Alexander Abian; Paula Kemp; Sergi Sverchkov

An iterative construction of bases for finitely generated modules over principal ideal domains

Czechoslovak Mathematical Journal, Vol. 43 (1993), No. 4, 577–582

Persistent URL: http://dml.cz/dmlcz/128432

Czechoslovak Mathematical Journal, 43 (118) 1993, Praha

AN ITERATIVE CONSTRUCTION OF BASES FOR FINITELY GENERATED MODULES OVER PRINCIPAL IDEAL DOMAINS

ALEXANDER ABIAN, Iowa, PAULA KEMP, SERGI SVERCHKOV, Springfield

(Received November 11, 1991)

The existence of a set of linearly independent generators (i.e., a basis) for a finitely generated Module V over a Principal Ideal Ring (i.e., a generalization of the Fundamental theorem of Abelian groups) is proved here in a well motivated way which starts by choosing from all possible sets of generators of V a set G of generators of V such that G has a smallest number of generators and such that G also contains an element, say, b of the minimal (as defined below) order. Then the process is repeated for the submodule of V generated by $G - \{b\}$, etc. The completion of the process yields a basis of V. The proofs are considerably simpler and more lucid than those known in the existing literature and remain the same whether V does or does not have elements of infinite order.

In what follows we shall use well known items and facts of any principal ideal domain R such as the existence of a greatest common divisor of finitely many elements of R (and its representation as a linear combination of these elements) the units and associates of R and the fact that R is a unique factorization domain, etc. [2, 3].

Lemma 1. *Let R be a principal ideal domain and let $a_n, \ldots, a_1$ be elements of R with a greatest common divisor g_n, i.e.,*

$$(a_n, \ldots, a_1) = g_n. \tag{1}$$

Then there exists an n by n matrix M_n with entries over R, whose first row is $a_n, \ldots, a_1$ and whose determinant is equal to g_n, i.e.,

$$\det M_n = g_n. \tag{2}$$

Proof. We use induction to prove the Lemma. The statement of the Lemma is trivially true for $n = 1$. Let us assume that the Lemma is true for the $n-1$ elements

$a_{n-1}, \ldots, a_1$ of R, i.e.,

(3) $$(a_{n-1}, \ldots, a_1) = g_{n-1}$$

and that there exists an $n-1$ by $n-1$ matrix M_{n-1} such that

(4) $$M_{n-1} = \begin{bmatrix} a_{n-1} & \cdots & a_1 \\ & \cdots & \\ & \cdots & \end{bmatrix} \quad \text{and } \det M_{n-1} = g_{n-1}.$$

Since R is a principal ideal domain from (1) and (3) it follows that

(5) $$g_n = pa_n + qg_{n-1} \quad \text{for some elements } p \text{ and } q \text{ of } R.$$

From (3) and (5) it follows that

(6) $$p(a_{n-1}/g_{n-1}), \ \ldots, \ p(a_1/g_{n-1}) \quad \text{are } n-1\text{-elements of } R.$$

Let M^*_{n-1} be an $n-1$ by $n-1$ matrix which is obtained by replacing the first row of the matrix M_{n-1} by the $n-1$ elements of R given in (6). But then, clearly, from (4) and (6) it follows that

(7) $$\det M^*_{n-1} = p.$$

Now, let us consider the n by n matrix M_n which extends the $n-1$ by $n-1$ matrix M^*_{n-1} on top by one row $a_n, a_{n-1}, \ldots, a_1$ (i.e., precisely a_n followed by the elements of the first row of matrix M_{n-1}) and on the left by one column as shown below:

(8) $$M_n = \begin{bmatrix} a_n & a_{n-1} & \cdots & a_1 \\ -q & & & \\ 0 & & M^*_{n-1} & \\ \vdots & & & \\ 0 & & & \end{bmatrix}.$$

But then expanding the determinant of M_n along its first column, from (4), (5) and (7) it follows $\det M_n = g_n$. Thus, M_n is an n by n matrix with entries over R, whose first row is $a_n, \ldots, a_1$ and M_n satisfies (2). Hence, the proof of the Lemma is complete. □

Corollary 1. *Let $a_1, \ldots, a_n$ be n relatively prime elements of a principal ideal domain R. Then there exists an n by n matrix M_n with entries over R whose first row is $a_1, \ldots, a_n$ such that $\det M = 1$. Moreover, M_n is invertible and M_n^{-1} is an n by n matrix with entries over R.*

Proof. By the assumption, $(a_1, \ldots, a_n) = 1$. Thus, from (1) and (2) it follows that $\det M_n = 1$. But then clearly, M_n^{-1} exists and its entries are over R. □

Lemma 2. *Let R be a principal ideal domain and V be an R-module generated by n generators $g_1, \ldots, g_n$. Let $a_1, \ldots, a_n$ be n relatively prime elements of R. Then V can be also generated by a set of n generators includes $a_1g_1 + \ldots + a_ng_n$ as one of the generators.*

Proof. Let M_n be the matrix mentioned in Corollary 1. Clearly,

$$(9) \qquad \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix} = M_n^{-1}M_n \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix} = M_n^{-1} \begin{pmatrix} a_1g_1 + \ldots + a_ng_n \\ \vdots \end{pmatrix}.$$

Obviously, the elements of the rightmost column appearing in (9) form a set of generators of V. Indeed, as (9) shows everyone of the n generators $g_1, \ldots, g_n$ of V is a linear combination of the elements of the rightmost column appearing in (9). But then since $a_1g_1 + \ldots + a_ng_n$ is one of the elements of the rightmost column appearing in (9), we see that there exists a set of n generators of V which includes $a_1g_1 + \ldots + a_ng_n$ (which could be 0) as one of the generators. Thus, Lemma 2 is proved. □

Remark 1. We note that the proof of Lemma 1 gives us a constructive method of building of the matrix M_n and that Lemma 2 gives us a constructive method of replacing a set of generators of R with another set of generators of R [cf. 1].

Let R be a principal ideal domain, we recall that elements x and y of R are called associates (denoted by $x \simeq y$) iff $x = uy$ for some unit u of R. We define order $<$ (read: less than) in R as follows:

$$(10) \qquad x < y \quad \text{if and only if } x \mid y \quad \text{and } x \not\simeq y,$$

i.e., x divides y and x and y are not associates. This means that x and y are not associates and that y is an elements of the ideal generated by x. Since R has no infinite properly ascending chain of ideals [3, p. 121], we have:

(11) every nonempty subset of R has a minimal (i.e., $<$ -minimal) element.

Let V be a module over a principal ideal domain R. As expected, a minimal annihilator (if it exists) of an element v of R is called order of v (denoted by $\operatorname{ord} v$); otherwise, v is said to be of infinite order. Clearly $\operatorname{ord} v$ is defined up to an associate. We observe that $\operatorname{ord} v$ coincides with its classical definition [3, p. 165]. Let $a_1v_1 + \ldots + a_nv_n$ be a linear combination of the elements v_i of V with a_i elements of R. We say that $a_1v_1 + \ldots + a_nv_n$ is nontrivial in v_n if and only if

$$(12) \qquad a_1v_1 + \ldots + a_nv_n = 0 \quad \text{and } a_nv_n \neq 0.$$

Lemma 3. *Let, as in* (12), $a_1v_1 + \ldots + a_nv_n$ *be nontrivial in* v_n *and* v_n *be not of infinite order. Then there exists a linear combination* $b_1v_1 + \ldots + b_nv_n$ *such that*

$$(13) \qquad b_1v_1 + \ldots + b_nv_n \quad \textit{is nontrivial in } v_n \quad \textit{and } b_n < \operatorname{ord} v_n$$

Proof. Indeed, let

$$(14) \qquad b_n = (a_n, \operatorname{ord} v_n) = xa_n + y(\operatorname{ord} v_n).$$

Clearly, $b_n \not\approx \operatorname{ord} v_n$ since otherwise , in view of (14), $\operatorname{ord} v_n$ would divide b_n and also would divide a_n contradicting (12). On the other hand, since b_n divides $\operatorname{ord} v_n$ from (10) it follows that $b_n < v_n$. But then, from (12) and (14) we obtain

$$\begin{aligned} 0 &= x(a_1v_1 + \ldots + a_nv_n) + y(\operatorname{ord} v_n)v_n \\ &= xa_1v_1 + \ldots + \big(xa_n + \ldots + y(\operatorname{ord} v_n)\big)v_n = b_1v_1 + \ldots + b_nv_n \end{aligned}$$

where $b_i = xa_i$ for $i < n$. Clearly, in the above $b_nv_n \neq 0$ since $b_n < \operatorname{ord} v_n$. Thus, (13) is established, and the Lemma is proved. □

Let R be a principal ideal domain and V be an R-module generated by n pairwise distinct nonzero generators $g_1, \ldots, g_n$. We recall that these n generators form a basis of V if and only if 0 (the zero of V) cannot be equal to a linear combination of $g_1, \ldots, g_n$ over R with some nonzero summands.

Theorem. *Let R be a principal ideal domain and V be a finitely generated R-module. Then V has a basis.*

Proof. We prove the Theorem in its following version. Let V be such that it can be generated by n generators $g_1, \ldots, g_n$ and not by less than n generators, where (to avoid the trivial case) we let $n > 1$. We use induction. Thus, we assume that any R-module which can be generated by $n - 1$ generators and not by less than

$n-1$ generators has a basis. Now, by (11), among all possible sets of n generators of V we choose a set $\{g_1, \ldots, g_{n-1}, b\}$ such that no set of n generators of V has an element of order (which could be infinite) less than the order of b. Clearly, the submodule S of V which is generated by the set $\{g_1, \ldots, g_{n-1}\}$ of $n-1$ generators cannot be generated by less than $n-1$ generators since V cannot be generated by less than n generators. Hence, by our assumption, S has a basis, say, $\{b_1, \ldots, b_{n-1}\}$. We prove the Theorem by showing that $\{b_1, \ldots, b_{n-1}, b\}$ is a basis of V. Obviously, $\{b_1, \ldots, b_{n-1}, b\}$ generates V. Let us assume to the contrary, and therefore

$$(15) \qquad a_1 b_1 + \ldots + a_{n-1} b_{n-1} + a_n b = 0 \quad \text{and } a_n b \neq 0.$$

But then $a_1, \ldots, a_{n-1}, a_n$ cannot be relatively prime since otherwise from Lemma 2 it would follow that $a_1 b_1 + \ldots + a_{n-1} b_{n-1} + a_n b$ could be a member of a set of n generators of V which by (15) would imply that 0 would be a member of a set of n generators of V and therefore V could be generated by less than n generators which is impossible. Hence, $a_1, \ldots, a_{n-1}, a_n$ are not relatively prime and $(a_1, \ldots, a_{n-1}, a_n) = d \neq 1$. But then from (15) we have

$$(16) \qquad d((a_1/d)b_1 + \ldots + (a_{n-1}/d)b_{n-1} + (a_n/d)b) = 0$$

where $(a_1/d), \ldots, (a_{n-1}/d), (a_n/d)$ are now relatively prime. But then, again, from Lemma 2 it would follow that $b^* = (a_1/d)b_1 + \ldots + (a_{n-1}/d)b_{n-1} + (a_n/d)b$ could be a member of a set of n generators of V which by (16) would lead to a contradiction if b were of infinite order. Thus, in (15), we let b be not of infinite order, and, in view of (13), without loss of generality we may assume that in (15) it is the case that $a_n < \operatorname{ord} b$. But then, from (16) we see that $\operatorname{ord} b^*$ divides d which in turn divides a_n and therefore by (10) we have $\operatorname{ord} b^* < \operatorname{ord} b$, contradicting the choice of b. Thus, the Theorem is proved. $\square$

Remark 2. From the proof of the Theorem it follows that if V is a finitely generated module over a principal ideal domain such that no set of generators of V has an element of not of infinite order then any set with least number of generators of V is a base of V. Also, since every finitely generated Abelian group is a finitely generated module over the integral domain of integers, the above Theorem and its proof implies the following Fundamental Theorem of Abelian Groups with a proof which does not consider two cases of Torsion and Torsion free subgroups of the group.

Corollary 2. *Every Finitely Generated Abelian group has a basis and therefore is a direct sum of its cyclic subgroups.*

Remark 3. The central lines of ideas and proofs given above are generalized version of the ideas in [4] to the case of Modules over principal ideal domains. The generalization is nontrivial as witnessed by Lemma 3 and the succeeding proofs. Also, it can be shown that based on Lemmas 1, 2, 3 an iterative process can be devised which starting with a set of generators of V will yield a basis of V in finitely many steps.

References

[1] *Abian, A.*: Construction of a basis for finitely generated Abelian groups., Abstracts, Amer. Math. Soc. *12* (1991), 507.

[2] *Hungerford, T. W.*: Algebra, Springer-Verlag, New York, 1974.

[3] *Jacobson, N.*: Lectures in Abstract Algebra, Springer-Verlag, New York, 1951.

[4] *Shenkman, E.*: The basis theorem for finitely generated Abelian groups, American Mathematical Monthly *67* (1960), 770.

Authors' addresses: Department of Mathematics, Iowa State University, Ames, Iowa 50011, USA; Department of Mathematics, Southwest Missouri State University, Springfield, Missouri 65804, USA.