cone*) is a cone $\hat{C}$ such that $-\hat{C} \cap \hat{C} = \{0\}$. It is immediately checked out that a cone $\hat{A}$ has full rank iff its polar $\hat{A}^*$ is a pointed cone. We have the following stronger statement, in this case, which follows the one of Theorem 7.

Theorem 8. *If* $\hat{A}$ *is a pointed cone,* F *may be chosen the set of all non-zero componants of* u*'s in* U *verifying* $u_j.u_s \geq 0$ *, for all* j,s *,* U *a set of representatives for the S-stable module* $M(A)$.

Since A is a finite set, we may find in it a subset A' of generators over K ; that is a set whose cone hull over K contains $\hat{A}$ and such that any element in A' is not in the cone hull of others in A' . A' is simply obtaine by successively deleting from A elements which are positive linear combinations of others in A over K . Now, since B has full rank, there is an isomorphism of R^n onto $M(B)$, the R-module spanned by the rows of B . Consider a b' in A' whose image under this isomorphism is $b'B \leq 0$. The support $s(b'B)$ of $b'B$ is minimal. For, if not, $b'B$ would be, by the lemma, a positive linear combination over K of ≤ 0 elements in $M(B)$ with minimal supports whose reciprocal images in R^n should be proportional to generators of A' , since any positive linear combination of more than one element in A' has an image in $M(B)$ whose support is the union of at least two distinct supports. We thus also observe that to any $b'B \leq 0$ with minimal support corresponds an $\alpha b' \in A'$, $\alpha > 0$, $\alpha \in K$. But we know, since here $B = T_1' \cup T_2 \cup -T_2$, that for every $b' \in A' \subset A$, $b'B$ has as componants the componants of some $u \leq 0$, $u \in U$ Hence $b'B$ has its componants in F . Now consider any $\ell \in \hat{A} = (\hat{A}^*)^*$. We have, by the Lemma, applied to $M(B)$, which is S-stable for $S = R\backslash\{0\}$.

$$0 \geq \ell B = \sum_{\ell' \in A'} \alpha_{\ell,\ell'} \ell' B \ , \ \alpha_{\ell,} \geq 0 \ , \tag{14}$$

all denominators of $\alpha_{\ell,}$ being in F . This means, by isomorphism,

$$\ell = \sum_{\ell' \in A'} \alpha_{\ell,\ell'} \ , \tag{15}$$

which shows that if $\hat{A} = R^n \cap \hat{A}(K)$, then $\hat{A} = R^n \cap \hat{A}(F^{-1}R)$. Now consider any $t \in R^n$ which belongs to $\hat{A}^*$. $tA \leq 0$ is by the lemma a linear combination of non-negative u's in $M(A)$ with coefficients in $F^{-1}R$. This means t is a positive linear combination of some elements in $T_1' \cup T_2 \cup -T_2$, the coefficients for elements in T_1' being in $F^{-1}R$,and, for elements in $T_2 \cup -T_2$, in R . Hence $\hat{A}^* = R^n \cap \hat{B}(F^{-1}R)$.

Before giving an application of Theorem 7,we study the inclusions

$$\hat{A}(R) \subset M(A^T) \cap \hat{A}(K) \subset R^n \cap \hat{A}(K),$$

where $M(A^T)$ is the R-module spanned by the columns of A .

We may have equality, for example when the columns of A form the canonica basis of R^n . The first inclusion may be a proper one, if

$$A = \begin{vmatrix} 1 & -1 & 3 \\ 1 & 1 & 2 \end{vmatrix},$$

$(0,1)^T$ belongs to $M(A^T)$ and to $\hat{A}(\mathbb{Q})$ but not to $\hat{A}(\mathbb{Z})$.

We will give the example of an infinite class of A's for which we have equality in place of the first inclusion and a proper inclusion in the second place.

The submonoïd of k-valencies in $\mathbb{N}^n$

As it comes out clearly from [6] the natural framework for the study of cones over the ring $\mathbb{Z}$ is the commutative monoïd since a cone in a submodule of $\mathbb{Z}^n$ may be considered a submonoïd of a commutative monoïd.

Let X be a finite set. We identify X with $\{1,2, \ldots ,n\}$. An element $d \in \mathbb{N}^n$ may thus be considered a mapping $d : X \to \mathbb{N}$. Now if we denote by P_k the set of k-subsets of X, $d = (d_i)_{i \in X}$ is called a k-valency if there exists a mapping $f : P_k \to \mathbb{N}$ such that

$$d_i = \sum_{\substack{u \in P_k \\ i \in u}} f(u) \quad , \forall \ i \in X \ . \tag{16}$$

The set of k-valencies form clearly a submonoïd of $\mathbb{N}^n$. Coming back to the previous notations, consider the set $A \subset \mathbb{N}^n$ consisting of all elements with the form $\sum_{i \in J} \ell_i$ with Card $J = k$ and $\{\ell_i\}_{i \in X}$ the canonical basis of $\mathbb{Z}^n$. Then the considered cone is $\hat{A}(\mathbb{Z})$. We show that $\hat{A}(\mathbb{Z}) = M(A^T) \cap \hat{A}(\mathbb{Q})$ by provi Theorem 9. Indeed Theorem 9 will show that $\hat{A}(\mathbb{Z}) = M' \cap \hat{A}'(\mathbb{Q})$ where M' denotes a submodule of $\mathbb{Z}^n$ containing $M(A^T)$ and A' is a finite set containing A. Actually $\hat{A}'(\mathbb{Q})$ will appear as the polar of a cone, polar who contains A. This will give the inclusion $\hat{A}(\mathbb{Z}) \supset M(A^T) \cap \hat{A}(\mathbb{Q})$ from which follows the announced equality.

THEOREM 9. *The mapping $d : X \to \mathbb{N}$ is a valency iff when ordering $d_{i_1} \geq \ldots \geq d_{i_j} \geq \ldots \geq d_{i_n}$ one has*

$$(k - r) \sum_{j \leq r} d_{i_j} \leq r \sum_{j > r} d_{i_j} \quad , r = 1,2, \ldots k - 1 \ . \tag{17}$$

and

$$\sum_{1 \leq i \leq n} d_i \equiv 0 \bmod k \ . \tag{18}$$

M' is the module of $x \in \mathbb{Z}^n$ verifying $\sum_{1 \leq i \leq n} x_i \equiv 0 \bmod k$ which actually

contains $M(A^T)$ and $\hat{A}'(\Omega)$ is the cone in $\mathbb{Z}^n$ polar to all opposites of elements of the canonical basis of $\mathbb{Z}^n$ and to all elements with the form

$$(19) \qquad (k - r) \sum_{\substack{i\in I \\ \mathrm{Card} I = r}} \ell_i - r \sum_{i\in \bar{I}} \ell_i \ .$$

This last fact follows from (17) where we relabel the componants of d in order that

$$(20) \qquad d_1 \geq d_2 \geq \ldots \geq d_n \ ,$$

by

$$(21) \quad (k - r) \sum_{\substack{i\in I \\ \mathrm{Card} I = r}} d_i \leq (k - r) \sum_{i\leq r} d_i \leq r \sum_{i>r} d_i \leq r \sum_{i\in \bar{I}} d_i \ .$$

We prove the theorem by recurrence on $\sum_{1\leq i\leq n} d_i$. We show that there exists an $x \in \mathbb{Z}^n$, $x = \sum_{i\in J} \ell_i$, Card $J = k$ such that

$$(22) \qquad d_i = x_i + d'_i \ , \ i = 1, \ldots ,n \ ,$$

and d' verifies the hypothesis. We built up x as follows.

If $d_k > d_{k+1}$, we make $x_i = 1$, $i = 1, \ldots ,k$, $x_i = 0$, $i > k$. Then $d'_i \geq d'_{i+1}$, $i = 1, \ldots , n - 1$, and

$$(23) \quad (k - r) \sum_{i\leq r} d'_i - r \sum_{i>r} d'_i = (k - r) \sum_{i\leq r} d_i - r \sum_{i>r} d_i \leq 0 \ .$$

As it shall be. If $d_k = d_{k+1} = 0$, (17) for $r = k - 1$ gives $d_i = 0$, $i = 1, \ldots ,n$. If $d_k = d_{k+1} > 0$, denote by j the smallest integer such that $d_{j+1} = d_k$ and by ℓ the largest integer with $d_\ell = d_k$. We make $x_i = 0$ except for $i \leq j$ (maybe this set of i is empty) and for

$i = \ell, \ell - 1, \ldots, \ell - k + j + 1$, where $x_i = 1$. We write again (22) and we have to show that (17) holds for d'. For easier notations, we write

$\sum_{i \le r} d_i = qr$ and $\sum_{i > r} d_i = p_r$. By hypothesis

$$p_r \equiv -q_r(k) . \tag{24}$$

Then

$$\forall\, r < k\ ,\ rp_r - (k - r)q_r \equiv rp_r - kq_r - rp_r \equiv 0(k) . \tag{25}$$

So we may write

$$rp_r - (k - r)q_r = kh_r\ ,\ r = 1, \ldots, k - 1 . \tag{26}$$

It follows that

$$k^{-1}(q_r + p_r) = h_r - h_{r-1} + d_r . \tag{27}$$

But

$$d_r k = d_k k < d_k \ell \le q_r + p_r\ ,\ \text{for}\ \ j < r \le k - 1 < \ell \tag{28}$$

then

$$d_r < k^{-1}(q_r + p_r) \quad \text{for} \quad j < r \le k - 1 < \ell\ ,$$

which means by (27) (note here that $p_r + q_r$ does not depend on r)

$$h_r \ge r - j\ ,\ j < r \le k - 1 < \ell . \tag{29}$$

Now if we had made $x_i = 1$, $i = 1, \ldots, k$ and $x_i = 0$, $i > k$, we would have had (23). Comparing the present situation to this one we have

$$(k - r) \sum_{i \le r} d'_i - r \sum_{i > r} d'_i = (k - r) \sum_{i \le r} d_i - r \sum_{i > r} d_i + (k - r)(r - j) \tag{30}$$

$$+ r(r - j) = kh_r + k(r - j) \le 0\ ,\ \text{by (29)}.$$

(30) completes the proof.

Remark: Th. 9 is a corollary of Theorem 1.1 Chapter 6 of H. Ryser [7]. But this result is made part of linear algebra. Observe that this argument could be general: an element d is in a finitely generated cone C iff it may be written $d' + x$, with $d' \in C$ and x a generator of C. What is now left to check out is that the inclusion $\hat{A}(\mathbb{Z}) \subset \mathbb{Z}^n \cap \hat{A}(\mathbb{Q})$ is a proper inclusion. Consider in A the set $\{x^{(1)}, \ldots, x^{(k+1)}\}$.

$$x^{(j)} = \sum_{\substack{1 \le i \le k+1 \\ i \neq j}} \ell_i \quad . \tag{31}$$

Then $k^{-1} \sum_{j \le k+1} x^{(j)}$ is in $\mathbb{Z}^n \cap \hat{A}(\mathbb{Q})$ and is certainly not in $\hat{A}(\mathbb{Z})$.

A relation between the three considered cones and finitely generated monoïds. We have seen in Theorem 7 that $R^n \cap \hat{A}(K) = R^n \cap \hat{A}(F^{-1}R)$. Now if f denotes the product of all elements in F, it is clear that $R^n \cap \hat{A}(K) \supset R^n \cap f^{-1}\hat{A}(R) \supset R^n \cap \hat{A}(F^{-1}S) \supset R^n \cap \hat{A}(K)$. Now $f^{-1}\hat{A}(R)$ is a finite generated cone over R in the R-module $f^{-1}R^n$. On the other hand,

$$M(A^T) \cap \hat{A}(K) = M(A^T) \cap R^n \cap \hat{A}(K) = M(A^T) \cap R^n \cap f^{-1}\hat{A}(R) \quad .$$

Thus the three cones that we consider are all intersections of at most three finitely generated cones in the R-module $f^{-1}R^n$.

When $R = \mathbb{Z}$, we may apply Theorem VI of [6], page 188 which teaches us in particular that if C', C'' are two finitely generated cones over $\mathbb{Z}$ in a commutative group, or in other words two stable sets under addition in an additive group, then their intersection is finitely generated over $\mathbb{Z}$. An immediate consequence is the following

Property 1: *If* A *is a finite set in* $\mathbb{Z}^n$, M *a* $\mathbb{Z}$*-submodule of* $\mathbb{Z}^n$ *over* $\mathbb{Z}$, $\hat{A}(\mathbb{Q})$ *the cone spanned by* A *in* $\mathbb{Q}^n$ *over* $\mathbb{Q}$, *then* $M \cap \hat{A}(\mathbb{Q})$ *is finitely generated over* $\mathbb{Z}$.

As well, all cones considered may be imbedded in the group generated in $\mathbb{Q}^n$ by the union of $f^{-1}A$ and a basis of $\mathbb{Z}^n$.

In particular, the three cones that we consider are finitely generated for $R = \mathbb{Z}$.

The problem of finding out the generators of such cones may be eased by an argument which generalized the one used for the cone of valencies and which follows the herebelow exploitation of some results in [6].

We call *ordered monoïd of non-negative elements* a commutative monoïd C in which the cancellation low holds and whose ordered set of elements verifies

(32) $\qquad x,y,z \in C \ , \ \& \ x \leq y \ \text{ implies } \ x + z \leq y + z$

and

(33) $\qquad x \in C \ \text{ implies } \ 0 \leq x \ .$

We first observe that a commutative monoïd is an ordered set of non-negative elements iff

(34) $\qquad x,y \in C \ \& \ x + y = 0 \ \text{ implies } \ x = y = 0 \ .$

If (34) is verified, we define

(35) $\qquad x \leq y \ \text{ iff } \ \exists \ z \in C \ , \ x + z = y \ .$

The relation defined is reflexive and transitive. Now if $x + z' = y$ and $y + z'' = x$, then

(36) $\qquad x + z' + z'' = x \ ,$

and, by the cancellation law, and (34)

(37) $$z' + z'' = 0 \ , \ z' = z'' = 0 \ .$$

This means

(38) $$x \leq y \quad \text{and} \quad y \leq x \quad \text{implies} \quad x = y \ .$$

(32) is verified for the ordered relation introduced and also (33) since $x = x + 0$. Conversely if an ordered monoïd verifies (32) and (33) this order is such that (34) is true.

Let $x + y = z$. Since $y \geq 0$, by (32), $x + y \geq x$, thus $z \geq x$. In particular if $x + y = 0$, then $x \leq 0$, and since $x \geq 0$, by antisymmetry, $x = 0$, $y = 0$.

Finding out a minimal set of generators of a monoïd C in which holds the cancellation law, when C is a submonoïd of a finitely generated monoïd C' whose largest submonoïd which is a group is contained in C .

We reduce the problem to that one where C verifies (34). Indeed let G be the submonoïd of C for which

(38) $$\forall \ x \in G \ , \ \exists \ x' \in C : x + x' = 0 \ .$$

G is a group and the congruence of monoïd

(39) $$Q = \{(x,y) \mid (x,y) \in C' \times C' \ , \ \exists \ z \in G \ , \ x + z = y\}$$

defines a quotient $C'/Q = \overline{C}'$ in which $C/Q = \overline{C}$ is a submonoïd. Every element in $\overline{C}'$ has the form $x + G$, $x \in C'$. The cancellation law holds in $\overline{C}'$ since

(40) $$\overline{x},\overline{y},\overline{z} \in \overline{C}' \quad \text{and} \quad \overline{x} + \overline{y} = \overline{x} + \overline{z}$$

means

$$x + y = x' + z' \text{ , for some } x,x' \in \overline{x}, y \in \overline{y} \text{ , } z + \overline{z} \text{ ,}$$

and since $x' + x'' = x$, $x'' \in G$

(41) $$x + y + x'' = x + z' \text{ , then } y + x'' = z' \text{ ,}$$

by the cancellation law in C' . This means

(42) $$\overline{y} \cap \overline{z} \neq \phi \text{ , } \overline{y} = \overline{z} \text{ .}$$

Now $\overline{x} + \overline{y} = 0$ means $x + y \in G$ for some $x \in \overline{x}$, $y \in \overline{y}$. By definition of G, this means $x + y$ has an opposite in C , then also x and y , thus $x,y \in G$. Finally $\overline{x},\overline{y} \in \overline{C}' \ \& \ \overline{x} + \overline{y} = 0 \Rightarrow \overline{x},\overline{y} = 0$, that is $\overline{C}'$ is an ordered monoïd of non-negative elements as well as $\overline{C}$.

Now G being an abelian group, it has a basis. Knowing a set of generato B of $\overline{C}$ (or $\overline{C}'$) we will get a set of generators of C (or C') by taking any representative in each element of B and the union of the basis of G and its opposite. In particular, if C' is finitely generated, $\overline{C}'$ and G are also finitely generated, since G is a subtractive submonoïd of C' , [6] Propositio 7.1, page 179. We are now in a situation of applying the following.

THEOREM 10. *Let C be a submonoïd of an abelian ordered monoïd C' of non-negative elements, C' finitely generated. Then the intersection of all subsets B of $C\backslash\{0\}$ verifying $B + C = C\backslash\{0\}$, that is*

(43) $$\forall\, x \in C\backslash\{0\} \text{ , } \exists\, y \in B \text{ , } \exists\, z \in C \text{ with } x = y + z$$

is the unique minimal set, for set inclusion, of generators of C .

For a better understanding of the meaning of this statement we suggest that the reader go back to the example dealt with in Theorem 9 and the remark after its proof. We know that $x \leq y$ iff $\exists\, z \in C$, $x + z = y$ is an order relation for C . Then the intersection of all subsets B of C verifying (43) contains all minimal elements for $\leq$ in C . We will then prove that the set B of minimal elements in C for $\leq$ verifies (43) and that B generates C . Observing that any possible set of generators of C would verify (43), the proof will be done. We first prove that the set $S(x) \subset C$ of all $y \leq x$, $y \in C\backslash\{0\}$ is finite for all x . This will prove the first assertion. Let $\phi : \mathbb{N}^m \to C'$ be a surjective morphism. $\phi^{-1}x$ is finite, since, if not, there would exist $t', t'' \in \phi^{-1}x, t' > t''$, as it is well known, and $\phi(t'-t'')=0$. Then the tradict the fact that $y + z = 0$, y , $z \in C'$ implies $y = z = 0$. Then the union T of all elements in $\mathbb{N}^m$ smaller than t , for t running over $\phi^{-1}x$ is finite. $T \cap \phi^{-1}C$ is finite as well. Now $\phi(T \cap \phi^{-1}C)$ contains the set $S(x)$ which is thus finite.

It immediately follows by recurrence on Card $S(x)$ that x is in the cone hull over $\mathbb{Z}$ spanned by the minimal elements in $S(x)$. Then C is generated by B .

COROLLARY. *If a cone T in $\mathbb{Z}^n$ has rank r , then its polar C has a unique minimal set of generators.*

T contains a cone T' spanned by a linearly independent set L of n elements in T . The polar C' of T' and C verify the hypothesis of the theorem. Notice that an easy direct argument begins with defining a linear isomorphism of T' onto $\mathbb{N}^n$.

An application of Theorem 7 to bounded polyhedrons in K^n *(*K *the field of fractions of a linearly ordered domain* R*).*

Property 2: Let A *be an* $n \times m$ *matrix with entries in* R *. Let*

$$P = \{ t \mid tA \leq c \ , \ t \in K^n \}$$

be a non-empty bounded polyhedron not reduced to one point. Let B *be the matrix formed by the rows of* A *and* $-c$ *. Then the mapping* $\phi : t \rightsquigarrow \{\alpha t, \alpha)\}_{\alpha \in}$ *is a bijection of* P *onto the set of all rays in* $\hat{B}^*(K)$ *, the polar of* $\hat{B}(K)$ *in* K^m *.*

ϕ is injective, since if $\{\alpha t,\alpha)\}_{\alpha \in K_+} = \{(\beta t',\beta)\}_{\beta \in K_+}$, then $(t,1) \in \{(\beta t',\beta)\}_{\beta \in K_+}$, $(t,1) = (t',1)$ and $t = t'$.

We now have to check out that ϕ is surjective. Clearly ϕ maps every point in P onto some ray of $\hat{B}^*(K)$, since $tA - c \leq 0$ implies $\alpha tA - \alpha c \leq 0$, $\forall \alpha \in K_+$. Let $(t,\beta) \in \hat{B}^*(K) \setminus \{0\}$. We have $\beta \neq 0$, since, if not, we would have $tA \leq 0$ for $t \neq 0$ and P would not be bounded. If we show that $\beta > 0$, the proof will be done, since then $\beta^{-1}t \in \underline{P}$ and $\{(\alpha\beta^{-1}t,\alpha)\}_{\alpha \in K_+}$ is a ray of $\hat{B}^*(K)$. Suppose $\beta < 0$. By hypothesis $\underline{P}$ is not empty. Let $t' \in \underline{P}$. Then $(-\beta t',-\beta) \in \hat{B}^*(K)$. But also $(t,\beta) \in \hat{B}^*(K)$. Thus $(t - \beta t')A \leq 0$, and by boundedness, $t' = \beta^{-1}t$. This entails $(-\beta\beta^{-1}t,-\beta) = (-t,-\beta)$ is in $\hat{B}^*(K)$ with (t,β) . Hence $tA = \beta c$, $t'A = c$.

Since t' was any point in $\underline{P}$, we see that we could have another point t'' in $\underline{P}$, since $(t' - t'')A = 0$ with $t' - t''$ would mean that P is unbounded. On the other hand, $\underline{P}$ cannot reduce to one point; hence $\beta > 0$ and ϕ is a bijection as claimed.

THEOREM 11: Let

$$P = \{ t \mid tA \leq c \ , \ t \in K^m \}$$

be a bounded polyhedron. Let $B = \begin{bmatrix} A \\ -c \end{bmatrix}$ *as previously and let* S *be any suital subset of* R *that makes* $M(B)$ *an* S*-stable module. Then there exist a finite* $F \subset S$ *such that every* t *in* $P \cap R^m$ *is a convex linear combination with coefficients in* $F^{-1}R$ *of vertices of* P .

If P is empty or reduced to one point, the statement is obvious. If not, P verifies the hypothesis of Property 2 and we apply Theorem 7 to $\hat{B}^*(K)$. The restriction of ϕ to the vertices of P is a bijection onto the set of rays of $\hat{B}^*(K)$ which are not positive linear combinations of other rays and which generate $\hat{B}^*(K)$. In each of those rays we find a point in R^m such that we obtain, by Theorem 7 every point in $\hat{B}^*(K) \cap R^m$ by a linear combination of that finite set T of points with coefficients in the set of ≥ 0 elements of $F^{-1}R$. In particular, to every point t in $P \cap R^m$ corresponds a (t,1) in $\hat{B}^*(K) \cap R^m$ which is such a linear combination and may be seen a convex linear combination of images under ϕ with coefficients in $F^{-1}R$ of vertices of P .

Corollary: If $R = \mathbb{Z}$ *and if* $M(B)$ *is a unimodular module, only vertices of* P *may be integer points.*

Hence M(B) is a stable module with $S = \{1,-1\}$ and since $F \subset S$, $F^{-1}\mathbb{Z} = \mathbb{Z}$. Then all convex linear combinations with coefficients in $F^{-1}\mathbb{Z}$ are trivial.

4. *Linear equations over a Prüfer domain*

We will here apply Theorem 5 with for A the example dealt with in 1.2.2. Thus A is the set of all cosets of all submodules of the R-module G, R a Prüfer domain, with the form hG, where h is a finitely generated ideal of R. We assume as before $\phi_\alpha : G \to \alpha G$ is injective for $\alpha \neq 0$. Our aim is to obtain Theorem 4 of [2] as a corollary of the present #2. Theorem 5. The axiom of choice, or more precisely the axiom of maximal ideals, will not be avoided in the general case. However, we will give a proof which does not require it whenever R is a principal ideal ring or the domain of integers of an algebraic number field.

We first show how the first assertion of Theorem 4 of [2] is a particular case of the one #2. Theorem 5. Let M in #2. Th. 5 be finitely generated and denote by B the $n \times m$ matrix whose rows span M. Suppose, moreover that B has the form $[A,-I]$ where I is the $n \times n$ identity matrix. Now make $\Gamma_j = G$, $j = 1, \ldots, m-n$ and $\Gamma_j = r_i + H_i$ $j = m-n+i$, $i = 1, \ldots, n$, where $H_i = h_i G$, h_i a non-zero f.g. ideal, for all i. Finally we make $b_a = 0$, $\forall\, a \in M$.

The first assertion of Th. 5 becomes, writing $A = (a_{ij})$,

$$(1) \qquad \exists\, x \in G^{m-n}, \quad \sum_{1 \le j \le m-n} a_{ij} x_j \equiv r_i(H_i) \quad i = 1, \ldots, n.$$

Now in Th. 4 of [2] this assertion is proved to be equivalent to the following (

Let $\{0\} \neq H = \cap H_i$. We know that $H = hG$, where $h = \cap h_i$. Now let Y be the submodule of R^n of those elements $y = (y_i)_{1 \le i \le n}$ verifying

$$(2) \qquad y_i H_i \subset H, \quad i = 1, \ldots, n.$$

(3) $\quad \forall\ y \in Y\ ,\ yA \equiv 0(h)\ \text{ implies } \sum_{1\le i\le n} y_i r_i \in H\ .$

We prove the following specialization of #2. Theorem 5 for R a Prüfer domain.

THEOREM 12: Let M and M' be two supplementary modules of R^m ($M \oplus M' = R^m$). Let be given $\Gamma_j = r_j + H_j$, $H_j = h_j G$, h_j a f.g. ideal of S, for all j. We denote by $M_G^\perp$ the submodule of those elements $x \in G^m$ verifying $\sum_{0\le j\le m} a_j x_j = 0$, $\forall\ a \in M$. Denote by $h : h_j$ the annihilator of h_j mod h. We denote $(h:h_j)_{i\le j\le m}$ by Y.

(4) $$\Gamma \cap M_G^\perp \neq \{\phi\}$$

iff

(5) $$\forall\ y \in M \cap Y,\ \sum_{1\le j\le m} y_j r_j \equiv 0\ (H)\ .$$

For the sake of better understanding, we observe that, since M is an S-stable module for $S = R\backslash\{0\}$, any finite set $U \subset M$ with one element in U for each minimal support of M is a set of representatives of M. We will show that (5) implies (20) of Th. 5. We first check directly:

The condition is necessary.

$$x \in \Gamma \cap M_G^\perp\ ,\ \text{then}\ \ x_j = r_j + g_j\ ,\ g_j \in H_j\ ,$$

and

(6) $$0 = \sum y_j x_j = \sum y_j r_j + \sum y_j g_j\ .$$

Since $y_j \in h : h_j$, $y_j g_j \in y_j h_j G \in hG = H$, which proves (5).

We first prove Th. 12 for R a finitely principal ideal ring, that is a ring where every f.g.i. is principal. This will be used as a lemma but it also

gives a statement of special interest in itself, since whenever $M \cap Y$ has a finite basis, (5) needs to be verified for the element of this basis only. This is being possible only by the fact that $H \neq \{0\}$. What we have to prove is

$$(7) \qquad \forall\, u \in U\ ,\ \sum_{1\leq j\leq m} u_j r_j \in \sum_{1\leq j\leq m} u_j H_j\ .$$

We have

$$(8) \qquad \sum_{1\leq j\leq m} u_j h_j \supset \sum_{1\leq j\leq m} u_j h = h \sum_{1\leq j\leq m} (u_j) = \alpha h\ ,$$

or

$$(9) \qquad \beta \sum_j \alpha^{-1} u_j h_j = h\ ,$$

with $\beta, \alpha^{-1}u_j \in R$, for all j.

Since $M \oplus M' = R^m$, $y = (y_j)_{1\leq j\leq m} = (\beta\alpha^{-1}u_j)_{1\leq j\leq m} \in M$. By (9), $y \in (h : h_j)_{1\leq j\leq m}$ and (5) applies. We then have, by (9) again

$$(10) \qquad \sum_{1\leq j\leq m} \beta\alpha^{-1} u_j r_j \in H = \sum_{1\leq j\leq m} \beta\alpha^{-1} u_j h_j G\ ,$$

which implies (7).

Now, if we prove that Theorem 12 is valid for every localization R_p of R, p a maximal ideal of R (R_p is the smallest ring containing R in which every element not in p has an inverse) with G_p, M_p, $h_{j,p}$ defined as in [3], then Lemma 1 of [3], slightly modified, will obviously prove Th. 12.

We know that R_p is a valuation ring, then every finitely generated ideal of R_p is principal. Also if $M \oplus M' = R^m$, it is easily verified that $M_p \oplus M'_p = R_p^m$.

We now prove Theorem 12, without the help of assumed maximal ideals, for R the ring of integers of an algebraic number field. Every proper ideal is here

a product of prime ideals. [8].

If h is a product of prime ideals, here is a proof that leads to an algorithm for actually finding a solution to

$$\sum a_{ij}x_j = 0 \ , \ \forall \ a \in M \ . \tag{11}$$

$$x_j \equiv r_j(H_j) \ . \tag{12}$$

We write $h = p_1^{i_1} \dots p_s^{i_s}$, where p_j is a finitely generated prime ideal. For having convenient notations, we write $p_1^{i_1} \dots p_{t-1}^{i_{t-1}} = k$ and $p_t^{i_t} = q = p^i$, for some $t \leq s$. By recurrence we assume that we have a solution $x^{(k)}$ to (11) with

$$x_j^{(k)} = r_j + \gamma^{(k)} r_j + \ell_j^{(k)} \ , \ \gamma^{(k)} \in k \ , \ \ell_j^{(k)} \in H_j \ . \tag{13}$$

If we prove that there exists a solution $x^{(q)}$ to (11) with

$$x_j^{(q)} = r_j + \gamma^{(q)} r_j + \ell_j^{(q)} \ , \ \gamma^{(q)} \in q \ , \ \ell_j^{(q)} \in H_j \ , \tag{14}$$

we will then be through: (14) will give us the basis for recurrence and, moreover, since, by properties of Prüfer rings,

$$k + q = (1) \ , \ k \cap q = kq \ , \tag{15}$$

we have $\alpha \in k$, $\beta \in q$ with $\alpha + \beta = 1$, and we will obtain $x^{(kq)} = \beta x^{(k)} + \alpha x^{(q)}$ and, by recurrence,

$$x_j^{(h)} = r_j + \gamma^{(h)} r_j + \ell_j^{(h)} \equiv r_j(H_j) \ . \tag{16}$$

Hence we prove (14). $q = p^i$ and we consider the localization of R at p.

As in Lemma 1 of [3] we find an $x^{(p)}$ solution of (11) with the property

$$x_j^p = y^{(p)} r_j + \ell_j^{(p)} \ , \ \ell_j^{(p)} \in H_j \ , \ y^{(p)} \notin p \ . \tag{17}$$

Now $w = (y^{(p)}) + p^i$ is a f.g.i. which divides p^i . p^i is a f.g. ideal. This implies w is the whole ring or a power of p . But $y^{(p)} \in w$, and $y^{(p)}$ does not belong to any power of p . Then $w = R$ and there exists $\alpha \in R$:

$$\alpha y^{(p)} \equiv 1 \ (p^i) \ . \tag{18}$$

Making $\alpha x^{(p)} = x^{(q)}$, (14) will be verified.

An algorithm for the case $R = G$

The preceeding proof gives a hint for an algorithm for actually solving (11) and (12).

Suppose that we are provided a solution $x^{(q)}$ with

$$x_j^{(q)} \equiv r_j(q + h_j) \ , \tag{19}$$

for every highest power $q = p^{\ell}$ of a prime (ideal) factor of h . Then (19) satisfies (14) and the argument of the proof allows the build-up of a solution to (11) and (12).

Now $q + h_j = p^{\ell_j}$, $0 \le \ell_j \le \ell$, and our problem reduces to solving (11) with the condition

$$x_j \equiv r_j(p^{\ell_j}) \ , \tag{20}$$

p a prime ideal.

Let Q denote the quotient ring R/p^{ℓ}. We will show how a solution to (11) and (20) modulo p^{ℓ} provides a solution. Let us first point out that the union of classes of the ideal p^{ℓ_j} mod p^{ℓ} is the ideal p^{ℓ_j} of R so a solution to (20) mod p^{ℓ} is a solution to (20). We consider a basis of the module M_p spanned by M over the local ring R_p of R. We may take this basis in M and make it the rows of a matrix A. The ideal spanned by the principal determinants Det (A^J) of A is the whole R_p so that there exists an A^J with determinant not in p. The rows of A span $M \subset M_p$ over R_p and thus

$$(21) \qquad Ax = 0 \ , \ x \in R^m \Rightarrow \sum_{0 \le j \le o} a_j x_j = o \ , \ \forall \ a \in M \ .$$

We make a left unimodular transformation of A over R_p in order that A^J becomes the identity matrix and we multiply each row of the resulting matrix by suitable elements not in p in order that the obtained matrix B has all its entries in R but verifies (21) like A does.

So B has a diagonal of units in Q. Let $\delta = \text{Det } B^J$ be the product of those units of Q. Then we may define r'_j, by

$$(22) \qquad \delta r'_j \equiv r_j(Q) \ .$$

Now suppose we find a solution to

$$(23) \qquad Bx' \equiv o \ (Q) \quad x'_j \equiv r'_j \ (p^{\ell_j}) \ .$$

Then, denoting B by (b_{ij}), we have the relations in R

$$(24) \qquad \sum_{1 \le j \le m} b_{ij} x'_j = \gamma_i \in p^{\ell} \ ; \ i = 1, \ \ldots \ n \ .$$

We thus find a y, $s(y) \subset J$, with $\sum_{1 \le j \le m} b_{ij} y_j = \delta \gamma_i$,

and for $x = \delta x' - y$, we have in R

$$Bx = 0 \ , \tag{25}$$

hence (11) is satisfied by x .

We observe that $\delta x_j' \equiv r_j(p^{\ell_j})$ and $y_j \in p^{\ell} \subset p^{\ell_j}$. Then

$$x_j \equiv r_j(p^{\ell_j}) \ , \ j = 1, \ \dots \ , m \ . \tag{26}$$

Since we made sure that (23) solves the problem, we are left with solving (23), which is equivalant to

$$\sum_{1 \le j \le m} b_{ij}\alpha_j z_j \equiv - \sum_{1 \le j \le m} b_{ij} r_j' \ (Q) \tag{27}$$

with $(\alpha_j) \equiv p^{\ell_j} \bmod p^{\ell}$, since we know that Q has a finite chain of ideals and is thus a principal ideal ring. It may occur that $\ell_j = 0$, then $\alpha_j = 1$. Any solution $z = (z_j)_{1 \le j \le m} \in Q^m$ to (27) gives a solution to (23) and hence solves the problem. There is no problem to diagonolize $(b_{ij}\alpha_j) \bmod Q$, with a left unimodular transformation.

Remark: If M is the module spanned by the rows of an echelon matrix A , that is an $n \times m$ matrix A having the identity matrix as a submatrix A^J , then δ of (22) is one and if the problem has a solution, then if h_j is the zero ideal for some $j \notin J$, the algorithm will provide a solution as well.

5. *Some properties of submodules of* R^n , R *a linearly ordered domain.*

Denote by $\overline{R}$ the linearly ordered field of fractions of a linearly ordered domain R .

5.1 *Definition:* R *separates its fractions whenever*

$$(1) \qquad \forall\ \alpha\beta^{-1} \in \overline{R}\ ,\ \exists\ \gamma \in R : \gamma \geq \alpha\beta^{-1}\ .$$

5.2 *Examples*

Notice that this does not mean that for any two elements in $\overline{R}$, then there exists an element in R larger than the first one smaller than the other, since this is not true for $\mathbb{Z}$, and $\mathbb{Z}$ verifies (1).

Let us show that if K is a linearly ordered field, $K[X]$, the ring of polynomials in X over K separates its fractions if a polynomial is positive in $K[X]$ whenever its leading coefficient is positive.

If $\alpha\beta^{-1} \leq 0$, we make $\gamma = 0$. If $\alpha\beta^{-1} > 0$ we write the fraction in order that $\alpha > 0$, $\beta > 0$. If $\beta \in K$, we make $\gamma = \alpha\beta^{-1}$. If $\beta \notin K$, we have $\beta > 1$ and

$$(2) \qquad \alpha\beta^{-1}\beta > \alpha\beta^{-1}\ .$$

Then $\gamma = \alpha$ verifies (1).

However, if a polynomial is positive in $K[X]$ whenever the coefficient of its term with lowest degree is positive, then $K[X]$ does not separate its fractions. Let us show indeed that X^{-1} is larger than any polynomial in $K[X]$. We know that 1 is > 0 , by the axioms of an ordered domain. Then if α is any polynomial in $K[X]$, we have

(3) $$1 > \alpha X ,$$

since the constant term of αX is 0. Now X is > 0, then X^{-1} is > 0 and

(4) $$X^{-1} \cdot 1 > X^{-1} \cdot \alpha X = \alpha .$$

5.3 *The ideal of inseparability*

Property 1: Let

$$T_\rho = \{\beta \mid \forall\ \delta \in R ,\ \delta\beta < \rho\} \quad \text{for} \quad \rho > 0 .$$

Then T_ρ *is an ideal. If* $\rho \geq 1$, T_ρ *is a prime ideal.*

If $\beta \in T_\rho$, then $-\beta \in T_\rho$ since $-\beta\delta \geq \rho$ implies $\beta(-\delta) \geq \rho$. Let $\beta', \beta \in T_\rho, \beta' \leq \beta$, and let us show that $\beta + \beta' \in T_\rho$.

(5) $$(\beta' + \beta)\delta \leq 2\beta\delta = \beta\delta' < \rho .$$

Now if α is any element in R, $(\alpha\beta)\delta = \beta\delta' < \rho$. If $\rho \geq 1$, $T\rho$ is a prime ideal since,

$$\alpha\delta' \geq \rho > 0 ,\ \beta\delta'' \geq \rho \Rightarrow \alpha\delta'\beta\delta'' \geq \alpha\delta'\rho \geq \rho^2 \geq \rho$$

which means $\alpha\beta \notin T_\rho$.

Note: If $\rho < 1$, T_ρ may not be a prime ideal. In the example previously given of $K[X]$ with $X < 1$, T_X is not a prime ideal since then $T_X = (X^2)$.

Definition: 1. We call T_ρ the ideal of inseparability if $\rho = 1$. In general T_ρ is the ideal of ρ-inseparability of R.

2. We say that R ρ-separates its fractions if

(6) $$\forall\, \alpha,\beta \in R\ \exists\, \gamma \in R : \gamma \geq \alpha\beta^{-1} \cdot \rho \ .$$

THEOREM 13: A ring ρ*-separates its fractions iff its ideal of* ρ*-inseparability* T_ρ ***reduces to*** $\{0\}$. T_ρ *is an interval. Now let* $\rho \geq 1$. *If* R_+ *is the set of pesitives of* R , $Q = \{\alpha + T_\rho | \alpha \in R_+\}$ *is a set of positives for* R/T_ρ *which gives* R/T_ρ *the structure of a linearly ordered domain which* $\overline{\rho}$*-separates its fractions.*

If $T_\rho \neq \{0\}$, then, $\exists\, \beta \in T_\rho$, $\beta > 0$. We see that $\beta^{-1}\rho$ is larger than any $\delta \in R$ since $\delta \geq \beta^{-1}\rho$ would mean $\beta\delta \geq \rho$.

On the other hand if R does not separate its fractions, there exists at least one $\beta \neq 0$ with

(7) $$\forall\, \delta \in R : \beta\delta < \rho \ ,$$

since, if not, to every $\beta \in 0$ would correspond a $\delta \in R$ with $\beta\delta \geq \rho$, and for any $\alpha > 0$, $\alpha\delta\beta \geq \alpha\rho$, $\alpha\delta \geq \alpha\beta^{-1}\rho$.

This means that to any fraction $\alpha\beta^{-1}$ corresponds a $\gamma = \alpha\delta$ which is larger than $\alpha\beta^{-1}\rho$. Let $\alpha \leq \beta \leq \gamma$, with $\alpha,\gamma \in T_\rho$. Then for every $\delta > 0$, $\beta\delta \leq \gamma\delta < \rho$ and for every $\delta < 0$, $\beta\delta \leq \alpha\delta < \rho$. Consequently $\beta \in T_\rho$ and T_ρ is an interval. If $\rho \geq 1$, R/T_ρ is a domain, since T_ρ is a prime ideal denote by Q the set of residue classes $T_\rho + \alpha$ where α runs over R_+ . The relations $Q + Q \subset Q$, $QQ \subset Q$, $-Q \cup Q = R/T_\rho$ follows from the correspondin relations for R_+ . Now we have to show that T_ρ is the only element in $-Q \cap$ Let $-\alpha + T_\rho \in -Q \cap Q$, $\alpha \geq 0$. We must have $\beta \in -\alpha + T_\rho$, for some $\beta \geq 0$, or $\alpha + \beta \in T_\rho$. Then $\forall\ \delta > 0$, $\alpha\delta \leq (\alpha + \beta)\delta < \rho$ and $\alpha \in T_\rho$.

Now the order relation for R/T_ρ is

$$\bar{\alpha} \leq \bar{\beta} \text{ iff } \forall\, \alpha \in \bar{\alpha}\,,\ \forall\, \beta \in \bar{\beta}\,,\ \alpha \leq \beta \text{ in } R\,.$$

Thus if (7) occurs for some $\bar{\beta} \in R/T_\rho$, this means every $\beta \in \bar{\beta}$ is in T_ρ, that is, $\bar{\beta} = 0$. Hence R/T_ρ $\bar{\rho}$-separates its fractions.

5.4 Let Y be a finite set. R^Y will be ordered canonically by its set $P = R_+^Y$ of positives. We denote by Π_J the linear mapping

$$(x_i)_{i\in Y} \rightsquigarrow (x_i)_{i\in J}$$

of R^Y onto R^J, $J \subset Y$. The *support* of $M \subset R^Y$ is the set of $i \in Y$ for which $\Pi_i M \neq \{0\}$.

Lemma: Let J be the support of a submodule M of R^Y. If R separates its fractions, then M is a directed group iff

$$(8) \qquad \exists\, v \in M\,,\ v_i > 0\,,\ \forall\, i \in J\,.$$

There are two equivalent ways of defining a directed group M. The first is to say that $\forall\ x,y \in M$, $\exists\, z \in M$ with $z \geq x$, $z \geq y$. The other uses the addition of M. It says that any x in M may be written $x = z - y$, where $z \geq 0$, $y \geq 0$, $x,y \in M$. If M is directed, to every x corresponds a z with $z \geq x$, $z \geq -x$. Thus by summing Card J of such z one obtains the v of (8).

We now prove that (8) is a sufficient condition. If $a \in -P$, $a = 0-(-a)$, thus d is the difference of two elements in P. Now we may suppose $a_i > 0$ for some i, and there exists an s such that

$$(9) \qquad v_s a_s^{-1} = \min_{a_i>0} v_i a_i^{-1}\,.$$

Since R separates its fractions, there exists a $\gamma \in R$:

$$\gamma \geq v_s^{-1} \quad . \tag{10}$$

Thus

$$P \cap M \ni w = \gamma a_s v \geq v_s^{-1} a_s v \geq a \quad . \tag{11}$$

Finally,

$$a = \gamma \alpha_s v - (\gamma a_s v - a) \in P \cap M - P \cap M \quad .$$

Counterexample for R not separating its fractions.

Let $K[X]$ be the previous example. (That is, $X < 1$.) Consider the module M spanned by $a = (-1 + X\ ,\ 1 + X\ )$ and $b = (1,-1)$. $a + b = (X,X)$ verifies (8). We show that nevertheless M is not directed. There should exist a $z = \alpha a + \beta b \geq b$ and $\geq -b$. That is

$$-\alpha + \alpha X + \beta \geq 1$$

$$\alpha + \alpha X - \beta \geq 1 \tag{12}$$

or

$$1 + \alpha - \alpha X \leq \beta \leq \alpha + \alpha X - 1 \quad . \tag{13}$$

But $1 - \alpha X$ is > 0 . Thus (13) entails

$$\alpha < \beta < \alpha \quad , \tag{14}$$

which is impossible.

Let us denote by Δ_J the operator $\mathrm{Ker}\Pi_{Y \setminus J}$. Notice that M is directe iff it is spanned by a subset of P . We investigate a case where this subset could be finite.

THEOREM 14: Let R *be a linearly ordered Noetherian domain which separates its fractions. A submodule* M *of* R^Y *(for Card* $Y < \infty$*) is directed iff it is spanned by a finite subset of* $P = R_+^Y$ *. Moreover, if* M *is directed, then every maximal sequence*

$$\{0\} \neq \Delta_{J_0} M \subset \Delta_{J_1} M \subset \ldots \subset \Delta_{J_s} M \subset \ldots \subset M \tag{16}$$

of distinct directed modules has length rank M *. More specifically if* R *is a principal ideal ring,* $\Delta_J M$ *is a direct factor of* $\Delta_{J'} M$ *,* $s < \dim M - 1$ *. This implies* M *has a basis in* $\underline{P}$ *.*

The condition is sufficient.

Let $B \subset P$ be a finite set spanning M . Then $M = \hat{B}(R) - \hat{B}(R) \subset P \cap M - P \cap M$ and M as directed.

Proof of the main assertions.

$$M = M_1 + \Delta_J M \tag{15}$$

where J is any maximal subset of Y for which $\Delta_J M$, distinct from M , is directed. If we also prove that $M/\Delta_J M$ has rank 1 and that M_1 is spanned by a finite set in P , the proof of the first two assertions will be done, as we will see. Indeed the vector space spanned by M over $\overline{R}$ in $\overline{R}^Y$ has then a basis formed with any element in $M_1 \setminus \Delta_J M$ and a basis of $\Delta_J M$. Then

$$\text{rank } M = 1 + \text{rank } \Delta_J M \tag{16}$$

Every maximal sequence (16) ends by some $\Delta_J M \subset M$ where J is a maximal subset of Y for which $\Delta_J M$, distinct from M , is directed. Since we claim that rank $\Delta_J M$ = rank M - 1 , the proof of the second assertion will be done by

recurrence on the rank. But by recurrence as well, $\Delta_J M$ is spanned by a finit set in P. Hence $M = M_1 + \Delta_J M$ is spanned by a finite set in P.

Let $s \in Y \backslash J$ such that $\Pi_s M \neq \{0\}$. By hypothesis, the ideal $\Pi_s M$ is finitely generated and

$$\Pi_s M = (d^1{}_s, d^2{}_s, \ldots, d^t{}_s) , \tag{17}$$

where $D = \{d^1, d^2, \ldots, d^t\} \subset M$. We may choose $d^j_s > 0$, $\forall$ j. We denote by M'_1 the module spanned by D and we first show that

$$M = M'_1 + \Delta_J M . \tag{18}$$

Since every element in M is the difference of two elements in $M \cap P$, it is enough to show that any $w \in M \cap P$ is in the second member of (18). We first show that either $w_s > 0$ or $w \in \Delta_J M$. We know, since $\Delta_J M$ is directed, tha if $J' \subset J$ is the support of $\Delta_J M$, there exists a $v \in \Delta_J M$, $v_j > 0$, $\forall j \in$ Consider any $d \in M'_1 \backslash \Delta_J M$ with $d_s > 0$. Let $w_\ell d_\ell^{-1}$ be the smallest fractio $w_j d_j^{-1} \geq 0$ where d_j runs over the componants of d for which $d_j > 0$. We see that

$$b = v + d_\ell w - w_\ell d \in P . \tag{19}$$

Now, $b_j > 0$, $\forall j \in J'$ and $b_\ell = 0$. Since there does not exist a support o a directed submodule of M properly contained in the support of M and havin J' as a proper subset, by the maximality of J for $\Delta_J M$ directed by the lemma, we must have

$$b \in \Delta_J M . \tag{20}$$

In particular, if $w \notin \Delta_J M$, we cannot have $w_s = 0$ since then s could be chosen as ℓ and for $w_j > 0$, $j \notin J$, $d_\ell w_j - w_\ell d_j = d_\ell w_j = b_j$ would be > 0, contradicting (20). By (17) we are thus able to take $d \in M_1'$ such that $d_s = w_s$. Finally, by (19) and (20)

(21) $$\forall\, j \notin J,\ d_\ell w_j = w_\ell d_j .$$

Making $j = s$ in (21) shows that $d_\ell = w_\ell$, and consequently, since $d_\ell > 0$,

(22) $$\forall\ j \notin J,\ 0 \le w_j = d_j .$$

(22) entails

(23) $$w - d \in \Delta_J M ,$$

which proves (18).

Since R is a ring which separates its fractions we may find $\beta > 0$ such that

$$\forall\, d^h \in D,\ d^h + \beta v \in P .$$

This comes from $d_j^h \ge 0$, $j \notin J$ as it is entailed from (19), (20) using $w \in M$, $w_j > 0$; for every j in the support of M. The $d^h + \beta v$ will now span M_1 and clearly

(24) $$M_1 + \Delta_J M = M_1' + \Delta_J M = M .$$

What is left to be shown is that for any two $d^h + \beta v$, $d^k + \beta v$ with $d^h, d^k \in D$ there exists a fraction ε in $\overline{R}$ such that

(25) $\varepsilon(d^h+\beta v) \equiv d^k+\beta v$ modulo the $\overline{R}$-vector space spanned by $\Delta_J M$ in $\overline{R}^Y$.

We will see that $\epsilon = d_j^h/d_j^h$, $\forall\ j \notin J$, j in the support of M . For, we consider (19) and (20) with $w \in M \cap P$, w having the pargest possible number of > 0 componants. We have

$$(26) \qquad \begin{cases} d_j^h = d_\ell^h w_j / w_\ell \ , \ \forall\ j \notin J \\ d_j^k = d_{\ell'}^k w_j / w_{\ell'} \ , \ \forall\ j \notin J \ . \end{cases}$$

or

$$(27) \qquad a_j^h = d_j^k d_\ell^h w_{\ell'} / d_{\ell'}^k w_\ell \ , \ \forall\ j \notin J \ ,$$

which proves (25).

Let us now investigate the more special case of R a principal ideal ring. Here, D reduces to one element. M_1 is spanned by one element which is not in $\Delta_J M$. Since R is a domain, $M_1 \cap \Delta_J M = \{0\}$ and the $+$ of (18) may be changed into the $\oplus$ of a direct sum. By recurrence, M is then the direct sum of rank M submodules, each one generated by an element in $P\backslash\{0\}$. This means that M has a basis in P , which was the last assertion of the theorem.

A question arises. Is Theorem 1 the best statement, or could we have $\Delta_{J_s} M$ a direct factor of $\Delta_{J_{s+1}} M$, when R is a Noetherian ring but not a principal ideal ring. Here is a counterexample.

Let M be the module spanned in $(\mathbb{Z}[X])^2$ by the two elements a and b , $a = (1, X+1)$, $b = (0, X-1)$. $\mathbb{Z}[X]$ is ordered with $X > 1$. M is directed. $c = (X-1)a - (X+1)b = (X-1, 0) \in P$. Then for $J = \{1\}$, J is maximal for $\Delta_J M$ being distinct from M and directed, by the lemma. Actually $\Delta_J M$ is the submodule of M spanned by c . For, if $x = \alpha a + \beta b \in \Delta_J M$, we

must have $\alpha(1) = 0$ and $\beta(-1) = 0$. Thus α belongs to the ideal $(X - 1)$ and β belongs to $(X + 1)$. Since the first componant of $\alpha a + \beta b$ does not depend on β, it is a multiple of $X - 1$. The second componant of $\alpha a + \beta b$ being zero, every element in $\Delta_J M$ is a multiple of c. We show that (c) cannot be a direct factor of M. Suppose

$$M = (c) \oplus M_1 . \tag{28}$$

We see that necessarily b belongs then to M_1. Then, by the requirement $M_1 \cap \Delta_J M = \{0\}$, we have

$$M_1 \subset \Delta_{\{2\}} M , \tag{29}$$

and since $\Delta_{\{2\}} M \subset (c) \otimes M_1$, $\Delta_{\{2\}} M \subset M_1$. The conclusion is

$$M = (c) \oplus \Delta_{\{2\}} M . \tag{30}$$

This is impossible since $a \notin (c) \oplus \Delta_{\{2\}} M$.

R is now a principal ideal ring.

Corollary 1. Let M be a directed submodule of R^Y and let L be a direct factor of M, directed as well. Then, there exists a directed module N such that $L \oplus N = M$. L has a basis contained in P which may be completed into a basis of M contained in P.

By hypothesis, $M = L \oplus L'$. Let $v \in M$ be the element verifying (8) and let $w \in L$ be the one obtained by substituting L to M in the lemma. Let B be a basis of L' :

$$v = \sum_{x \in B} \alpha_x x + t , \quad t \in L \tag{31}$$

and B may be chosen in order that

(32) $$\alpha_x \geq 0 \ , \ \forall x \in B \ .$$

Now $\beta > 0$ is chosen in order that the set $\beta w + B = B'$ has all elements with all > 0 componants in the support of L. Then $\sum_{x \in B} \alpha_x(\beta w + x) \geq \sum_{x \in B} \alpha_x x$ has all > 0 componants in the support of M. Hence the module N spanned by B' is directed and $L \oplus N = M$.

Corollary 2. Let A be an $m \times n$ matrix, $m < n$, with entries in R_+. If the columns of A span R^m, then A may be completed into a square invertible matrix with entries in R_+.

5.5 In #3, we have considered finitely generated cones in K^n and their intersections with R^n, K the field of fractions of R. We will use Th.14 for studying the intersections of their faces with R^n.

Definition. A face of dimension i of a convex set C of K^n is a maximal subset F with dimension i of C such that the convex hull of $C \backslash F$ does not meet F.

Let C be a finitely generated pointed cone of dimension k in K^n. (That is C is not reduced to zero and $-C \cap C = \{0\}$). We may then define a morphism ϕ of K^n onto K^k whose restriction at the smallest subspace E containing C is an isomorphism onto K^k. Consequently, the polar of ϕC in K^k has rank k as the polar of a pointed cone should, and its image under ϕ^{-1} in K^n, which we may define straightforward by

(33) $$C_E^* = \{x \mid x \in E \ , \ \forall\, y \in C \ , \ \langle x,y\rangle \leq 0\} \ ,$$

has a finite set U of generators the rank of which is k. We have

$$E \oplus E^\perp = K^n \ ,$$

and ϕ may be defined in order that $\phi E^\perp = \{0\}$, where $E^\perp$ is the orthogonal of E in K^n; rank $E^\perp = n - k$.

Let V be the union of U and a basis of $E^\perp$. We denote by L the K-vector space of the $(\alpha_u)_{u\in V}$, $\alpha_u \in K$, such that

(34) $$\sum_{u\in V} \alpha_u u = 0 \ .$$

Since rank $V = n$, that is, the maximum rank for a subset of K^n, the morphism $\psi : K^n \to K^V$ defined by $\psi x = (\langle x,u\rangle)_{u\in V}$, $\forall\, x \in K^n$ is an isomorphism of K^n onto $L^\perp$, the orthogonal of L in K^V. We observe that

(35) $$x \in -C \iff \psi x \in \Delta_U L^\perp \cap K_+^V \ ,$$

since the polar of C_E^* in E is C. Now, since ϕC_E^* is the polar cone in K^k of a cone ϕC with rank k, ϕC_E^* is a pointed cone, and so is C_E^*. This means $\Delta_U L \cap K_+^V = \{0\}$ and, by a well known theorem on linear inequalities (which may be deduced from #2 Th. 4) there exists an $x \in K^n$ such that $\langle x,u\rangle > 0$, $\forall\, u \in U$. But we may find a $y \in E^\perp$ such that $\langle y,u\rangle = \langle x,u\rangle$, $\forall\, u \in V\backslash U$. Then for $z = x - y$, $\psi z \in \Delta_U L^\perp \cap K_+^V$, and $\langle z,u\rangle > 0$, for all $u \in U$. This means that $\Delta_U L^\perp$ is directed.

Property 2. F is a face of C iff $-\psi F = \Delta_J L^\perp \cap K_+^V$, for some $J \subset U$ where $\Delta_J L^\perp$ is directed.

The condition is necessary.

If F is a face of C, $-\psi F$ is a subset of $\Delta_U L^\perp \cap K_+^V$. Let J be the union of the supports of the elements in $-\psi F$. Then $J \subset U$, and there exists an element v in $-\Psi F$ with support J. This means that $\Delta_J L^\perp$ is directed. We have $-\psi F \subset \Delta_J L^\perp \cap K_+^V$ and we must show that $-\psi F = \Delta_J L^\perp \cap K_+^V$. Suppose $w \in \Delta_J L^\perp \cap K_+^V$ and $w \notin -\psi F$. Since $s(w) \subset s(v) = J$, there would exist $\alpha > 0$ such that $v - \alpha w \geq 0$. For example $\alpha = \min_{w_j>0} v_j w_j^{-1}$. By the definition of a face, if i is the dimension of F, $F \cup \{\psi^{-1} w\}$ has rank $i + 1$, since $-\psi^{-1} w \in C$. Then $v - \alpha w$ is not in $-\psi F$, since, if it were, w would be a linear combination of elements in $-\psi F$. Finally if such a w would exist, $v/2$ would be in the middle of the segment $[(v - \alpha w), \alpha w]$ whose extremities are not in $-\psi F$. This implies F could not be a face.

The condition is sufficient.

$\Delta_J L^\perp$ is directed, J is contained in U and we must show that $-\psi^{-1}(\Delta_J L^\perp \cap K_+^V) = F$ is a face. F is certainly contained in C and it is a maximal set with dimension rank F since, if $x \in C \setminus F$, the support of $-\psi x$ is not contained in J and consequently

$$\operatorname{rank}((\Delta_J L^\perp \cap K_+^V) \cup \{-\Psi x\}) = \operatorname{rank}(\Delta_J L^\perp \cap K_+^V) + 1 .$$

Now every element in $-\psi(C \setminus F)$ has a support which is not contained in J. Then a convex linear combination of such elements has a support which cannot be contained in J. This completes the proof.

Corollary 3. Let C be a finitely generated pointed cone in R^n, where K is the field of fractions of a ring R verifying the hypothesis of Theorem 2.

Denote by M_i *the module spanned over* R *by* $R^n \cap C_i$ *, where* C_i *is the face with dimension* i *of the sequence*

$$C_0 \subset C_1 \subset \ldots \subset C_k = C \ . \tag{36}$$

Then M_i *(which has rank* i *) is spanned by a finite subset of* $C_i \cap R^n$ *. If* R *is a principal ideal ring,* M_i *is a direct factor of* M_{i+1} *,* $i < k$ *.* M_k *is a direct factor of* R^n *.*

Let us denote by N the module ψR^n and by M the module $\Delta_U N$. Now by Property 2

$$-\psi C_i = \Delta_{J_i} L^{\perp} \cap K_+^V \ , \ i = 0, \ \ldots \ ,k \tag{37}$$

where $\Delta_{J_i} L^{\perp}$ is directed. $M \cap \Delta_{J_i} L^{\perp}$ is directed as well, since if $v \in \Delta_{J_i} L^{\perp}$, $v_j > 0$ for all j in the support of $\Delta_{J_i} L^{\perp}$, there exists an $\alpha \in R$ such that $\alpha \psi^{-1} v \in R^n$ and then $\alpha v \in M$. Let $B_i \subset R_+^V$ (Theorem 2) be a finite set generating $M \cap \Delta_{J_i} L^{\perp}$. Then $\psi^{-1}(-B_i)$ is a subset of $C_i \cap R^n$ which spans M_i , since $\psi(M_i) \subset M \cap \Delta_{J_i} L^{\perp}$. (M_i has the same rank i as C_i since to i linearly independant elements in C_i over K correspond i linearly independant elements in $C_i \cap R^n$). This entails

$$\psi(M_i) = M \cap \Delta_{J_i} L^{\perp} \ , \ i = 0, \ \ldots \ ,k \ . \tag{38}$$

Now, we have $M \cap \Delta_{J_i} L^{\perp} = \Delta_{J_i} M$, since $M \cap \Delta_{J_i} L^{\perp} = \Delta_U \psi R^n \cap \Delta_{J_i} L^{\perp}$ $= \Delta_{J_i} \psi R^n \cap \Delta_{J_i} \psi K^n = \Delta_{J_i} \Delta_U \psi R^n = \Delta J_i M$. The sequence (M_i) is thus mapped by ψ onto a sequence of directed modules

(39) $$\Delta_{J_o} M \subset \ldots \subset \Delta_{J_i} M \subset \Delta_{J_{i+1}} M \subset \ldots \subset \Delta_{J_k} M = M$$

which is easily seen to be maximal since rank $\Delta_{J_i} M = i$, $\forall\, i$. Hence the first assertion regarding principal ideal rings follows from Theorem 2. Now $-\psi(C \cap R^n) = -\psi M_k = M$. If $\alpha x \in \psi^{-1}M$ with $\alpha \in R$, $x \in R^n$, then

$$\forall\, u \in V\backslash U \ , \ \langle \alpha x, u \rangle = 0 \ , \text{ thus } \ \forall\, u \in V\backslash U \ , \ \langle x, u \rangle = 0 \ ,$$

which means $\psi x \in M$, or $x \in \psi^{-1}M$. Hence $\psi^{-1}M = M_k$ is a direct factor of R^n .

If R does not separate its fractions, corollary 3 fails. Consider the cone C spanned by $(1,1 - X)$ and $(1,1+X)$ in K^2 , where $R = Q[X]$ for any linearly ordered field Q and where $X < 1$. If (α,β) is any element in C , it is easily seen that $\alpha(X - 1 \ , \ X + 1) + \beta(1 \ , \ -1)$ is ≥ 0 . If the corollary were true, there would be in $C \cap R^2$ a basis of a direct factor with dimension 2 of R^2 , that is, of R^2 itself. To this basis would then correspond a basis of ≥ 0 elements of the R-module spanned by $(X - 1 \ , \ X + 1)$ and $(1, -1)$. This would entail that any element is the difference of two ≥ 0 elements. This fails to be true as proved in 5.6.

References

[1] P. Camion, Modules Unimodulaires. Journal of Combinatorial Theory, Vol. 4. 1968.

[2] P. Camion, L. S. Levy and H. B. Mann. Linear Equations over a Commutative Ring. Journal of Algebra, Vol. 18 p. 432 - 446 (1971).

[3] P. Camion, L. S. Levy and H. B. Mann. Prüfer Rings. Journal of Number Theory, Vol. 5 No. 2, April 1973.

[4] P. Camion, Characterization of Totally Unimodular Matrices. Proc. Amer. Math. Soc. 16, No. 5 (Oct. 1965).

[5] N. Bourbaki, Algebra, Chap. VI (Groupes et corps ordonnés) Herman, Paris.

[6] S. Eilenberg and M. P. Schützenberger, Rational sets in Commutative Monoïds. Journal of Algebra 13, 173 - 191 (1963).

[7] H. J. Ryser, Combinatorial Mathematics. The Carus Mathematical Monographs, John Wiley and Sons, Inc. (Ch. 6. Theorem 1.1).

[8] H. Mann, Introduction to Algebraic Number Theory. The Ohio State University, Columbus.

[9] P. Camion and J. F. Maurras, Polyèdres à sommets entiers daus le cube unité. (To be published).