SOME BASIC MACHINE ALGORITHMS FOR INTEGRAL ORDER COMPUTATIONS

BY

HAROLD BROWN

STAN-CS-72-258
FEBRUARY 1972

COMPUTER SCIENCE DEPARTMENT
School of Humanities and Sciences
STANFORD UNIVERSITY

Some Basic Machine Algorithms for Integral Order Computations

by Harold Brown

Abstract: Three machine implemented algorithms for computing with integral orders are described. The algorithms are:

1. For an integral order R given in terms of its left regular representation relative to any basis, compute the nil radical J(R) and a left regular representation of R/J(R).
2. For a semisimple order R given in terms of its left regular representation relative to any basis, compute a new basis for R and the associated left regular representation of R such that the first basis element of the transformed basis is an integral multiple of the identity element in $Q \otimes R$.
3. Relative to any fixed Z-basis for R, compute a unique canonical form for any given finitely generated Z-submodule of $Q \otimes R$ described in terms of that basis.

This research was supported mainly by the National Science Foundation -under grant number GP-16793 and in part by ONR 00014-67-A-0112-0057-NR 044-402. Reproduction in whole or in part is permitted for any purpose of the United States Government.

Some Basic Machine Algorithms for Integral Order Computations

Introduction and Definitions. In the investigation of certain algebraic questions such as arithmetics in rational algebras and integral group representations, the concept of a Z-order frequently occurs. A Z-order is a discrete algebraic structure R, +,. satisfying:

1.1 R, +, . is an associative ring (not necessarily commutative or with identity),

1.2 R, + is a free Z-module of finite rank, i.e., R, + is a "vector space" over the rational integers with a finite Z-basis.*

For example, the set of all upper triangular n x n matrices with integral entries, T_n, forms a Z-order of rank $n(n+1)/2$.

Let $B = \{b_1,\ldots,b_n\}$ be any Z-basis for the Z-order R. The left regular representation of R with respect to B is the (ring and Z-module) homomorphism $LR_B: R \to M_{nxn}(Z)$ from R into the Z-order of n x n integral matrices induced by $LR_B(b_j) = (t_{ik}^{(j)})$ where $b_j \cdot b_k = \Sigma_i t_{ik}^{(j)} b_i$. The coordinate map $V_B: R \to M_{nx1}(Z)$ given by $V_B(x) = (x_1,\ldots,x_n)^T$ where $x = \Sigma_i x_i b_i$ is also a Z-module homomorphism. LR_B and V_B are related as follows: For any $x = \Sigma_i x_i b_i$ and y in R, $V_B(x \cdot y) = LR_B(x)V_B(y) = \Sigma_i x_i LR_B(b_i)V_B(y)$. Thus, the structure of R is

*Basic definitions and theorems for Z-modules can be found, e.g., in MacLane and Birkhoff, Algebra, for rings in Divinsky, Rings and Radicals and for orders in Deuring, Algebren.

completely determined by the integral matrices $LR_B(b_i)$, $i = 1,\ldots,n$. This concrete representation of R as a set of n, n x n integral matrices is very convenient for computational purposes, particularly on a machine, and it will be assumed here that all orders are described by such representations. Note that $B' = \{b'_1,\ldots,b'_n\}$ is another Z-basis for R if and only if $b'_i = \Sigma_j u_{ij} b_j$ where $U = (u_{ij})$ is unimodular, i.e., U is an integral matrix with $DET(U) = \pm 1$. Moreover,=

1.3 $V_{B'}(x) = U^{-T} V_B(x)$.

1.4 $LR_{B'}(x) = U^{-T} LR_B(x) U^T$.

1.5 $LR_{B'}(b'_j) = \Sigma_t u_{jt} U^{-T} LR_B(b_t) U^T$.

Since a Z-order R is of finite rank, R, considered as a ring, satisfies the ACC (ascending chain condition) on left ideals. Also, R contains a unique maximal nil left ideal, J(R), consisting of the sum of all nil left ideals in R. Thus, by Levitzki's theorem, J(R) is also theuniquemaximal nilpotent ideal of R. J(R) is called the nil radical of R. For example, $J(T_n)$ is the subset of all strictly upper triangular matrices in T_n and $J(M_{nxn}(Z))$ consists of only the zero matrix.

Lemma. R/J(R) is an order.

Proof. It needs only be shown that R/J(R) is free as a Z-module. By the basis theorem for finitely generated Z-modules, this is tantamount to showing that R/J(R) is torsion free. Assume that $m(r + J(R)) = J(R)$ for some r + J(R) in R/J(R) and $0 \neq m$ in Z. Then $mr \in J(R)$. Since J(R) is nil, $(mr)^k = m^k r^k = 0$ for some $k \in N$. Since R is free, it is torsion free. Thus $r^k = 0$, i.e., $r \in J(R)$ and $r + J(R) = J(R)$.

In most applications of the theory of orders, the order R is considered as being embedded in the rational algebra $Q \otimes R$, the tensor product of Q and R over Z. $Q \otimes R$ can be considered as the algebra of all n x 1 rational column vectors with multiplication defined by $(x_i)(y_j) = \Sigma_i x_i LR_B(b_i)(y_j)$. It follows directly from the definitions that:

1.6 $Q \otimes R$ is an n-dimensional algebra over Q with

$$J(Q \otimes R) = Q \otimes J(R).$$

1.7 $Q \otimes R/Q \otimes J(R) \underset{Q}{\cong} Q \otimes (R/J(R))$.

For example, $Q \otimes (\Gamma_n/J(\Gamma_n)) \underset{Q}{\cong} M_{nx1}(Q)$ where the operations are componentwise.

Since $Q \otimes (R/J(R))$ is a finite dimensional algebra over Q, it satisfies the DCC (descending chain condition) on left ideals. Moreover, $J(Q \otimes (R/J(R))) = 0$. Thus $Q \otimes (R/J(R))$ is a semisimple algebra. In particular, $Q \otimes (R/J(R))$ nas an identity element e.

The usual initial step in computational problems involving orders is to determine $J(R)$ and $R/J(R)$. Also, these problems usually require working with numerous Z-submodules of $Q \otimes (R/J(R))$. We present here effective algorithmic procedures to:

I. Determine a Z-basis for J(R) in terms of the given representation of R.

II. Determine the structure of the order R/J(R) in a normalized form, i.e., determine a set of defining matrices, $M_1, \ldots, M_k$, for R/J(R) such that M_1 is an integral multiple of the identity matrix.

III. Determine when two finitely generated Z-submodules of $Q \otimes R$

described in terms of a basis B of R are equal.

In a second paper we will describe an effective procedure for embedding R/J(R) into a maximal %-order of $Q \otimes (R/J(R))$. These algorithms have been implemented on an IBM 360/67.

Algorithms. The basic computational procedure used in the algorithms is unimodular row reduction of an integral matrix. This procedure is central for many algorithms in discrete algebra, e.g., the basis theorem for finitely generated abelian groups.

A matrix $A = (a_{ij})$ is said to be in row reduced form (or row echelon form) if it satisfies the following condition:

> If a_{ks} is the first nonzero entry in the k-th row of A, then for all i>k and j<s, $a_{ij} = 0$.

Lemma. For any s x t integral matrix $M = (m_{ij})$, there is an s x s unimodular matrix U such that UM is in row reduced form.

The proof of this lemma is given by the following algorithm. The termination of the algorithm is a consequence of the well-ordering of the positive integers.

Row Reduction Algorithm.

1 Initialize: $j \leftarrow 1$, $h \leftarrow 1$, $U = (u_{pq}) \leftarrow$ sxs identity matrix.

2 Search the j-th column of M for an element of minimal nonzero magnitude, say m_{kj}. If no such element exists, go to step 6.
If m_{kj} is the only nonzero element in the j-th column, go to step 4.

3 Do for i = h,h+1,...,k-1,k+1,...,s:
Divide m_{ij} by m_{kj} getting an integral quotient q_i and remainder

r_i with $|r_i| < |m_{kj}|$, i.e., $mij = m_{kj}q_i + r_i$. For $v = j,\ldots,t$, $m_{iv} \leftarrow m_{iv} - m_{kv}q_i$ and for $v = 1,\ldots s$, $u_{iv} \leftarrow u_{iv} - u_{kv}q_i$. If $r_i \neq 0$, $k \leftarrow i$ and go to step 3.

4 Interchange the h-th and k-th rows of M and the h-th and k-th rows of U.

5 $h \leftarrow h + 1$.

6 $j \leftarrow j + 1$.

7 If $j = s$ or $h > t$, exit, otherwise go to step 2.

In a machine implementation of the algorithm, devices such as immediately exiting the search in step 2 and setting q_i to $\pm m_{ij}$ if an element m_{kj} of magnitude 1 is found can speed up the process considerably for certain classes of matrices.

The algorithm for I and II is based on the trace bilinear form $T: R \times R \to Z$ defined by $T(x,y) = TRACE(LR_B(x \cdot y))$. T is a symmetric form, and by 1.4 it is independent of basis choice. T is completely determined relative to a basis B of R by the symmetric integral matrix $M_B = (T(b_i,b_j))$, and $T(x,y) = V_B(x)^T M_B V_B(y)$. If U is a unimodular change of basis matrix carrying B onto the basis B', then $M_{B'} = UM_BU^T$. Since $DET(U) = \pm 1$, $DET(M_B)$ depends only on R. This determinant is called the Z-discriminant of R, and it is nonzero if and only if $J(R) = 0$.

The relationship between J(R) and T is given in the following lemma:

Lemma. Let RAD(T) be the submodule of elements in R orthogonal to R, i.e., $RAD(T) = \{ x \in R \mid T(x,y) = 0 \ \forall \ y \in R \}$. Then $RAD(T) = J(R)$.

Proof. For any $x \in J(R)$ and $y \in R$, $x \cdot y$ is in J(R) since J(R) is

an ideal in R. J(R) is nil. Thus $(x \cdot y)^k = 0$ for some $k \in N$, and, since LR_B is a homomorphism, $LR_B(x \cdot y)^k = 0$. But any nilpotent matrix must have zero trace. Hence $J(R) \subseteq RAD(T)$. Conversely, if $x \in RAD(T)$, then $T(x, x^k) = 0$ for any $k > 0$, i.e., $TRACE(LR_B(x)^k) = 0$ for any $k > 1$. This implies that the characteristic polynomial of $LR_B(x)$ is of the form z^t, i.e., that $LR_B(x)$ is a nilpotent matrix. Hence by the definition of LR.., x is nilpotent. Similarly, $r \cdot x$ is nilpotent for any r in R. Thus x generates a nil left ideal in R, and $x \in J(R)$.

Let $U = (u_{ij})$ be a unimodular matrix such that UM_B is in row reduced form. Then UM_B is of the block form $\begin{bmatrix} A \\ O \end{bmatrix}$ where the rows of A are X-independent (or, equivalently, Q-independent). Since M_B is symmetric, UM_BU^T is of the form $\begin{bmatrix} W & 9 \\ O & Q \end{bmatrix}$ where W is a nonsingular d x d integral matrix. Let $b_i' = \Sigma_j u_{ij} b_j$. Then $B' = \{b_i'\}$ is a Z-basis for R, and the last n-d elements of B' form a Z-basis for RAD(T) and hence for J(R). Moreover, the set $\{b_1' + J(R) \mid i = 1, \ldots, d\}$ forms a Z-basis for R/J(R). Thus, the set $\{LR_{B'}(b_i') \mid i = d+1, \ldots, n\}$ corresponds to a %-basis f'or J(R) and the upper left d x d blocks of the matrices $LR_{B'}(b_i')$, i = 1,...d, form a set of defining matrices for the order R/J(R).

The order R/J(R) has zero nil radical, and, for notational simplicity, we assume henceforth that J(R) = 0, i.e., that $Q \otimes R$ is semisimple, Since $Q \otimes R$ is semisimple, $Q \otimes R$ contains an identity element e and $LR_B(e) = I_n$. Here, we extend LR_B to $Q \otimes R$ in the obvious manner and I_n denotes the n x n identity matrix. B is a Q-basis for $Q \otimes R$. Hence e can be expressed as

$e = \Sigma_i (q_i/h_i)b_i$ with q_i and h_i in Z and $GCD(q_i, h_i) = 1$. Let $t = LCM[h_i]$. Then $Ze \cap R = Zte$. Note that the coefficients q_i/h_i and hence t can be constructively determined, e.g., by using the row reduction algorithm to solve over Q the $n^2 \times n$ system of linear equations $I_n = \Sigma_i (x_i/y_i) LR_B(b_i)$, x_i and y_i in Z.

From the equations $\Sigma_j (q_j/h_j) t_{ii}^{(j)} = 1$, $i = 1,\ldots,n$, it follows by an elementary number theoretic argument that $GCD(q_i t/h_i) = 1$, i.e., that the entries in $V_B(te)$ are relatively prime. (Here, as before, $(t_{st}^{(j)}) = LR_B(b_j)$). Since multiplication of $V_B(te)$ by a unimodular matrix does not change the GCD of the entries, we can use the row reduction algorithm to construct a unimodular matrix S satisfying $V_B(te)^T S = (1,0,\ldots,0)$. The matrix S^{-1} is unimodular and has as first row $V_B(te)^T$. Hence, the basis $(bj) = S^{-1}(b_i)$ has as first element te, and the matrices $LR_{B'}(b_i')$, $i = 1,\ldots, n$, form a representation for the order R of the desired type.

These procedures effectively solve I an3 IT. The row reduction algorithm also yields an effective procedure for III.

Let H be a finitely generated Z-submodule of $Q \otimes R$. H can be described relative to a basis $B = (b_i)$ of R by a nonzero integer D_H and an integral matrix F_H as follows: Say $H = \Sigma_{i=1}^{k} Zh_i$. Then $h_i = \Sigma_{j=1}^{n} q_{ij} b_j$, $q_{ij} \in Q$, $i = 1,\ldots,k$. Let D_H be the LCM of the denominators of the q_{ij} and $F_H = D_H(q_{ij})$. H is completely determined relative to B by the pair (D_H, F_H). Moreover, this representation of H by a pair (D_H, F_H) admits a normal form.

A representation (D_H, F_H) of H relative to B is said to be in (Hermite) normal form if:

2.1 $D_H > 0$.

2.2 $F_H = (f_{ij})$ has no zero rows.

2.3 If f_{st} is the first nonzero entry in the s-th row of F_H, then (i) $f_{st} > 0$, (ii) $f_{ij} = 0$ for $i > s$ and $j \leq t$, (iii) $0 \leq f_{it} < f_{st}$ for $i < s$.

2.4 The GCD of D_H and the f_{ij} is 1.

If (D_H, F_H) is any representation of H relative to B, then the following algorithm gives an effective procedure for determining a normal form representation, (D'_H, F'_H), for H relative to B:

Normal Form Algorithm.

1 $D'_H \leftarrow |D_H|$.

2 Apply the row reduction algorithm to F_H, obtaining a unimodular matrix W such that $WF_H = (t_{ij})$ is in row reduced form. Note that since W is unimodular, the elements $\Sigma_j (t_{ij}/D'_H) b_j$, $i = 1, \ldots, k$, form a Z-generating set for H.

3 Delete any zero rows in WF_H, obtaining an m x n matrix $F'_H = (f'_{ij})$.

4 Do for i = l,...;n:

Determine the first nonzero entry in the i-th row of F'_H, say f'_{it}. If $f'_{it} < 0$, $f'_{ij} \leftarrow -f'_{ij}$, j = t,...,n.

Do for s = 1,...,i-1:

If $f'_{st} < 0$ or $f'_{st} > f'_{it}$, subtract $\lfloor f'_{st}/f'_{it} \rfloor$ - times the i-th row of F'_H from the s-th row.

Note that these row operations correspond to unimodular transformations of F'_H, and hence F'_H still determines a Z-generating set (in fact a Z-basis) for H.

5 Compute the GCD, say D, of D'_H and the f'_{ij}.

6 $D'_H \leftarrow D'_H/D$; $F'_H \leftarrow (1/D)F'_H$.

In particular, it follows from this algorithm that relative to any basis B of R a finitely generated Z-module, H, possesses a normal form representation.

Let $B' = (b'_{ij})$ be another basis for R, say $(b'_{j\,i}) = U(b_{j\,i})$. If (D_H, F_H) is any representation of H relative to B, then $(D_H, F_H U^{-1})$ is a representation of H relative to B'. If (D_H, F_H) is a normal form representation, then $(D_H, F_H U^{-1})$ satisfies 2.1, 2.2 and 2.4, but need not satisfy 2.3.

The utility of the normal form representation is a consequence of the following lemma:

Lemma. Any two normal form representations of H relative to B, say (D_H, F_H) and (D'_H, F'_H), must be idetical.

Proof. By 2.4 and 2.1, D_H (D'_H) is the least positive integer such that $D_H H \subseteq R$ ($D'_H H \subseteq R$). Hence D_H and D'_H depend only on H, and $D_H = D'_H$. F_H and F'_H are both row reduced matrices by 2.3(ii). Since neither matrix has any zero rows, the row dimension of F_H (F'_H) is equal to the Z-rank of H, i.e., F_H and F'_H are of the same dimensions, and the sets of elements of H determined by $F_H(b_i)$ and by $F'_H(b_i)$ form L-bases for H. Thus there is a unimodular matrix T such that $F'_H = TFH$.

From an analysis of the entry patterns in T, F_H and F'_H it follows that I' is an upper triangular matrix and F_H and F'_H have the same echelon pattern. Since T is unimodular, its diagonal entries must be ±1, and 2.3(i) implies that they must be positive. Using these observations and 2.3(iii), an induction argument on the row dimension gives that T must be the identity matrix, i.e., that $F_H = F'_H$.

The normal form algorithm effectively solves III. Note that for computations involving Z-submodules of $Q \otimes R$, it is usually most efficient to carry all submodules in normal form representation relative to some fixed basis of R as this eliminates any problems of redundancy.

Implementation. The programs implementing these algorithms are structured as a sequence of subroutines. The row reduction algorithm program is coded in System/360/OS assembler language. The rest of the routines are coded in FORTRAN IV.

The subroutines are:

1. ROWFRM, the row reduction algorithm routine.
2. INV, a routine to find the inverse of a unimodular matrix.
3. DE!', a routine to compute the determinant of a square integral matrix.
4. GCD, a simple Euclid% algorithm program.
5. RADRDC, the routine to determine J(R) and R/J(R).
6. IDBAS, a routine to transform the basis of a semisimple order R into one in which the first basis element is a multiple of the identity in $Q \otimes R$.
7. NORFRM, a routine implementing the normal form algorithm.

ROWFRM, INV, DET and NORFRM are each $O(n^3)$ units of time processes where n is the row dimension of the matrix. RADRDC and IDBAS are both $O(n^4)$ units of time processes where n is the Z-rank of R.

Examples.

1. Let T_2 denote the Z-order of all upper triangular 2 x 2 matrices with integral entries. Let R be the suborder of T_2 with Z-basis $B = \{b_1, b_2, b_3\}$ where

$$b_1 = \begin{bmatrix} 2 & 3 \\ 0 & 2 \end{bmatrix}, \quad b_2 = \begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix}, \quad b_3 = \begin{bmatrix} 3 & 6 \\ 0 & 2 \end{bmatrix}.$$

Then,

$$LR_B(b_1) = \begin{bmatrix} -6 & -16 & -8 \\ 2 & 6 & 2 \\ 4 & 8 & 6 \end{bmatrix}, \quad LR_B(b_2) = \begin{bmatrix} -8 & -20 & -10 \\ 4 & 10 & 4 \\ 4 & 8 & 6 \end{bmatrix},$$

$$LR_B(b_3) = \begin{bmatrix} -12 & -30 & -15 \\ 3 & 9 & 3 \\ 8 & 16 & 11 \end{bmatrix},$$

and

$$M_B = \begin{bmatrix} 12 & 16 & 16 \\ 16 & 24 & 20 \\ 16 & 20 & 22 \end{bmatrix}.$$

The row reduction algorithm applied to M_B yields the unimodular matrix

$$U = \begin{bmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 4 & -1 & -2 \end{bmatrix}$$

satisfying

$$UM_BU^T = \begin{bmatrix} 4 & -4 & 0 \\ -4 & 6 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Thus J(R) has rank 1 and R/J(R) has rank 2 and discriminant 8.

Let B' be the basis obtained by $(b_i') = U(b_i')$. Then,

$$b_1' = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}, \quad b_2' = \begin{bmatrix} 1 & 3 \\ 0 & -2 \end{bmatrix}, \quad b_3' = \begin{bmatrix} 0 & -3 \\ 0 & 0 \end{bmatrix},$$

and, using 1.5,

$$LR_{B'}(b_1') = \begin{bmatrix} 2 & -2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad LR_{B'}(b_2') = \begin{bmatrix} -2 & 3 & 0 \\ 0 & 1 & 0 \\ -2 & 2 & 1 \end{bmatrix},$$

$$LR_{B'}(b_3') = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 2 & -2 & 0 \end{bmatrix}.$$

Hence, b_3' is a basis for J(R) with corresponding matrix $LR_{B'}(b_3')$, and R/J(R) is the order with defining matrices

$$m_1 = \begin{bmatrix} 2 & -2 \\ 0 & 0 \end{bmatrix}, \quad m_2 = \begin{bmatrix} -2 & 3 \\ 0 & 1 \end{bmatrix}.$$

Let S be the order of rank 2 with defining matrices m_1 and m_2 and basis C. J(S) = 0, and $Q \otimes S$ is semisimple. The unique solution of $x_1 m_1 + x_2 m_2 = I_2$ is $x_1 = 3/2$, $x_2 = 1$. Thus $t = 2$, and $V_C(te)^T = (3,2)$. The unimodular matrix

$$W = \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix}$$

satisfies $V_C(te)^T W = (1,0)$, and

$$W^{-1} = \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}.$$

Using 1.5, we obtain the desired normalized representation matrices for $R/J(R) \cong S$, namely

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 0 \\ 2 & 1 \end{bmatrix}.$$

With this representation, it is easy to see that $Q \otimes R/J(R) \cong QXQ$ where the operations on QXQ are componentwise and $R/J(R) \cong 2ZX.Z$.

2. Let R be the Z-order of all upper triangular 3 x 3 matrices

with integral entries, and let $B = \{e_{sk} \mid 1 \leq s \leq k \leq 3\}$ be the natural Z-basis for R, i.e., $e_{sk} = (\delta_{is}\delta_{kj})$. Let H be the Z-submodule of $Q \otimes R$ with L-generating set

$$h_1 = \begin{bmatrix} 1/5 & 2/3 & 1/5 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad h_2 = \begin{bmatrix} 1/6 & 11/30 & 1/6 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad h_3 = \begin{bmatrix} 1/15 & 8/15 & 1/5 \\ 0 & 0 & 1/6 \\ 0 & 0 & 0 \end{bmatrix},$$

$$h_4 = \begin{bmatrix} 1/15 & 3/10 & 1/6 \\ 0 & 0 & 2/15 \\ 0 & 0 & 0 \end{bmatrix}, \quad h_5 = \begin{bmatrix} 1/15 & 1/3 & 1/6 \\ 0 & 0 & 2/15 \\ 0 & 0 & 0 \end{bmatrix}.$$

H is represented relative to B by the pair (D_H, F_H) with $D_H = 30$ and

$$F_H = \begin{bmatrix} 6 & 20 & 6 & 0 & 0 & 0 \\ 5 & 11 & 5 & 0 & 0 & 0 \\ 2 & 16 & 6 & 0 & 5 & 0 \\ 2 & 9 & 5 & 0 & 4 & 0 \\ 2 & 10 & 5 & 0 & 4 & 0 \end{bmatrix}.$$

Via the row reduction algorithm: F_H is unimodularly transformed into

$$F'_H = \begin{bmatrix} 1 & -21 & -19 & 0 & -20 & 0 \\ 0 & -1 & -205 & 0 & -244 & 0 \\ 0 & 0 & 1 & 0 & 56856 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

The normal form algorithm applied to F'_H yields

$$F''_H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Hence, H has the unique normal form representation relative to B (D_H, F''_H), and H has as a Z-basis $\{(1/30)e_{11}, (1/30)e_{12}, (1/30)e_{13}, (1/30)e_{23}\}$.

*Note that in this example a relatively large entry is produced by the row reduction algorithm. These large entries occur often, particularly in intermediate calculations, and overflow must be watched for.

References

1, G. H. Bradley "Algorithms for Hermite and Smith normal matrices and linear Diophantine equations," Math. Comp. 25 (1971), 897-907.

2. C. Hermite, "Sur l'introduction des variables continues dan la théorie des nombres," J. Reine Angew Math. 41 (1851), 191-216.

3. H. J. Zassenhaus, "Ein Algorithmus zur Berechnung einer Minimalbasis über gegebener Ordnung," ISNM 7 (1967), 90-103.