C. R. Math. Rep. Acad. Sci. Canada Vol. **36** (4) 2014, pp. 106–113

Lattice Geometry and Reduction of Finitely Generated Abelian Groups to a Normal Form

Leonid Monin

Presented by Pierre Milman, FRSC

Abstract. In this paper the geometry of the lattice is used to prove basic theorems about subgroups and factor groups of $\mathbb{Z}^n$. We suggest a geometric algorithm which reduces a finitely generated abelian group to its normal form.

Résumé. Dans ce papier, un argument de géométrie sur les réseaux est utilisé pour prouver des théorèmes fondamentaux sur les sous-groupes ou les groupes quotients de $\mathbb{Z}^n$. Nous proposons un algorithme géométrique qui réduit un groupe abélien finement engendré à sa forme normale.

Introduction The classification of subgroups of the standard lattice $\mathbb{Z}^n \subset \mathbb{R}^n$ up to an automorphism of $\mathbb{Z}^n$ is well-known. The standard proof uses row/column reduction of an integer matrix of generators to the Smith normal form which was first introduced in [4]. In this paper we give a different, more geometric proof of this result based on the geometry of the lattice.

In Section 3 we prove the normal form theorem for subgroups of $\mathbb{Z}^n$. This proof uses some simple results about bihomomorphisms from a product of abelian groups to $\mathbb{Z}$ (see Section 1), and facts about automorphisms of $\mathbb{Z}^n$ (see Section 2).

Section 4 is dedicated to the notion of integral volume. It helps to find the normal form of a subgroup of $\mathbb{Z}^n$ (Section 5) and the normal form of a finitely generated abelian group given by a finite set of generators and by relations between them (Section 6).

Acknowledgements. I would like to thank A. Khovanskii for the formulation of the problem and his basic guidance on this work. I would like to thank the referee for the careful reading of this paper and the very useful Referee's Report.

1. **Bihomomorphisms of abelian groups to $\mathbb{Z}$** Let G_1, G_2 be two abelian groups, and $F : G_1 \times G_2 \to \mathbb{Z}$ be a map such that the restriction of F to one coordinate, with the other fixed, is a homomorphism. We will call such a function *a bihomomorphism.* Let d be the minimal positive integer which can be written as $F(x, y)$ for some $x \in G_1$, $y \in G_2$. We will call d *the characteristic number* for the triple G_1, G_2 and F.

Received by the editors on April 2, 2014; revised August 13, 2014.
AMS Subject Classification: 52B20.
Keywords: Integer lattice, Integer volume, Normal Smith form.

THEOREM 1.1. *Any value $F(x, y) \in \mathbb{Z}$ is divisable by d.*

PROOF. We prove the theorem in a few steps.

1. We say that the element $x_0 \in G_1$ is *extreme* if there exists some $y(x_0) \in G_2$ such that $F(x_0, y(x_0)) = d$. If $x_0 \in G_1$ is extreme, then the number $F(x_0, y)$ is divisible by d for any $y \in G_2$. Indeed, the set of elements $F(x_0, y)$ forms the subgroup of $\mathbb{Z}$ which contains d, but doesn't contain any number z such that $0 < z < d$.

2. Extremality of elements $y \in G_2$ is defined similarly. As before, if $y_0 \in G_2$ is extreme, then the number $F(x, y_0)$ is divisible by d for any $x \in G_1$.

3. If F is not everywhere zero, then extreme elements from G_1 generate it. Indeed, let $F(x_0, y_0) = d$. Then, due to **1**, $F(x, y_0) = kd$, $k \in \mathbb{Z}$, for any $x \in G_1$. Then $F(x - (k-1)x_0, y_0) = kd - (k-1)d = d$, which means that the element $z = x - (k-1)x_0$ is extreme. But $x = z + (k-1)x_0$, which is the sum of two extreme elements.

The theorem follows immediately from **1** and **3**. □

COROLLARY 1.2. *Let $J_1 \supset J_2 \supset \cdots \supset J_k$ be a chain of subgroups of G_1. Let d_i be the characteristic number for the triple J_i, G_2 and F. Then, $d_{i+1} \vdots d_i$ for any $i = 1, 2, \ldots, k-1$.*

PROOF. The proof is an iterative application of Theorem 1.1 to the groups $J_1, \ldots, J_{k-1}$. □

We will say that the pair of elements $(x_0, y_0) \in G_1 \times G_2$ is *F-conjugated* for G_1 and G_2, if $F(x_0, y_0) = d$.

PROPOSITION 1.3. *For any pair of F-conjugated elements (x_0, y_0) the group G_1 is a direct sum of subgroups (x_0) and $G_1(y_0)$, where (x_0) is generated by x_0, and $G_1(y_0)$ consists of elements $x \in G_1$ such that $F(x, y_0) = 0$.*

PROOF. The intersection of the subgroups (x_0) and $G_1(y_0)$ is $\{0\}$. Indeed, any non-zero element z of (x_0) can be written as $z = mx_0$, where $m \neq 0$. Thus $F(z, y_0) = md \neq 0$ and $z \notin G_1(y_0)$.

If $x \in G_1$ and $F(x, y_0) = kd$ (see point **2** from the proof of Theorem 1.1), then $x = kx_0 + (x - kx_0)$ and $kx_0 \in (x_0)$, $x - kx_0 \in G_1(y_0)$. □

DEFINITION 1.4. *We will call a chain of subgroups $G_1 = J_0 \supset \cdots \supset J_k$ equipped with sequences of elements $x_0 \in J_0, \ldots, x_{k-1} \in J_{k-1}$ and $y_0, \ldots, y_{k-1} \in G_2$ F-compatible, if the following is true for any $i = 0, \ldots, k-1$:*

(1) *the pair $(x_i, y_i) \in J_i \times G_2$ is F-conjugated for groups $J_i \subset G_1$ and G_2;*
(2) *$J_{i+1} = J_i(y_i)$ (i.e. J_{i+1} is a subgroup of J_i, consisting of the all elements $x \in J_i$ such that $F(x, y_i) = 0$).*

The following theorem can be proved by repeated application of Proposition 1.1.

THEOREM 1.5 (Decomposition Theorem). *For any F-compatible chain, the group G_1 is a direct sum of subgroups $(x_0), \ldots, (x_{k-1}) \subset G_1$ and the group J_k.*

2. **Rational subspaces of $\mathbb{R}^n$ and automorphisms of $\mathbb{Z}^n$** From now on we will deal only with triples G_1, G_2 and F of the following type:

(1) G_1 is a subgroup of the standard integral lattice $\mathbb{Z}^n$ of $\mathbb{R}^n$;
(2) G_2 is the standard integral lattice $(\mathbb{Z}^n)^*$ of the dual space $(\mathbb{R}^n)^*$;
(3) $F(x, y) = \langle x, y\rangle$, where $x \in G_1$, $y \in G_2$.

Thus the group G_2 and the function F will be fixed, and G_1 will be a subgroup of $\mathbb{Z}^n$.

A vector $v \in \mathbb{Z}^n$ is called *primitive* if the greatest common divisor of the coordinates of v is 1.

LEMMA 2.1. *A vector $v \in \mathbb{Z}^n$ is primitive if, and only if, there exists a covector $f_v \in (\mathbb{Z}^n)^*$ such that $\langle f_v, v\rangle = 1$.*

PROOF. The greatest common devisor of coordinates $a_1, a_2, \ldots, a_n$ of v is 1, iff there are integers $k_1, k_2, \ldots, k_n$, such that $k_1a_1 + k_2a_2 + \cdots + k_na_n = 1$. We can take $f_v = k_1x_1 + k_2x_2 + \cdots + k_nx_n$. □

The following corollary is an immediate consequence of Lemma 2.1.

COROLLARY 2.2. *Let G_1 be a subgroup of $\mathbb{Z}^n$. Let $v \in G_1$ be an extreme element and d be the characteristic number for the triple $G_1, (Z^n)^*$ and F. Then the vector v/d is primitive.*

LEMMA 2.3. *For any complete flag of rational spaces $L_1 \subset \ldots \subset L_n = \mathbb{R}^n$, where $\dim L_i = i$, there is a basis $v_1, \ldots, v_n$ of the lattice $\mathbb{Z}^n \subset \mathbb{R}^n$ such that $v_1, \ldots, v_i$ is a basis of the group $L_i(\mathbb{Z}) = L_i \cap \mathbb{Z}^n$ for any $i = 1, \ldots, k$.*

PROOF. For $n = 1$ there is nothing to prove. Assume that the lemma is proved for any $n < k$.

Let v_1 be a primitive vector in L_1 (clearly, v_1 is a basis of L_1 and $L_1(\mathbb{Z})$). There exists $f_1 \in (\mathbb{Z}^n)^*$ such that $\langle f_1, x_1\rangle = 1$. By Proposition 1.1, for any $i \leq n$ the group $L_i(\mathbb{Z})$ is the direct sum of $L_1(\mathbb{Z})$ and $L_i(\mathbb{Z})(f_1)$. Similarly, for any $i \leq n$, L_i is a direct sum of L_1 and the kernel of f_1 on L_i.

The required basis for the flag $L_i \cap (\ker f_1)$ exists by induction. □

COROLLARY 2.4. *For any k-dimensional rational space $L \subset \mathbb{R}^n$, the group $L(\mathbb{Z})$ is isomorphic to $\mathbb{Z}^k$. Moreover, there is a basis $e_1, \ldots e_n$ of $\mathbb{Z}^n$ such that $e_1, \ldots, e_k$ is a basis of $L(\mathbb{Z})$.*

Lemma 2.3 gives a nice description of the group $Aut(\mathbb{Z}^n)$ of automorphisms of $\mathbb{Z}^n$. This description consists of two parts:

1. The group $Aut(\mathbb{Z}^n)$ acts on the space of complete rational flags and by Lemma 2 this action is transitive.
2. The stabilizer of the standard flag is the group of upper triangular integral matrices with 1 or -1 on the diagonal.

3. **Normal form of a subgroup of $\mathbb{Z}^n$** We say that a subgroup $G \subset \mathbb{Z}^n$ is in *normal form* with respect to a basis $e_1, \dots, e_n$ of $\mathbb{Z}^n$ if there exist $k \leq n$ and a collection of integers $a_1, \dots, a_k$ such that G is generated by the vectors $a_1 e_1, \dots, a_k e_k$ and a_i divides a_{i+1}, for $i = 1, \dots, k-1$. The sequence $a_1, \dots, a_k$ is called the *elementary divisors* of G.

Theorem 3.1 (Normal form theorem). *Any subgroup $G \subset \mathbb{Z}^n$ can be reduced to a normal form with respect to some basis of $\mathbb{Z}^n$.*

Proof. Let G be any subgroup of $\mathbb{Z}^n$. Let $A_1 = G \supset \cdots \supset A_l \neq 0 \supset A_{l+1} = 0$ be any F-compatible chain equipped with the sequences of elements $a_1, \dots, a_l$ and $c_1, \dots, c_l \in (\mathbb{Z}^n)^*$. By the decomposition theorem, G is the direct sum of the groups $(a_1), \dots, (a_l)$.

Let d_i be the characteristic number of the function $F(A_i, (\mathbb{Z}^n)^*)$. The vector $b_i = \dfrac{a_i}{d_i}$ is primitive, so b_i is F-conjugated with c_i for the pair $(\mathbb{Z}^n, (\mathbb{Z}^n)^*)$. Let $B_1 = \mathbb{Z}^n$ and $B_{i+1} = B_i(c_i)$. The chain of groups $B_1 \supset \cdots \supset B_l$ equipped with the sequences of elements $b_1, \dots, b_l$ and $c_1, \dots, c_l$ is F-compatible, so $\mathbb{Z}^n$ is the direct sum of groups $(b_1), \dots, (b_l)$ and B_{l+1}. Let $b_{l+1}, \dots, b_n$ be the extension of $b_1, \dots, b_l$ to the basis of $\mathbb{Z}^n$.

The group G is generated by the vectors $a_1 = d_1 b_1, \dots, a_l = d_l b_l$, and as $d_{i+1} \vdots d_i$, for any $i = 1, 2, \dots, k-1$, G is reduced to normal form with respect to the basis $b_1 \dots, b_n$. □

Remark. *To choose a basis of $\mathbb{Z}^n$ such that the group G is reduced to the normal form in this basis is the same as to find an automorphism of $\mathbb{Z}^n$ which reduces G to a normal form in the standard basis. We will use both of these points of view.*

The elementary divisors of two groups $G_1, G_2 \subset \mathbb{Z}^n$ coincide if, and only if, there is an automorphism A of $\mathbb{Z}^n$, such that $A(G_1) = G_2$.

4. **Integral volume** In this section we discuss the notion of integral volume. This notion has proved to be very useful in Newton polyhedra theory (see for example [3]), in the theory of multidimensional continued fractions (see for example [2]) and in several other areas.

On a real k-dimensional space L there is a Lebesgue measure invariant under translations, which is unique up to a scaling by a positive constant. Let $P(v_1, \dots, v_k) \subset L$ be a parallelepiped with the sides $v_1, \dots, v_k$.

Definition 4.1. *The integral k-volume on a k-dimensional rational space $L \subset \mathbb{R}^n$ is the invariant Lebesgue measure μ on L normalized by the condition $\mu(P(e_1, \dots, e_k)) = 1$ for some basis $e_1, \dots, e_k$ of the group $L(\mathbb{Z})$.*

The integral k-volume is well-defined: a linear map $A : L \to L$ that maps a basis of $\mathbb{Z}^k$ to another basis of $\mathbb{Z}^k$ has determinant 1 or -1, i.e. A preserves an invariant measure on L.

The *integral length* of the vector $v \in \mathbb{Z}^n$ is by definition the integral 1-volume of the segment $P(v)$ containing the points λv for $0 \leq \lambda \leq 1$. It is easy to see that the integral length of $v \in \mathbb{Z}^n$ is equal to:

(1) the number of points $x \in \mathbb{Z}^n$ that can be represented in the fom $x = \lambda v$ for $0 \leq \lambda < 1$;
(2) the number of elements of finite order in the group $\mathbb{Z}^n/G$, where G is the group generated by v;
(3) the greatest common divisor of the coordinates of v with respect to some basis of $\mathbb{Z}^n$.

Theorem 4.2 below generalizes these facts. To formulate it, we need the following observation. If $e_1, \ldots, e_n$ is the standard basis of $\mathbb{R}^n$, then the multi-vectors $e_{i_1} \wedge \cdots \wedge e_{i_k}$, where $1 \leq i_1 < \cdots < i_k \leq n$, form a basis of $\Lambda^k\mathbb{R}^n$. The group $\Lambda^k\mathbb{Z}^n$ is the standard integer lattice of $\Lambda^k\mathbb{R}^n$ with respect to this basis.

THEOREM 4.2. *Assume that then vectors $v_1, \ldots, v_k \in \mathbb{Z}^n \subset \mathbb{R}^n$ are linearly independent over $\mathbb{Q}$, and let L be the rational space spanned by them. The integral k-volume of the parallelepiped $P(v_1, \ldots, v_k) \subset L$ is equal to:*

(i) the number of points $x \in \mathbb{Z}^n$ that can be represented in the form $x = \lambda_1 v_1 + \ldots + \lambda_k v_k$, where $0 \leq \lambda_i < 1$, $i = 1, \ldots k$;
(ii) the number of elements of finite order in the group $\mathbb{Z}^n/G$, where G is the group generated by $v_1, \ldots, v_k$;
(iii) the integral length of the vector $v_1 \wedge \ldots \wedge v_k \in \Lambda^k\mathbb{Z}^n$, or in other words the greatest common divisor of all coordinates of the vectors $v_1 \wedge \ldots \wedge v_k$ with respect to some basis of $\Lambda^k\mathbb{Z}^n$.

PROOF. The quantities defined in $(i) - (iii)$ are invariant under the action of automorphisms of the lattice $\mathbb{Z}^n$. Let us prove it for the third quantity. An automorphism A of the lattice $\mathbb{Z}^n$ defines an automorphism $\Lambda^m A$ of $\Lambda^m\mathbb{Z}^n$. As $\Lambda^m A$ is an automorphism, it does not change integral length of vectors.

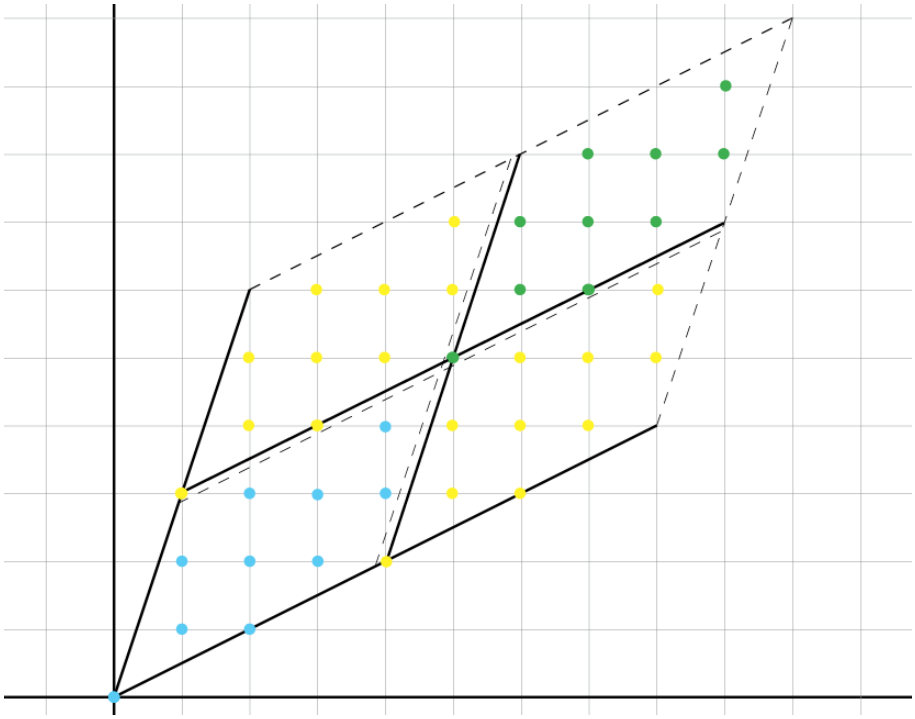
As all three quantities from Theorem 4.2 are invariant under the action of automorphisms of the lattice $\mathbb{Z}^n$, by the normal form theorem we can consider only collections in the normal form. For such collections the statement of the theorem is obvious. □

The equality of the quantity in (i) and the integral volume of a collection of vectors can be proved in another way without using the normal form theorem.

LEMMA 4.3. *Let vectors $v_1, \ldots, v_m \in \mathbb{Z}^m \subset \mathbb{R}^m$ be linearly independent over $\mathbb{Q}$. Then the number of points $x \in \mathbb{Z}^m$ that can be represented in a form $x = \lambda_1 v_1 + + \ldots + \lambda_k v_k$, where $0 \leq \lambda_i < 1$, $i = 1, \ldots k$, $(n(v_1, v_2, \ldots, v_m))$ equals to the integer m-volume of the parallelepiped P generated by vectors $v_1, v_2, \ldots, v_m$ $(Vol_i(P))$.*

PROOF. Denote by kP the image of the parallelogram P under the homothety with coefficient k. The number of all integer points inside kP asymptotically for

k tends to infinity equals to the $k^m Vol_i(P)$ and asymptotically equals to $k^m n(P)$ (see picture below). Therefore $n(P) = Vol_i(P)$. □



5. **Geometry of $\mathbb{Z}^n$ and normal form theorem** Consider the following problem:

PROBLEM 5.1. *Let $V \subset \mathbb{Z}^n$ be a given set. Find the elementary divisors of the group $G(V)$ generated by V.*

For a finite set V an algorithm of reduction of the integer matrix which has vectors from V as columns to Smith normal form gives a reduction of the group $G(V)$ to normal form. Therefore, Smith's theorem solves the problem.

The theorem below provides an algorithmic solution of this problem without finding the basis with respect to which $G(V)$ is reduced to a normal form, and explains the geometrical meaning of the elementary divisors of $G(V)$.

THEOREM 5.2. *Let $a_1, \dots, a_k$ be the elementary divisors of $G(V)$. Then for any $1 \le l \le k$ the product $\Pi_{i=1}^{l} a_i$ is equal to the greatest common divisor of integral l-volumes of all l-dimensional parallelepipeds with sides belonging to V.*

PROOF. The theorem immediately follows from the normal form theorem. Indeed, for a group in the normal form the statement of the theorem is clear, but $G(V)$ can be reduced to the normal form by a lattice automorphism, which does not change the integral volume of the collection of vectors. □

6. **Classification of the finitely generated abelian groups** The following theorem is classical (see [1] for example).

THEOREM 6.1 (Classification theorem). *Any finitely generated abelian group G is isomorphic to a group:*

$$(\mathbb{Z}/b_1\mathbb{Z}) \oplus (\mathbb{Z}/b_2\mathbb{Z}) \oplus \ldots \oplus (\mathbb{Z}/b_l\mathbb{Z}) \oplus \mathbb{Z}^k,$$

where b_i divides b_{i+1} for any $1 \leqslant i \leqslant \mathrm{l}-1$.

PROOF. The group G is isomorphic to the factor group $\mathbb{Z}^n/G_f$, where G_f is a subgroup of $\mathbb{Z}^n$ generated by relations on the generators of G. The group G_f can be reduced to the normal form in some basis of $\mathbb{Z}^n$.

Let $a_1, \ldots, a_m$ be the elementary divisors of G_f. Assume that $a_1 = \ldots = a_s = 1$, and $a_{s+1} \neq 1$. Then, $G \cong \mathbb{Z}^n/G_f$ is isomorphic to a group:

$$(\mathbb{Z}/b_1\mathbb{Z}) \oplus (\mathbb{Z}/b_2\mathbb{Z}) \oplus \ldots \oplus (\mathbb{Z}/b_l\mathbb{Z}) \oplus \mathbb{Z}^k,$$

where the numbers $b_1, \ldots, b_l$ and k can be found as follows. First of all $l = m-s$, then for $1 \leq i \leq l = m-s$,

$$b_i = a_{i+s}, \quad k = n - m.$$

□

Therefore, Theorem 5.2 also solves the following problem.

PROBLEM 6.2. *Find the numbers $b_1, \ldots, b_l$ and k for an abelian group G defined by a given set of generators $e_1, \ldots, e_n$ and by a given set V of relations between them.*

Let us consider two examples of applications of Theorem 5.2.

EXAMPLE 6.3. *Let $V = \{v_1 = (-1,-1,-6), v_2 = (2,0,2), v_3 = (3,-1,-2)\} \in \mathbb{Z}^3$. Find the elementary divisors of the group $G(V)$ generated by V.*

Note that $\Lambda^2 V = \{v_1 \wedge v_2 = (-2,4,-2), v_1 \wedge v_3 = (4,20,-4), v_2 \wedge v_3 = (-2,10,2)\}$ and $\Lambda^3 V = \{v_1 \wedge v_2 \wedge v_3 = 0\}$. Hence the elementary divisors of the group $G(V)$ are $a_1 = 1, a_2 = 2$. Indeed, in the basis $e_1 = (-1,-1,-6), e_2 = (1,0,1)$, $e_3 = (-1,-1,-5)$ the group G_V is generated by vectors e_1 and $2e_2$.

Example 6.4. *Let G be an abelian group generated by u_1, u_2, u_3 with the relations:*

$$\begin{aligned} -u_1 - u_2 - 6u_3 &= 0; \\ 2u_1 + 2u_3 &= 0; \\ 3u_1 - u_2 - 2u_3 &= 0. \end{aligned}$$

Find the numbers $b_1, \ldots, b_l$ and k from the classification theorem for G.

As the elementary divisors for the group G_V (see Example 6.4) are $a_1 = 1$, $a_2 = 2$, G is isomorphic to the group:

$$(\mathbb{Z}/2)Z \oplus \mathbb{Z}.$$

References

1. Dummit, D., Foote R. (2004). *Abstract Algebra, 3rd Edition*, John Wiley & Sons, Inc., Hoboken, NJ.
2. Karpenkov, O. (2013.) *Geometry of Continued Fractions*, Algorithms and Computation in Mathematics, 26, Springer, Heidelberg.
3. Kushnirenko, A. G. (1975). Newton polyhedron and Milnor numbers, *Functional Analysis and Its Applications*, **9**(1), 74–75.
4. Smith, H. J. S. (1861). On systems of linear indeterminate equations and congruences, *Phil. Trans. R. Soc. Lond.*, **151**(1), 293–326.

Department of Mathematics, University of Toronto, Toronto, ON Canada M5S 2E4
e-mail: lmonin@math.toronto.edu