RESEARCH PAPERS

Acta Cryst. (1998). A**54**, 517–531

Crystallographic Algorithms and Tables

J. Opgenorth, W. Plesken* and T. Schulz

RWTH Aachen, Lehrstuhl B für Mathematik, Templergraben 64, 52062 Aachen, Germany.
E-mail: plesken@willi.math.rwth-achen.de

(*Received 4 August 1997; accepted 5 November 1997*)

Abstract

A survey of definitions, theorems and algorithms for crystallographic groups are given in a dimension-independent fashion. These and some tables (including the Bravais groups up to dimension 6) form the basis of the computer package *CARAT*, which can handle crystallographic space groups up to dimension 6.

1. Introduction

International Tables for Crystallography, Vol A (Hahn, 1995) cannot easily be extended to higher dimensions, mainly because the number of affine classes of space groups (= affine space-group types, *e.g.* 219 in three dimensions) grows rapidly with the dimension. Four (Brown *et al.*, 1977) seems to be the dimension where such an extension still makes sense. Since there is a demand for it (Janner & Janssen, 1977; Janssen, 1986; Janssen *et al.*, 1992), we suggest a set of algorithms and tables for handling space groups up to dimension 6 in the present paper. These tables and algorithms have been put together into a computer package called *CARAT*, the first test versions of which are available *via* the Internet (http://samuel.math.rwth-aachen.de/~LBFM/carat/). The general philosophy is to design parameter sets for isomorphism types of space groups, which enable the user of the package to construct and recognize groups. Some basic information is contained in tables, *e.g.* a table of Bravais groups; other information can be computed, *e.g.* testing $\mathbb{Z}$-equivalence or determining generators of normalizers of crystallographic point groups. In some cases, it does not make sense to output all computable information but to count the number of objects only and to be able to compare the specific ones in which one is interested.

Obviously, the very basis of designing such a package is to have precise definitions for the equivalence relations of the groups to be considered. Though they are in the literature, the short repetition of the basic definitions and structures in §2 will hopefully avoid misunderstandings. Next comes a description of the basic tasks to be performed in §3. These vary in difficulty and complexity. Therefore, a rough idea of the algorithms involved might be somewhat helpful; the remaining §4 gives details on that, in particular on the newly developed algorithms. We have taken pains to enable even the inexperienced user to get relevant information from the system, *i.e.* some global commands are designed to perform tasks that one would normally do in several steps. In principle, the user can build up his own library of groups and identify new groups with the old ones in his library, if a relevant equivalence exists, or otherwise add the group to his library. In this way, the system mimics a learning process.

Since the terminology used by crystallographers and the one used by mathematicians does not always agree, we give a dictionary in Table 1 and use mainly the mathematical notation. Generally speaking, crystallographers prefer to think of their groups as groups of mapping, whereas *CARAT* deals with the associated groups of matrices obtained by choosing a coordinate system. Another difference is that the crystallographer usually does his computations in some fixed coordinate system by fixing a 'conventional' cell, thus allowing non-integral coefficiencts for translations of 'centered' lattices, whereas *CARAT* prefers to work with coordinates such that the translation vectors of the translation lattice consist of all integral columns.

2. Basic definitions

2.1. *General definitions and structures*

The most important concept of group theory is that of group actions. This concept cannot be overstressed, since it is the guiding principle behind most applications as well as in the general theory and in the present algorithmic context. It is particularly evident in geometric situations like in crystallography, where it makes the basic equivalence relations natural and algorithmically approachable.

Definition 1. (Alperin & Bell, 1995.) Let G be a group with unit element 1 and let M be a set:

(i) G *acts* or *operates* on M (from the left) if there is a mapping $G \times M \to M$ which takes the pair $(g, m) \in G \times M$ to the element gm of M such that

Table 1. *Corresponding terms in mathematical and crystallographic terminology*

Mathematical terminology	Crystallographic terminology
$\mathbb{Z}$-class	Arithmetic crystal class
$\mathbb{Q}$-class	Geometric crystal class
Bravais flock	Bravais type
Affine class of space groups	Space-group type
Lattice basis	Primitive basis
Finite unimodular groups	Crystallographic point groups
Degree (*e.g.* space groups of degree n)	Dimension (*e.g.* n-dimensional space groups)
Stablizers in space groups of points)	Site-symmetry groups

$g_2(g_1m) = (g_2g_1)m$ for all $g_1, g_2 \in G$ and all $m \in M$

(note on the left side the action map is applied twice, on the right side one such application is replaced by a group multiplication) and

$$1m = m \text{ for all } m \in M.$$

If G acts on M, one calls M a *G-set*.

(ii) If G acts on M, two elements $m_1, m_2 \in M$ lie *in the same orbit*, if there is a $g \in G$ with $gm_1 = m_2$. 'Being in the same orbit' is an equivalence relation on M, sometimes denoted by $\sim_G$, *i.e.* the *G-orbits* $Gm := \{gm | g \in G\}$ for $m \in M$ partition M into pairwise disjoint subsets. The set $M/\sim_G$ of equivalence classes or orbits is usually denoted by $G\backslash M$ (and called the quotient M mod G).

(iii) If G acts on M and $m \in M$, then $G_m := \{g \in G | gm = m\}$ is called the *stabilizer* of m in G. (Clearly, G_m is a subgroup of G, in symbols $G_m \leq G$.) The intersection of all stabilizers G_m with $m \in M$ is called the *kernel of the action* (and is a normal subgroup of G). (Stabilizers in space groups of points in affine space are more familiar to crystallographers under the name site-symmetry groups.)

(iv) If G acts on two sets M_1 and M_2, a map $\phi : M_1 \to M_2$ is called a *G-map* or *compatible with G*, if $\phi(gm) = g\phi(m)$ for all $g \in G$ and $m \in M_1$. If ϕ is bijective, it is called a *similarity* and the two actions are called *similar*.

When one analyses the definition of G action on a set M, one sees that it amounts to having a homomorphism of G into the group of all permutations of M. Therefore, one also uses the term *permutation representation* in this context. If M carries additional structure, like being an affine space or a vector space and the permutation group is replaced by the automorphism group of the structure, the action gets the corresponding attribute, like being affine or linear. This means that for each $g \in G$ the induced map $\bar{g} : M \to M : m \to gm$ preserves the structure of M, *e.g.* it is affine or linear. Of course, if a group G acts on a set M, each of its subgroups also acts on M and respects the structure of M if G does. It is also implicitly understood that G-maps between G-sets with preserved structures are also compatible with these structures. The investigation of linear actions of groups on vector spaces forms an important part of group theory called representation theory (Alperin & Bell, 1995; Curtis & Reiner, 1962; Serre, 1977). In the sequel, $K^{m\times n}$ denotes the set of all $m \times n$ matrices with entries in K, which is usually the field $\mathbb{Q}$ of rational numbers or $\mathbb{R}$ of real numbers, or the ring $\mathbb{Z}$ of rational integers.

Example 1.

(i) The *general linear group* $GL_n(K) := \{g \in K^{n\times n} | \det(g) \neq 0,$ *i.e.* g is invertible$\}$ over a field K like the field $\mathbb{Q}$ of rational numbers or the field $\mathbb{R}$ of real numbers acts on the K-vector space $K^{n\times 1}$ of n columns over K by matrix multiplication from the left. This is a linear action. One checks easily that self-similarities of $K^{n\times 1}$ as $GL_n(K)$ set are given by multiplications with nonzero elements of K.

(ii) $GL_n(\mathbb{R})$ acts linearly on $\mathbb{R}^{n\times n}_{\text{sym}} := \{F \in \mathbb{R}^{n\times n} | F^{\text{tr}} = F\}$, where $g \in GL_n(\mathbb{R})$ maps $F \in \mathbb{R}^{n\times n}_{\text{sym}}$ onto $g^{-\text{tr}}Fg^{-1}$. [Here and in the sequel, $g^{-\text{tr}} := (g^{-1})^{\text{tr}} = (g^{\text{tr}})^{-1}$ is the transpose of the inverse of the invertible matrix g.] The positive-definite symmetric matrices of degree n ('metric tensors') form one orbit $\mathbb{R}^{n\times n}_{\text{sym},\,>0}$ and the stabilizer of the unit matrix I_n is the *orthogonal group* $O_n(\mathbb{R})$.

(iii) $GL_n(\mathbb{Q})$ acts on $\mathcal{Z}_n := \{L | L$ is a full $\mathbb{Z}$ lattice in $\mathbb{Q}^{n\times 1}\}$, where a full $\mathbb{Z}$ lattice in $\mathbb{Q}^{n\times 1}$ consists of the $\mathbb{Z}$ linear combinations of a $\mathbb{Q}$-basis of $\mathbb{Q}^{n\times 1}$. Here, $gL := \{gl | l \in L\}$ for any $g \in GL_n(\mathbb{Q})$, $L \in \mathcal{Z}_n$. This action is *transitive, i.e.* it has just one orbit. The stabilizer of $L = \mathbb{Z}^{n\times 1}$ is $GL_n(\mathbb{Z})$.

(iv) $GL_n(\mathbb{Z})$ acts on all the sets in (i) (ii) and (iii) since it is a subgroup of each of the groups there. In particular, a *Bravais group* can be defined to be the stabilizer of a positive-definite matrix $F \in \mathbb{R}^{n\times n}_{\text{sym}}$ in $GL_n(\mathbb{Z})$. Such a Bravais group is necessarily finite; details will be discussed later.

(v) $GL_{n+1}(\mathbb{R})$ acts linearly on the $\mathbb{R}$-vector space $\mathbb{R}^{1\times(n+1)}$ of $(n+1)$ rows by $gr := rg^{-1}$. The stablizer of $e_{n+1} := (0, \ldots, 0, 1)$ is called the *affine group* $\text{Aff}_n(\mathbb{R})$, which acts *via* matrix multiplication from the left on the n-dimensional *affine space* $A_n(\mathbb{R})$, which we define as $A_n(\mathbb{R}) := \{x \in \mathbb{R}^{(n+1)\times 1} | e_{n+1}x = 1\}$ consisting of augmented columns of the form $\binom{a}{1}$ with $a \in \mathbb{R}^{n\times 1}$. In more concrete terms, the elements g of $\text{Aff}_n(\mathbb{R})$ are augmented matrices, *i.e.* matrices of the form

$$g = \begin{pmatrix} h & t \\ 0 & 1 \end{pmatrix},$$

where $h \in GL_n(\mathbb{R})$ is called the *linear part* of g, $t \in \mathbb{R}^{n\times 1}$, and 0 stands for an n row of zeros. The action g of $\mathrm{Aff}_n(\mathbb{R})$ on $A_n(\mathbb{R})$ is given by matrix multiplication:

$$g = \begin{pmatrix} h & t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a \\ 1 \end{pmatrix} = \begin{pmatrix} ha+t \\ 1 \end{pmatrix}.$$

Requiring h to lie in $O_n(\mathbb{R})$ rather than in $GL_n(\mathbb{R})$ yields the *Euclidean group* Eucl_n of *Euclidean motions* (written as matrices). Restricting h even further to be the unit matrix I_n yields the *translation group*. Since Eucl_n is a subgroup of the affine group $\mathrm{Aff}_n(\mathbb{R})$, one obtains the action of the Euclidean group on the affine space $A_n(\mathbb{R})$ in this set up.

(vi) (*Cf.* Alperin & Bell, 1995.) If G is any group and U a subgroup of G, then G acts on the set $G/U := \{gU | g \in G\}$ of *cosets* of U in G by multiplication from the left: $G \times G/U : (g, hU) \mapsto ghU$. This action is transitive and any transitive action of G on some set M is similar to this action for a suitable choice of U, namely $U = G_m$ the stabilizer of any $m \in M$ in G. This well known fact will also be used in *CARAT* to compute subgroups of finite groups: Say G is finite and we are interested in the subgroups H of G containing U. Then $H/U \subseteq G/U$ forms a block for the G-action. A subset N of the transitive G-set M is called a block if the images of N under G are pairwise disjoint, *i.e.* form a partition of M. Since blocks containing a fixed $m \in M$ are in bijection with the subgroups H with $G_m \leq H \leq G$ and since blocks are usually easy to compute, this gives a good way to compute subgroups in certain specialized situations.

The main interest in this paper lies in finite subgroups of $GL_n(\mathbb{Z})$ because they turn up as point groups of space groups. To classify them, we work with various notions of conjugation action, which can also be defined in a quite general context.

Example 2. (*Cf.* Alperin & Bell, 1995.) Let G be a group.

(i) G acts on $M := G$ *via conjugation, i.e.* $G \times G \to G : (g, m) \mapsto {}^g m := gmg^{-1}$. The orbits of this action are called *conjugacy classes of elements* and the stabilizers are called *centralizers*. This action actually respects the group structure of $M = G$, *i.e.* each $g \in G$ induces an automorphism of G, called the inner automorphism induced by g.

(ii) Denote the set of all subgroups of G by $\mathcal{U}(G)$. Then the conjugation action of G on G induces a conjugation action of G on $\mathcal{U}(G)$, for which we also use the exponent notation, *i.e.* ${}^g U := \{{}^g u | u \in U\}$ for any $U \leq G$, $g \in G$. The orbits under this action are the *conjugacy classes of subgroups* and the stabilizers are the *normalizers, i.e.* $N_G(U) := \{g \in G | gUg^{-1} = U\}$ is called the normalizer of $U \leq G$ in G. Note that the set $\mathcal{U}_{\mathrm{fin}}(G)$ of finite subgroups of G is invariant (as a whole) under the conjugation action of G, and therefore G acts on $\mathcal{U}_{\mathrm{fin}}(G)$ as well.

In the notation developed so far, one of the most complicated issues we are dealing with is to enumerate $GL_n(\mathbb{Z})\backslash\mathcal{U}_{\mathrm{fin}}(GL_n(\mathbb{Z}))$ and to recognize for any given element $U \in \mathcal{U}_{\mathrm{fin}}(GL_n(\mathbb{Z}))$ to which conjugacy class it belongs, or, in more conventional terms: find the $\mathbb{Z}$-classes [= $GL_n(\mathbb{Z})$-conjugacy classes] of finite unimodular groups of degree n [= finite subgroups of $GL_n(\mathbb{Z})$] and give a method of deciding to which $\mathbb{Z}$-class a given group belongs. Since this task gets rather difficult if the degree n gets bigger, we deal with two easier tasks first:

(i) classify the finite unimodular groups only up to $\mathbb{Q}$-equivalence, *i.e.* up to conjugacy in $GL_n(\mathbb{Q})$;

(ii) classify only the $\mathbb{Z}$-classes of Bravais groups.

Before we go into the details of these two points, we repeat a metamathematical remark by H. Zassenhaus, whose pioneering work made the development presented here possible (Plesken, 1996): Whenever you classify subgroups, also describe their normalizers. We give ample evidence of the wisdom of this statement below. The main reason is that the normalizer plays the role of a geometric automorphism group of the whole situation considered.

Remark 1. Let G be a group acting on a set M and let $U \leq G$ be a subgroup of G. Then the action of G on M induces an action of $N_G(U)$ on the set $U\backslash M$ of U orbits:

$$N_G(U) \times U\backslash M \to U\backslash M : (n, Um) \mapsto nUm = Unm.$$

In particular, the set

$$\mathrm{Fix}_U(M) := \{m \in M | um = m \text{ for all } u \in U\}$$

is an $N_G(U)$ set.

2.2. *Rational and integral equivalence: invariant lattices*

Classifying $\mathbb{Q}$-classes of finite subgroups of $GL_n(\mathbb{Z})$ really amounts to classifying conjugacy classes of finite subgroups of $GL_n(\mathbb{Q})$, *i.e.* finding representatives of $GL_n(\mathbb{Q})\backslash\mathcal{U}_{\mathrm{fin}}(GL_n(\mathbb{Q}))$. This follows immediately from part (i) of the following remark, which is already due to Burnside. Because of this, we can often use the terms $\mathbb{Q}$-class of a finite unimodular group and the $GL_n(\mathbb{Q})$-conjugacy class of groups containing it as synonymous.

Remark 2. Let G be a finite subgroup of $GL_n(\mathbb{Q})$.

(i) $\mathcal{Z}(G) := \mathrm{Fix}_G(\mathcal{Z}_n)$ is not empty, *i.e.* there exists a G-invariant lattice in $\mathbb{Q}^{n\times 1}$. In particular, G is conjugate under $GL_n(\mathbb{Q})$ to a subgroup of $GL_n(\mathbb{Z})$.

(ii) $N_{GL_n(\mathbb{Q})}(G)\backslash\mathcal{Z}(G)$ is in bijection with the $\mathbb{Z}$-classes in the $\mathbb{Q}$-class of G.

Proof.

(i) Choose an arbitrary lattice $L_0 \in \mathcal{Z}_n$ and take L to be the lattice generated by all gL_0 with $g \in G$. Since all the gL_0 lie in $\mathbb{Q}^{n\times 1}$ and are permuted by G, one has $L \in \mathrm{Fix}_G(\mathbb{Z}_n)$. Writing the action of G on L with respect to a lattice basis amounts to conjugating G into $GL_n(\mathbb{Z})$.

(ii) Easy.

A good example for (ii) is the trivial group $\langle I_n\rangle < GL_n(\mathbb{Q})$.

Note that a $\mathbb{Q}$-class splitting only into finitely many $\mathbb{Z}$-classes is the content of the famous Jordan–Zassenhaus theorem (Zassenhaus, 1938). We might be able to provide a list of representatives of $\mathbb{Q}$-classes up to degree $n \leq 6$. An algorithm deciding whether two finite subgroups of $GL_n(\mathbb{Q})$ are conjugate is described later on.

We take the opportunity to demonstrate the use of maps compatible with group actions in the context of Remark 2. First, recall from representation theory the notions of *(rational) enveloping algebra*

$$\overline{\mathbb{Q}G} := \left\{ \sum_{g\in G} a_g g \in \mathbb{Q}^{n\times n} | a_g \in \mathbb{Q} \text{ for all } g \in G \right\}$$

and of the *commuting algebra* $C_{\mathbb{Q}}(G) := \{c \in \mathbb{Q}^{n\times n} | cg = gc \text{ for all } g \in G\}$ of a finite subgroup G of $GL_n(\mathbb{Q})$. The centre $\overline{\mathbb{Q}G} \cap C_{\mathbb{Q}}(G)$ of the enveloping algebra $\overline{\mathbb{Q}G}$ has a unique set of primitive idempotents (or projection operators) $e_1, \ldots, e_s$, where s is the number of homogeneous components of $\mathbb{Q}^{n\times 1}$ as $\mathbb{Q}G$-module, in fact the $e_i\mathbb{Q}^{n\times 1}$ are the homogeneous components of this module.

Remark 3. (Plesken, 1978, 1981.) Let G be a finite subgroup of $GL_n(\mathbb{Q})$ and $e_1, \ldots, e_s$ be the primitive idempotents of the centre of $\overline{\mathbb{Q}G}$.

(i) The elements of $\mathcal{Z}^{\mathrm{h.d.}}(G) := \{L \in \mathcal{Z}(G) | L = \oplus_{i=1}^{s} e_i L\}$ are permuted amongst themselves by the $N_{GL_n(\mathbb{Q})}(G)$ action. [The elements of $\mathcal{Z}^{\mathrm{h.d.}}(G)$ are called homogeneously decomposable† G-lattices.]

(ii) $\theta : \mathcal{Z}(G) \to \mathcal{Z}^{\mathrm{h.d.}}(G) : L \mapsto \oplus_{t+1}^{s} e_i L$ is an $N_{GL_n(\mathbb{Q})}(G)$-map.

(iii) The fibres of θ are finite, *i.e.* for any homogeneously decomposable lattice $L \in Z^{\mathrm{h.d.}}(G)$ the set $\theta^{-1}(L) := \{X \in \mathcal{Z}(G) | \oplus_{i=1}^{s} e_i X = L\}$ is finite. [In fact, each $X \in \theta^{-1}(L)$ satisfies $|G|L \leq X \leq L$.]

(iv) For any $L \in \mathcal{Z}(G)$ let $N_L(G)$ denote the stabilizer of L in $N_{GL_n(\mathbb{Q})}(G)$. For $L \in \mathcal{Z}^{\mathrm{h.d.}}(G)$, the action of $N_{GL_n(\mathbb{Q})}(G)$ on $\mathcal{Z}(G)$ induces an action of the stabilizer $N_L(G)$ on $\theta^{-1}(L)$ such that

(*a*) For $X \in \theta^{-1}(L)$ the stabilizer of X in $N_L(G)$ is equal to $N_X(G)$.

(*b*) Let $\{L_1, \ldots, L_d\}$ be a set of representatives of $N_{GL_n(\mathbb{Q})}(G)\backslash\mathcal{Z}^{\mathrm{h.d.}}(G)$ and for each i, $1 \leq i \leq d$, let R_i be a set of representatives of $N_{L_i}(G)\backslash\theta^{-1}(L_i)$. Then, $\cup_{i=1}^{d} R_i$ is a set of representatives of $N_{GL_n(\mathbb{Q})}(G)\backslash\mathcal{Z}(G)$.

The reader will have noticed already that writing matrices with respect to a lattice basis B of $L \in \mathcal{Z}(G)$ turns G into a finite unimodular group G_B and $N(L)$ into $N(L)_B = N_{GL_n(\mathbb{Z})}(G_B)$. Remark 3 will turn out to be a valuable tool in the algorithmic splitting of $\mathbb{Q}$-classes into $\mathbb{Z}$-classes. There are some situations where the crystallographic notion of primitivity (based on a case-to-case definition) is related to the concept of homogeneous decomposability above.

2.3. *Bravais groups and invariant quadratic forms*

In complete analogy to Remark 2, one has the following remark in respect to the action of $GL_n(\mathbb{R})$ on $\mathbb{R}^{n\times n}_{\mathrm{sym},\,>0}$ described in Remark 2(i), which is also classical, probably due to Maschke.

Remark 4. Let G be a finite subgroup of $GL_n(\mathbb{R})$.

(i) $\mathrm{Fix}_G(\mathbb{R}^{n\times n}_{\mathrm{sym},\,>0})$ is not empty, *i.e.* there exists a G-invariant positive-definite symmetric matrix. In particular, G is conjugated under $GL_n(\mathbb{R})$ to a subgroup of $O_n(\mathbb{R})$.

(ii) $N_{GL_n(\mathbb{R})}(G)\backslash\mathrm{Fix}_G(\mathbb{R}^{n\times n}_{\mathrm{sym},\,>0})$ consists of just one element, *i.e.* the action is transitive. In particular, any two subgroups of $O_n(\mathbb{R})$ that are conjugate under $GL_n(\mathbb{R})$ are conjugate to each other $O_n(\mathbb{R})$.

Definition 2. (Brown *et al.*, 1973, 1977.) Let $G \leq GL_n(\mathbb{Z})$ be a finite unimodular group.

(i) $\mathcal{F}(G) := \mathrm{Fix}_G(\mathbb{R}^{n\times n}_{\mathrm{sym}}) = \{F \in \mathbb{R}^{n\times n}_{\mathrm{sym}} | g^{\mathrm{tr}} F g = F \text{ for all } g \in G\}$ is called the *space of (invariant) forms of* G and $\mathcal{F}_{>0}(G) := \{F \in \mathcal{F}(G) | F \text{ positive definite}\}$ is called the *Bravais manifold of* G.

(ii) For any subset $\mathcal{F}$ of $\mathbb{R}^{n\times n}_{\mathrm{sym}}$ containing at least one positive-definite matrix $B(\mathcal{F}) := \{g \in GL_n(\mathbb{Z}) | g^{\mathrm{tr}} F g = F \text{ for all } F \in \mathcal{F}\}$ is called the *Bravais group of* $\mathcal{F}$.

(iii) $B(G) := B(\mathcal{F}(G))$ is called the *Bravais group of* G.

(iv) Two finite subgroups of $GL_n(\mathbb{Z})$ belong to the same *Bravais flock* or are called *Bravais equivalent*, if their Bravais groups are $\mathbb{Z}$-equivalent.‡

† In the original publications (Plesken, 1981; Plesken & Hanrath, 1984) the term almost decomposable was used.

‡ In view of Hahn (1995, p. 721), one might prefer the slightly more precise term 'Bravais flock of matrix groups'. Though we speak of Bravais equivalence, we do not use the term Bravais classes for Bravais flocks to avoid the confusion with $\mathbb{Z}$-classes of Bravais groups.

Clearly, $\mathcal{F}(G)$ is a real vector space, $\mathcal{F}_{>0}(G)$ is non-empty, in fact $\mathcal{F}_{>0}(G)$ is an open cone in $\mathcal{F}(G)$. The Bravais group $B(\mathcal{F})$ is a finite unimodular group and, since $\mathcal{F}(G) = \mathcal{F}(B(G))$, one has $B(B(G)) = B(G)$. Finally, if two finite unimodular groups are $\mathbb{Z}$-equivalent, their Bravais groups are also $\mathbb{Z}$-equivalent. There is more than one reason why Bravais groups are important in the present context. They subdivide $\mathcal{U}_{\text{fin}}(GL_n(\mathbb{Z}))$ into finitely many Bravais flocks. Representatives of the $\mathbb{Z}$-classes of Bravais groups are available in *CARAT* up to degree 6. There are 1, 5, 14, 64,189, 841† classes of degree 1, 2, 3, 4, 5, 6, respectively. It is conceivable that the present version of *CARAT* could be extended by a command to compute a set of representatives of the $\mathbb{Z}$-classes in any given Bravais flock. Last, but not least, the normalizers of the Bravais groups in $GL_n(\mathbb{Z})$ can be computed *via* their action on the Bravais manifold. This is the key to computing generators for the normalizer of any finite unimodular group and for testing $\mathbb{Z}$-equivalence of finite unimodular groups. It is this final point we want to explain in some more detail now.

Remark 5. Let $G \leq GL_n(\mathbb{Z})$ be finite and $B := B(G)$ its Bravais group. Denote the normalizers of G and B in $GL_n(\mathbb{Z})$ by $N(G)$ and $N(B)$, respectively.

(i) $N(G)$ acts *properly discontinuously* on the Bravais manifold $\mathcal{F}_{>0}(G)$ (*cf*. Example 1 and Remark 2), *i.e.* the orbits are discrete subsets of the Bravais manifold and the stabilizers are finite.

(ii) $N(B) = \{g \in GL_n(\mathbb{Z}) | g^{\text{tr}}\mathcal{F}(B)g = \mathcal{F}(B)\}$. [Note that $\mathcal{F}(G) = \mathcal{F}(B)$.]

(iii) $N(G) \leq N(B)$ with finite index, in fact $N(G)$ is the stabilizer $N(B)_G$ of G in the conjugation action of $N(B)$ on the set of subgroups of B.

(iv) The action of $N(B)$ on $\mathcal{F}(B)$ is linear and the Bravais group B is equal to the kernel of the action.

In §4, we shall see that the discontinuous action of $N(B)$ on the Bravais manifold not only enables one to find generators for $N(B)$ but also to decide $\mathbb{Z}$-equivalence for Bravais groups. The geometry behind our procedure is of interest in itself, since it allows one to find the densest lattice packings of spheres with the given Bravais groups as an automorphism group. More to the point for $\mathbb{Z}$-equivalence of arbitrary finite unimodular groups, this is only a very finite problem by Remark 5(iii), after everything is dealt with on the level of Bravais groups.

For the analysis of crystal families in the next section, we need a slight variation of the notion of Bravais groups, which only differs from the one given above by working with all bilinear forms instead of the symmetric ones.

Definition 3. (Plesken, 1977; Plesken & Hanrath, 1984). Let $G \leq GL_n(\mathbb{Z})$ be a finite unimodular group.

(i) $\mathcal{F}_I(G) := \{F \in \mathbb{R}^{n\times n} | g^{\text{tr}}Fg = F \text{ for all } g \in G\}$ is called the *enlarged space of (invariant) forms* of G.

(ii) For any subset $\mathcal{F}$ of $\mathbb{R}^{n\times n}$ containing at least one symmetric positive-definite matrix, the group $B_I(\mathcal{F}) := \{g \in GL_n(\mathbb{Z}) | g^{\text{tr}}Fg = F \text{ for all } F \in \mathcal{F}\}$ is called the *strict Bravais group* of $\mathcal{F}$.

(iii) $B_I(G) := B_I(\mathcal{F}_I(G))$ is called the *strict Bravais group*‡ of G.

(iv) Two finite subgroups of $GL_n(\mathbb{Z})$ belong to the *same strict Bravais flock* or are called *strictly Bravais equivalent*, if their strict Bravais groups are $\mathbb{Z}$-equivalent.

Clearly, $G \leq B_I(G) \leq B(G)$ and $B_I(B_I(G)) = B_I(G)$, finally $B(B_I(G)) = B(G)$ and $B_I(B(G)) = B(G)$. For instance,

$$B_I\left[\left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle\right] = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$$

is of order 4 with

$$\mathcal{F}_I\left[\left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle\right] = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} | a, b \in \mathbb{R} \right\},$$

whereas the Bravais group is of order 8. The definition of strict Bravais flocks is not so natural from a geometric point of view, but very convenient from an algebraic point of view, since G and $B_I(G)$ not only have the same generalized space of invariant forms but also the same (rational) enveloping algebra $\overline{\mathbb{Q}G}$ and therefore also the same commuting algebra $C_{\mathbb{Q}}(G)$ introduced before Remark 3. The reason for this is that $C_{\mathbb{Q}}(G) = F_0^{-1}\mathcal{F}_I(G)$ for any nonsingular $F_0 \in \mathcal{F}_I(G)$.

2.4. *A symbol for crystal families*

When a finite unimodular group G is given, one will first try to find its crystal family, before one determines its Bravais type or its $\mathbb{Q}$-class, not only because this is a coarser subdivision of finite unimodular groups than either of the latter ones but also because crystal families can be given a meaningful symbol, which carries a lot of information about the structure. More important than the symbol itself is the fact that there are primitive symbols and a grammar by which the primitive symbols are put together. The notation for the primitive symbols and the symbols connecting the primitive symbols is a matter of taste and background.

† The original publication (Plesken & Hanrath, 1984) lists 826 classes. In preparing the inclusion tables for the Bravais groups, we found that four $\mathbb{Z}$-classes of Bravais groups were missing in the crystal family 3; 1, 1; 1 and nine $\mathbb{Z}$-classes of Bravais groups missing in the crystal family 3; 2-2; 1, one $\mathbb{Z}$-class in 4-1; 2-2, and one $\mathbb{Z}$ class in 4-1; 1; 1.

‡ The original publications (Plesken, 1977; Plesken & Hanrath, 1984) use the slightly misleading term generalized Bravais group.

Definition 4. (Brown *et al.*, 1977.) The classes of the finest equivalence relation on $\mathcal{U}_{\text{fin}}(GL_n(\mathbb{Z}))$ coarser than both $\mathbb{Q}$-equivalence and Bravais equivalence, are called *crystal families*. *I.e.* two finite subgroups, G, H of $GL_n(\mathbb{Z})$ belong to the same crystal family if there is a sequence of groups $G_i \leq GL_n(\mathbb{Z})$ for i running from 0 to some m, with $G = G_0$, $H = G_m$ and G_i is $\mathbb{Q}$-equivalent to G_{i+1} for some of the i's and Bravais equivalent for the remaining i's.

As an immediate consequence of the definition, one sees the following: If two finite unimodular groups G and H are in the same crystal family then there is a $t \in GL_n(\mathbb{Q})$ with $t\mathcal{F}(G)t^{\text{tr}} = \mathcal{F}(H)$. By using some elementary representation theory, one can assume that G is in the same crystal family as a group H with elements of the form

$$\text{diag}(\underbrace{h_1, \ldots, h_1}_{m_1}, \underbrace{h_2, \ldots, h_2}_{m_2}, \ldots, \underbrace{h_k, \ldots, h_k}_{m_k}),$$

where diag denotes a block-diagonal matrix and where the matrix h_i on the (block) diagonal runs through all elements of a finite unimodular group H_i of degree n_i and where each h_i occurs m_i times. Of course, $m_1n_1 + m_2n_2 + \ldots + m_kn_k = n$. The groups H_i can be taken to be irreducible, *i.e.* all the sublattices of $\mathbb{Z}^{n_i \times 1}$ they leave invariant are of finite index in $\mathbb{Z}^{n_i \times 1}$. We leave it as an easy exercise in representation theory to see that the matrices in $\mathcal{F}(H)$ are of the shape

$$\text{diag}(F_1, F_2, \ldots, F_k),$$

where the F_i are symmetric of degree m_in_i computable from H_i. The simplest case is when the multiplicity m_i is 1. Then the condition is simply $F_i \in \mathcal{F}(H_i)$. In case $m_i > 1$, the matrix F_i can be understood as an $m_i \times m_i$ 'block matrix' with (block) entries $f_{st}^{(i)} \in \mathbb{R}^{n_i \times n_i}$ of degree n_i with $1 \leq s, t \leq m_i$ satisfying

$$f_{st}^{(i)} = f_{ts}^{(i)\text{tr}} \quad \text{for all } s, t$$

and

$$h^{\text{tr}} f_{st}^{(i)} h = f_{st}^{(i)} \quad \text{for all } h \in H_i.$$

Since the off-diagonal blocks $f_{st}^{(i)}$ (with $s \neq t$) need not be symmetric, one is forced to consider enlarged spaces of invariant forms and strict Bravais groups introduced in Definition 3. In particular, we see that the second condition for the off-diagonal $f_{st}^{(i)}$ really means $f_{st}^{(i)} \in \mathcal{F}_I(H_i)$. Aiming at a symbol for the crystal family, one first needs to specify the constituent groups H_i more precisely. In case the multiplicity m_i is one, one only needs to specify in which irreducible crystal family H_i lies. Hence, we need symbols for the irreducible crystal families up to degree 6 (where irreducible of course means that all groups in the crystal family are irreducible). Next one needs to consider the slightly more complicated (and rarer) case $m_i > 1$. In this case, the above analysis shows that one has to introduce strict crystal families for irreducible groups. They are of course build up from strict Bravais flocks and $\mathbb{Q}$-classes in the same way as crystal families are from Bravais flocks and $\mathbb{Q}$-classes.

Definition 5. (Plesken & Hanrath, 1984.)

(i) The *symbols* for the irreducible crystal families of degree n are of the form n-s, where -s stands for some symbol (possibly empty) to be chosen to distinguish the irreducible families of degree n in case there is more than one. (These are called *primitive symbols of the first kind*.) For $1 \leq n \leq 6$, the following symbols have been chosen: 1, 2-1 (square), 2-2 (hexagonal), 3 (cubic), 4-1 (hypercubic), 4-1′ (octagonal), 4-2 (diisohexagonal orthogonal), 4-2′ (dodecagonal), 4-3 (icosahedral), 4-3′ (decagonal), 5-1 (hypercubic), 5-2, 6-1 (hypercubic), 6-2 (triisohexagonal orthogonal), 6-2′, 6-3, 6-3′, 6-4, 6-4′ (icosahedral). (The names are chosen such that n-i' usually contains subgroups of groups in n-i. The families containing the reflection groups of degree n isomorphic to the symmetric group on $n + 1$ symbols are 1, 2-2, 3, 4-3, 5-2, 6-3. The names in brackets are from Brown *et al.* (1977).

(ii) The *symbols* for the strict irreducible crystal families of degree n are of the form n-s, where -s stands for some symbol (possibly empty) to be chosen. (These are called *primitive symbols of the second kind*.) For $1 \leq n \leq 3$, the following symbols have been chosen: 1, 2-1 (square), 2-1′, 2-2 (hexagonal), 2-2′, 3 (cubic). (Again the names are chosen such that n-i' usually contains subgroups of groups in n-i. The family 1 and the strict family 1 are equal, the same for 3; the famly 2-1 is the union of the strict families 2-1 and 2-1′, also the family 2-2 is the union of the strict families 2-2 and 2-2′.)

(iii) The *symbol* for the crystal family containing the group H described above is

$$\underbrace{n_1\text{-}s_1, \ldots, n_1\text{-}s_1}_{m_1}; \underbrace{n_2\text{-}s_2, \ldots, n_2\text{-}s_2}_{m_2}; \underbrace{n_k\text{-}s_k, \ldots, n_k\text{-}s_k}_{m_k},$$

where n_i-s_i is the primitive symbol of the (irreducible) crystal family containing H_i in case $m_i = 1$ or it is the primitive symbol for the (irreducible) strict crystal family containing H_i in case $m_i > 1$.†

The reader might have noticed that everything becomes much easier if one only talks about strict crystal family. This notation differs slightly from the one originally introduced but it has the merit of being easy to input into a computer. It has also been suggested to use $\perp$ instead of semicolons (for obvious reasons); again the mathematics is only in the grammar and in the existence of the primitive symbols, not in the way the compounds of the symbol are visualized. The only ambiguity left is the order in which the symbols come. One can prove

† If one omits the -s_i parts of the symbol, one gets the decomposition scheme of Plesken (1981) of the crystal family. This defines a coarser equivalence relation than the concept of family.

Table 2. *Crystal families up to dimension 4*

Symbol	1	1, 1	1; 1	2-1	2-2	1, 1, 1	1, 1; 1	1; 1; 1	1; 2-1	1; 2-2	3
dim $\mathcal{F}(G)$	1	3	2	1	1	6	4	3	2	2	1

Symbol	1, 1, 1, 1	1, 1, 1; 1	1, 1; 1, 1	1, 1; 1; 1	1; 1; 1; 1	1, 1; 2-1	1; 1; 2-1
dim $\mathcal{F}(G)$	10	7	6	5	4	4	3

Symbol	1, 1; 2-2	1; 1; 2-2	1; 3	2-1, 2-1	2-1; 2-1	2-1′, 2-1′	2-1; 2-2
dim $\mathcal{F}(G)$	4	3	2	3	2	4	2

Symbol	2-2, 2-2	2-2; 2-2	2-2′, 2-2′	4-1	4-1′	4-2	4-2′	4-3	4-3′
dim $\mathcal{F}(G)$	3	2	4	1	2	1	2	1	2

that two symbols as defined above refer to the same crystal family if and only if they are obtained from each other by permuting the k sections separated by semicolons. To make the symbol unique, one could work with some lexicographic ordering according to some ordering of the primitive symbols, but the program is robust against such permutations. Table 2 shows the crystal families up to dimension 4.

As an advertisement for group actions, the reader who has missed explicit mentions of group actions in this section is reminded that the complete analysis is based on representation theory, *i.e.* the theory of linear group actions.

2.5. *Space groups*

The final issue concerns the space groups themselves. Recall from Example 1(v) the notation for the Euclidean group Eucl_n and its translation subgroup $T(\mathrm{Eucl}_n)$. An easy but essential fact is that $T(\mathrm{Eucl}_n)$ is a normal subgroup of Eucl_n and that the conjugation action of Eucl_n on $T(\mathrm{Eucl}_n)$ is (by the most obvious map) similar to its action on $\mathbb{R}^{n\times 1}$ *via* taking the linear parts of the Euclidean motions. Now a space group R is a subgroup of Eucl_n, whose translation subgroup $T(R) := R \cap T(\mathrm{Eucl}_n)$ is a full lattice in $T(\mathrm{Eucl}_n) \equiv \mathbb{R}^{n\times 1}$, *i.e.* spanned (as a group) by n $\mathbb{R}$-linearly independent vectors. This forces the group of linear parts of R to be a finite subgroup of $O_n(\mathbb{R})$, which upon choice of a lattice basis can be conjugated under $GL_n(\mathbb{R})$ into $GL_n(\mathbb{Z})$. The resulting finite unimodular group is unique up to conjugacy within $GL_n(\mathbb{Z})$. Writing the whole space group R now as matrices with respect to suitable coordinates yields a group as follows.

Definition 6. (Zassenhaus, 1948; Holt & Plesken, 1989.) Let $G \leq GL_n(\mathbb{Z})$ be a finite unimodular group.

(i) A map $v : G \to \mathbb{R}^{n\times 1}$ is called a *vector system*,† if $v(gh) \equiv v(g) + gv(h) (\mathrm{mod}\ \mathbb{Z}^{n\times 1})$ for all $g, h \in G$. The vector systems form a group $V(G, \mathbb{R}^{n\times 1})$ under addition. Each vector system $v \in V(G, \mathbb{R}^{n\times 1})$ induces a *1-cocycle* $\bar{v} : G \to \mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1} : g \mapsto v(g) + \mathbb{Z}^{n\times 1}$ taking values in $\mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1}$ and conversely each 1-cocyle with values in this factor group is induced by a vector system. The set of all these 1-cocycles forms a group under addition denoted by $C^1(G, \mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1})$.

(ii) A vector system $v_t : G \to \mathbb{R}^{n\times 1} : g \mapsto t - gt$ for some fixed $t \in \mathbb{R}^{n\times 1}$ is called an *inner vector system* and the induced 1-cocyle $\overline{v_t}$ a *coboundary*. These form subgroups $I(G, \mathbb{R}^{n\times 1})$ of $V(G, \mathbb{R}^{n\times 1})$ and $B^1(G, \mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1})$ of $C^1(G, \mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1})$, respectively. The factor group $H^1(G, \mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1}) := C^1(G, \mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1})/B^1(G, \mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1})$ is called the *first cohomology group* of G with values in $\mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1}$ or, in abuse of notation [since it is isomorphic to $H^2(G, \mathbb{Z}^{n\times 1})$], the *group of extensions* of $\mathbb{Z}^{n\times 1}$ by G. $H^1(G, \mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1})$ is isomorphic to the factor group $V(G, \mathbb{R}^{n\times 1})/I(G, \mathbb{R}^{n\times 1})$.

(iii) For any vector system $v \in V(G, \mathbb{R}^{n\times 1})$ call

$$R(G, v) := \left\{ \begin{pmatrix} g & v(g)+t \\ 0 & 1 \end{pmatrix} | g \in G, t \in \mathbb{Z}^{n\times 1} \right\}$$

the *space group associated with G and v*.

Clearly, $R(G, v)$ is a space group with translation subgroup $T(R(G, v))$ consisting of all translations by vectors in $\mathbb{Z}^{n\times 1}$. For $v_1, v_2 \in V(G, \mathbb{R}^{n\times 1})$, the two space groups $R(G, v_1)$ and $R(G, v_2)$ are equal if and only if $\overline{v_1} = \overline{v_2}$, they are conjugate by a translation if and only if v_1 and v_2 induce the same element in $H^1(G, \mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1})$. From the practical point of view, it is important to note that a vector system is essentially determinded by its values on a generating set of the point group because they determine the resulting space group uniquely. For instance, the group

$$G := \left\langle g_1 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, g_2 := \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$$

allows a vector system v with

$$v(g_1) = \begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix}$$

and

† Crystallographers might prefer the term 'column system' but the name vector system has a long mathematical tradition.

$$v(g_2) = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Then,

$$R(G,v) = \left\{ \left(\begin{array}{cc|c} 1 & 0 & a \\ 0 & 1 & b \\ \hline 0 & 0 & 1 \end{array}\right), \left(\begin{array}{cc|c} 1 & 0 & \frac{1}{2}+a \\ 0 & 1 & b \\ \hline 0 & 0 & 1 \end{array}\right), \left(\begin{array}{cc|c} -1 & 0 & a \\ 0 & -1 & b \\ \hline 0 & 0 & 1 \end{array}\right), \left(\begin{array}{cc|c} -1 & 0 & \frac{1}{2}+a \\ 0 & 1 & b \\ \hline 0 & 0 & 1 \end{array}\right) \middle| a, b \in \mathbb{Z} \right\}.$$

Note that whereas v is not inner, $2v$ is an inner vector system.

By the Bieberbach theorems, the translation subgroup is not only a normal but a characteristic subgroup of a space group, and therefore two space groups are isomorphic if and only if they are conjugate in the affine group $\mathrm{Aff}_n(\mathbb{R})$. This immediately translates into the following remark.

Remark 6. (Zassenhaus, 1948.) Let $G \leq GL_n(\mathbb{Z})$ be a finite unimodular group and denote its normalizer in $GL_n(\mathbb{Z})$ by $N(G)$.

(i) $N(G)$ acts on the group $V(G, \mathbb{R}^{n\times 1})$ of all vector systems of G, where $n \in N(G)$ maps $v \in V(G, \mathbb{R}^{n\times 1})$ to ${}^n v$ defined by ${}^n v : g \mapsto nv(n^{-1}gn)$. Since this action respects $I(G, \mathbb{R}^{n\times 1})$, it induces an action on $H^1(G, \mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1})$.

(ii) Two $v_1, v_2 \in V(G, \mathbb{R}^{n\times 1})$ gives rise to two isomorphic space groups $R(G, v_1)$ and $R(G, v_2)$ if and only if v_1 and v_2 represent elements in $H^1(G, \mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1})$, which lie in the same orbit under the action of $N(G)$.

CARAT also provides facilities to transform a subgroup of $R(G, v)$ of finite index into the form $R(H, w)$ for a suitable finite unimodular group H and a suitable vector system w for H. (Actually all the vector systems *CARAT* provides take already values in $|G|^{-1}\mathbb{Z}^{n\times 1}/\mathbb{Z}^{n\times 1}$ rather than $\mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1}$.) It can test two space groups $R(G, v)$ and $R(H, w)$ for isomorphism, $\mathbb{Z}$-equivalence, $\mathbb{Q}$-equivalence, Bravais equivalence and it can determine the family symbols.

3. Basic tasks

3.1. *Types of problems and general philosophy*

This chapter will enumerate the tasks *CARAT* is designed to deal with. It will also give the user an idea what is involved and what is easy, difficult or time consuming. The actual algorithms will be discussed in §4. Not everything that is discussed here is realized already; where it is not, we say so. *CARAT* is designed to have as little overlap as possible with existing group-theoretical packages like *GAP* or *MAGMA* (*cf.* Schönert, 1993; Bosma & Cannon, 1996) (for information on how to obtain these packages, refer to the Internet sites given in the reference list) on the one hand, but more importantly it should solve most if not all common tasks in the realm of crystallographic groups without accessing other systems. Moreover, the user should not be forced to learn a new language but only be able to work in a Unix environment: the user keeps his own files, which are basically of two types. These files can be used as input for the programs of the package. The programs produce output files in such a way that they are either already in one of the prescribed input formats or can easily be turned into these formats.

There are two main types of problems *CARAT* is designed to deal with and a further type for which some development is in progress or access to other packages becomes necessary: enumeration; recognition and comparison; general investigation.

Some enumerative tasks have been solved within *CARAT* by providing a list of representatives, *i.e.* *CARAT* has tables that can be accessed *via* a program call. Obviously, a list of all affine classes or even $\mathbb{Z}$-classes is out of the question because it is too long. But *CARAT* can provide key lists from which by specification of suitable parameters it might be able to use its programs to compute representatives of the groups in the specified realm. The key lists that are already available are the following: Bravais groups up to degree 6, inclusions of Bravais manifolds and Bravais groups. The key lists that one could further wish to have are: $\mathbb{Q}$-classes up to degree 6; information about Bravais minimal subgroups of Bravais groups. All other information should be computable from these with the programs in *CARAT*. One should however be aware that enumeration gets less and less interesting the more classes there are in the specified realm. It can also become physically impossible, *e.g.* there are $\mathbb{Z}$-classes of space groups of degree 6 splitting up into more than 1 million affine classes. In the case of affine classes in a $\mathbb{Z}$-class, the program can still give the number of classes without enumerating them. Here is a list of enumerative tasks that will be commented upon below:

(*a*) splitting a $\mathbb{Z}$-class in affine classes;
(*b*) splitting a $\mathbb{Q}$-class into $\mathbb{Z}$-classes;
(*c*) splitting a Bravais flock into $\mathbb{Z}$-classes;
(*d*) splitting a crystal family into a Bravais flocks;
(*e*) splitting a crystal family into $\mathbb{Q}$-classes;
(*f*) enumerating inclusions between Bravais groups.

In case one has a crystallographic group and wants to compare it with another one or find an equivalent one in a list that *CARAT* supplies or the user has made himself, various programs are available for computing relevant invariants or performing comparisons such as testing

affine, $\mathbb{Z}$-, $\mathbb{Q}$- or Bravais equivalence. In part, these programs are also used for the enumerative tasks above. An important aspect of this is that the various equivalence relations do a lot towards a parametrization of the groups, in the sense that each group gets a name that is as meaningful as possible, *i.e.* enables the user to read off the family, the Bravais flock *etc*. to which the group belongs. Beyond this there is the following observation: Say *CARAT* has a program to enumerate representatives of certain classes starting out for the certain data it has stored. For the user, it is as meaningful to speak of the nth representative as it would be for him to talk about the nth group in list k of a certain book, because each time the program generates these representatives from the same data by the same algorithm its nth object will be the same as before. Here is a list of the tasks concerning recognition and comparison:

(a) deciding affine equialence;
(b) deciding $\mathbb{Z}$-equivalence;
(c) deciding $\mathbb{Q}$-equivalence;
(d) deciding Bravais equivalence;
(e) computing the family symbol.

Coming to the last point, which is rather vague at this stage, one could think of computing interesting geometric or group-theoretical invariants of the object under inspection. For some of these, one will have to use other packages; many programs are under development like computing fundamental domains, computing orbits on certain objects, finding subgroup relations *etc.*

3.2. *Enumeration*

3.2.1. *Splitting a $\mathbb{Z}$-class into affine classes*. The basic structure behind the problem is discussed in Definition 6 and Remark 6: Suppose the $\mathbb{Z}$-class is given by a representative $G \leq GL_n(\mathbb{Z})$. One needs to compute the orbits of the normalizer $N_{GL_n(\mathbb{Z})}(G)$ on the cohomology group $H^1(G, \mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1})$ by the Zassenhaus algorithm. One is given a set of vector systems $v_i \in V(G, \mathbb{R}^{n\times 1})$ such that the representatives of the isomorphism classes are given by the $R(G, v_i)$. The first vector system v_1 is the 0-vector system representing the symmorphic (or split) space group.

If G is given by generating matrices, one needs a presentation of G in terms of these generators, *i.e.* defining relations, to compute $H^1(G, \mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1})$. There are two programs available to compute such a presentation, one for soluble groups G and one for arbitrary groups G. The later one computes a fundamental domain and is then based on Poincaré's method of neighbouring transformations for which one gets defining relators by walking around the edges of the fundamental domain of co-dimension two. The complexity of this procedure depends on the order of G. Once the presentation is available, the cohomology group is quickly computed. There are cases where one wants to do this first before one computes the normalizer, because $H^1(G, \mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1})$ might be of order 1 or 2, in which case the normalizer has the same number of orbits. In all other cases, one usually needs generators for the normalizer $N_{GL_n(\mathbb{Z})}(G)$, which are computed by Opgenorth's algorithm described in §4 (Opgenorth, 1997). The cost of this mainly depends on the dimension of the space $\mathcal{F}(G)$ of forms of G, on the index of $N_{GL_n(\mathbb{Z})}(G)$ in $N_{GL_n(\mathbb{Z})}(B(G))$, and to a lesser extent on the orders of G and $B(G)$, in case $G \neq B(G)$. This is so since the normalizer of the Bravais group $B(G)$ is computed first, *cf*. Remark 5. Again, once the normalizer is given, the computation of the orbit representatives in $H^1(G, \mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1})$ does not take too long, unless the cohomology group is very big [like in the case of the group of all diagonal matrices in $GL_6(\mathbb{Z})$, where the cohomology group has order 2^{30} falling into 1 540 944 orbits]. In such a case, one can use the same program to compute the number of orbits first. This is based on the Burnside–Cauchy lemma, that the average number of fixed points of the (acting) group elements is equal to the number of orbits.

3.2.2. *Splitting a $\mathbb{Q}$-class into $\mathbb{Z}$-classes*. The method proceeds in two steps:

The basic structure behind this problem was described in Remark 2: Say a finite subgroup G of $GL_n(\mathbb{Z})$ [or $GL_n(\mathbb{Q})$ for that matter] is given. Then one needs to compute a set of representatives of the orbits in the $\mathcal{F}(G) := \mathrm{Fix}_G(\mathcal{Z}_n)$ of G-invariant (full) lattice in $\mathbb{Q}^{n\times 1}$ under the action of the rational normalizer $N_{GL_n(\mathbb{Q})}(G)$. This might be a theoretically satisfying description of the problem, but its algorithmic solution is more involved, since both $\mathcal{Z}(G)$ and $N_{GL_n(\mathbb{Q})}(G)$ are too complicated to be 'computed' first and to get the orbits afterwards. Certainly, one needs a means to compute lattices, which is provided by the 'centering' algorithm described in §4 and is not too expensive (if one knows what one is looking for). Secondly, one needs a means to decide whether two lattices give rise to $\mathbb{Z}$-equivalent groups. This is also available by a slight extension of the method computing the integral normalizer and will be discussed below and in the next section. In the method described below, which is based on Remark 3, the integral normalizers are also needed. Finally, one needs a method to decide when one has found enough lattices. To outline the method, denote the subgroup of $GL_n(\mathbb{Z})$ obtained from the action of G on some lattice $L \in \mathcal{Z}(G)$ with respect to some chosen $\mathbb{Z}$-basis of L by $G(L)$.

Step 1: Compute representatives of the $N_{GL_n(\mathbb{Q})}(G)$ orbits on $\mathcal{Z}^{\mathrm{h.d.}}(G)$ as follows:

start with $L_1 = \oplus_{i=1}^{s} e_i\mathbb{Z}^{n\times 1}$ (*cf*. Remark 3);

compute generators for the normalizer of $G(L_1)$ in $GL_n(\mathbb{Z})$;

compute the maximal G-sublattices of L_1 in $\mathcal{Z}^{\mathrm{h.d.}}(G)$ which are of p-power index in L_1, where p is a prime number dividing the order $|G|$ of G;

compute orbit representatives of the $N_{GL_n(\mathbb{Z})}(G(L_1))$ orbits on the set of these maximal sublattices of L_1;

check which of the representatives L give rise to a group $G(L)$ which is $\mathbb{Z}$-equivalent to an earlier obtained $G(L_i)$, discard these, add the L's giving rise to new $G(L)$'s to the list of lattices L_i to be treated like L_1.

Step 2: For each homogeneously decomposable lattice $L_i \in \mathcal{Z}^{\text{h.d.}}(G)$ obtained in step 1 proceed as follows:

compute the (finite) set $\theta^{-1}(L_i)$ of G-sublattices X of L_i satisfying $\oplus_{j=1}^{s} e_i X = L_i$, *cf.* Remark 3. This computation is done 'layer by layer' starting with the maximal sublattices of L_i followed by the second maximal ones *etc.*;

compute a set R_i of representatives of the $N_{GL_n(\mathbb{Z})}(G(L_i))$ orbits on the set $\theta^{-1}(L_i)$ of sublattices of L_i previously determined. The $G(L)$ with $L \in \cup R_i$ form a set of representatives of the $\mathbb{Z}$-classes in the $\mathbb{Q}$-class of G. [Note that from Remark 3 the normalizers of the $G(L)$ can be obtained as the stabilizers of the $N_{GL_n(\mathbb{Z})}(G(L_i))$ from step 1 of the L's in R_i.]

This method works for all cases up to degree 6. Its complexity depends on the dimension of $\mathcal{F}(G)$ (for the normalizer computations) and on the class number $|N_G L_n(\mathbb{Q})(G)\backslash\mathcal{Z}(G)|$. For instance, the $\mathbb{Q}$-class of the group

$$\langle \text{diag}(1,-1,1,-1,1,1), \text{diag}(1,-1,-1,1,-1,1), \text{diag}(1,1,-1,1,1,-1)\rangle$$

of order 8 splits into 325 $\mathbb{Z}$-classes. (These $\mathbb{Z}$-classes split into 21 621 affine classes.)

3.2.3. *Splitting a Bravais flock into $\mathbb{Z}$-classes*. Here one wants to enumerate all subgroups G of a Bravais group B with $B(G) = B$ up to $\mathbb{Z}$-equivalence. Note that two such groups G are $\mathbb{Z}$-equivalent if and only if they are conjugate under $N_{GL_n(\mathbb{Z})}(B)$. Since the subgroups G with $B(G) = B$ only form a small fraction of all subgroups of B, we propose to solve this problem by listing the Bravais minimal subgroups G of B up to $N_{GL_n(\mathbb{Z})}(B)$ conjugacy in a table and to compute the others from this table. Of course, $G \leq B$ is called Bravais minimal if $B(G) = B$ and $B(H) \neq B$ for all proper subgroups $H < G$ of G. Note that if G is Bravais minimal and H is rationally equivalent to G then H is also Bravais minimal [in its Bravais group $B(H)$, which need not be $\mathbb{Q}$-equivalent to $B(G)$]. Therefore, the tables of the Bravais minimal subgroups of the Bravais groups, which at the moment are not yet realized in *CARAT*, could best be established as a side project of computing tables of the $\mathbb{Q}$-classes, *cf.* §3.2.5 below. In the description of the method how to find the $\mathbb{Z}$-classes in a Bravais flock, we pretend that a list for each Bravais group B to be investigated, a list of the permutation representations on the cosets of the Bravais minimal subgroups [up to $N_{GL_n(\mathbb{Z})}(B)$ action], is available. Then one could proceed in two steps as follows:

Step 1: Find the subgroups G of B with $B(G) = B$ up to conjugacy in B:

Starting with the permutation representations of B on the cosets of the Bravais minimal subgroups G of B, compute the permutation representations of B on the cosets of any intermediate group H with $G \leq H \leq B$. Computing the permutation representations on the minimal blocks of any permutation representation gives Example 1(vi). B-conjugacy is tested by using the well known fact that two subgroups H of B are conjugate in B if and only if the permutation representations of B on the cosets of the subgroups H are equivalent. In particular, since the actions will be described as permutations on some fixed generating set of B, one has equivalence if the degrees are equal and the stabilizer of a point in the first action also stabilizes a point in the second action. (Note that the desired subgroups are given as these stabilizers.)

Step 2: decide conjugacy in $N_{GL_n(\mathbb{Z})}(B)$:

Here we rely on the decision procedures for $\mathbb{Z}$-equivalence to be described below (*cf.* §3.3.2).

Of course, in practice one will mix the two steps to minimize the number of redundant groups one computes. The costs of the procedure depend to some extent on the maximal index of the Bravais minimal subgroups of B in B and on the number of $\mathbb{Z}$-classes in the Bravais flock.

3.2.4. *Splitting a crystal family into Bravais flocks*. Computing all Bravais groups in a crystal family is usually complex and time consuming and the result does not take too much space to formulate. Therefore, this problem is solved in *CARAT* by tables that are based on existing classifications of Bravais groups in the literature (up to degree 6) (*cf.* Brown *et al.*, 1977; Plesken, 1981; Plesken & Hanrath, 1984). Recall from Definition 5 that each crystal family can be addressed by a symbol. The most readily available Bravais groups B in a given crystal family are the homogeneously decomposable ones, *i.e.* those for which the natural lattice $L := \mathbb{Z}^{n\times 1}$ splits into a direct sum $L = \oplus_{i=1}^{s} e_i L$, where $e_1, \ldots, e_s$ are the primitive idempotents of the center of the enveloping algebra $\overline{\mathbb{Q}B}$, *cf.* Remark 3. (Of course, $s = 1$ is admitted.) Concerning their group-theoretic structure, homogeneously decomposable Bravais groups are direct products of Bravais groups of lower degree, in case the number s of homogeneous components is bigger than 1. More interestingly, any Bravais group B can be assigned a homogeneously decomposable Bravais group in the same crystal family: Let $L := \mathbb{Z}^{n\times 1}$ be the natural lattice of B and let $L' := \oplus_{i=1}^{s} L$, where $e_1, \ldots, e_s$ are the primitive idempotents of the center of the enveloping algebra $\overline{\mathbb{Q}B}$ as above. Clearly, B acts on L', *i.e.* $L' \in \mathcal{Z}(B)$. Let $B(L')$ be the subgroup of $GL_n(\mathbb{Z})$ obtained from the action of B on L' with respect to some lattice basis of L'. Then the Bravais group $B(B(L'))$ of $B(L')$ is the associated homogeneously decomposable

Bravais group of B, well defined up to $\mathbb{Z}$-equivalence (*cf.* Plesken, 1981; Plesken & Hanrath, 1984).

When one specifies a symbol for a crystal family, *CARAT* will first answer with the number of $\mathbb{Z}$-classes of homogeneously decomposable Bravais groups in this family and the number of $\mathbb{Z}$-classes of Bravais groups associated with each of the homogeneously decomposable Bravais group. If one specifies a Bravais group, one gets generators, a basis of the form space and generators for the normalizer in $GL_n(\mathbb{Z})$. If the Bravais group is homogeneously decomposable, one also gets bases for the lattices of the other Bravais groups which are associated with the specified homogeneously decomposable Bravais group.

3.2.5. *Splitting a crystal family into* $\mathbb{Q}$*-classes*. Computing representatives of the $\mathbb{Q}$-classes in a crystal family is not necessarily a problem that can be solved quickly, though there are powerful general-purpose subgroup routines in packages like *GAP* and *MAGMA* available. But then $\mathbb{Q}$-equivalence has to be tested afterwards. Therefore, we suggest tabulating representatives of the $\mathbb{Q}$-classes for each crystal family up to degree 6 (which might be just about feasible). These tables have not yet been computed. For the $\mathbb{Q}$-equivalence tests, we refer to §3.3.3.

3.2.6. *Enumerating inclusions between Bravais groups*. It is remarkable to note that there are only finitely many pairs (B_1, B_2) of Bravais groups with $B_1 \leq B_2$ up to conjugation under $GL_n(\mathbb{Z})$. This is an immediate consequence of the Jordan–Zassenhaus theorem. To enumerate representatives is more difficult. Since the computations are time consuming, *CARAT* again goes for tables. These tables can answer the following questions for a given Bravais group B:

How many $N_{GL_n(\mathbb{Z})}(B)$-conjugacy classes of Bravais groups H with $H \leq B$ are there?

How many Bravais groups H with $H \leq B$ are there?

How many $N_{GL_n(\mathbb{Z})}(B)$-conjugacy classes of Bravais groups H with $B \leq H$ are there?

List representatives of the $N_{GL_n(\mathbb{Z})}(B)$-conjugacy classes of Bravais groups H with $H \leq B$.

List representatives of the $N_{GL_n(\mathbb{Z})}(B)$-conjugacy classes of Bravais groups H with $B \leq H$.

Since the program only runs through tables one gets answers reasonably quickly.

3.3. *Recognition and comparison*

3.3.1. *Deciding affine equivalence*. The basic structure was explained in §3.2.1 and the basic idea is that of the standard representative: We may assume that the groups are already in the form that they yield the same point group G on the same generators and that generators for the normalizer $N_{GL_n(\mathbb{Z})}(G)$ are given. The elements of $H^1(G, \mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1})$ are given some lexicographic ordering. Then one can compute for the vector systems of both groups the lexicographic first element in their orbits under the normalizer $N_{GL_n(\mathbb{Z})}(G)$ acting on $H^1(G, \mathbb{R}^{n\times 1}/\mathbb{Z}^{n\times 1})$.

There are some problems with first transforming the groups to the desired shape such that the comparison can be made. For these, one can usually employ the $\mathbb{Z}$-equivalence routine in §3.3.2. There is one situation when more work has to be done: if a space group R is given as a subgroup of another space group. In this case, one first has to find a presentation of the group $\overline{R}$ of linear parts of R on the linear parts of the generating set by which R is given. Inserting the generators of R in the defining relators yields a generating set of the translation subgroup $T(R)$ of R as modulus for $\overline{R}$. This generating set is then turned into a $\mathbb{Z}$-basis for $T(R)$ from where it is a routine application of the $\mathbb{Z}$-equivalence routine to transform R into the desired shape.

3.3.2. *Deciding* $\mathbb{Z}$*-equivalence*. We may assume that the two finite unimodular groups to be checked for $\mathbb{Z}$-equivalence are already checked for Bravais equivalence, *cf.* §3.3.4, and are subgroups of the same Bravais group B. Then they are $\mathbb{Z}$-equivalent if and only if they are conjugate under the normalizer $N_{GL_n(\mathbb{Z})}(B)$, which can be checked by an orbit calculation since the orbit is finite.

3.3.3. *Deciding* $\mathbb{Q}$*-equivalence*. Suppose two finite subgroups G, H of $GL_n(\mathbb{Q})$ are given by generators. The first problem is to find generators for H that might correspond to the given generators of G under the conjugation by some matrix of $GL_n(\mathbb{Q})$. The basic idea, which is not yet implemented in the present version of *CARAT*, is to view the enveloping $\mathbb{Z}$-order $\overline{\mathbb{Z}G} := \left\{ \sum a_g g \in \mathbb{Q}^{n\times n} | a_g \in \mathbb{Z} \text{ for all } g \in G \right\}$ as a $\mathbb{Z}$-lattice equipped with bilinear forms induced from traces and with other structures resulting from the origin of the lattice from a group. As a result, one has to check only very few isometries ι from $\overline{\mathbb{Z}G}$ to $\overline{\mathbb{Z}H}$ respecting all these structures, whether they are induced by a rational conjugation. This checking essentially amounts to solving the $\mathbb{Q}$-linear system of equations $Xg = \iota(g)X$, where g runs through the generating set of G and $X \in \mathbb{Q}^{n\times n}$ is unknown. Details are given in §4.

At the moment, one is forced to check $\mathbb{Q}$-equivalence *via* splitting into $\mathbb{Z}$-classes and checking $\mathbb{Z}$-equivalence.

3.3.4. *Deciding Bravais equivalence*. We may assume that the two groups G and H to be compared for Bravais equivalence lie already in the same crystal family, *cf.* §3.3.5. The next move is to compute some rather cheap invariants, *e.g.* elementary divisors for a trace pairing of $\mathcal{F}(G) \cap \mathbb{Z}^{n\times n}$ with $\mathcal{F}(G^{\mathrm{tr}}) \cap \mathbb{Z}^{n\times n}$. If all these invariants agree, a more serious computation is performed, which computes the G-perfect forms in $\mathcal{F}(G)$ and the corresponding Voronoi domains in $\mathcal{F}(G^{\mathrm{tr}})$, *cf.* Definition 8, from which one can easily compute generators for the normalizer $N_{GL_n(\mathbb{Z})}(G)$. Comparing all perfect forms for G with one perfect form for H yields the desired equivalence test and transforms H under a unimodular matrix into $B(G)$ in case both groups lie in the same

Bravais flock. The complexity of the method mainly depends on the dimension of $\mathcal{F}(G)$. Details are given in §4.

3.3.5. *Computing the family symbol.* The basic idea is to compute the homogeneously decomposable Bravais group associated with the given finite unimodular group G and compare it with the list of homogeneously decomposable Bravais groups. The main step is to compute the primitive idempotents $e_1, \ldots, e_s$ of the center of the enveloping algebra $\overline{\mathbb{Q}G}$, *cf.* Remark 3. This amounts to a standard problem of linear algebra, namely to factorize the minimum polynomial of one or some elements in this center. The present implementation of *CARAT* makes essential use of the assumption that the degree of the groups is at most 6.

4. Main algorithms

4.1. *The three basic algorithms*

Of course, there are a couple of standard group-theoretical algorithms, like computing an orbit of a group given by a finite generating set acting on some finite set or computing generators for a stabilizer or computing a $\mathbb{Z}$-basis of a lattice given by some generating set *etc.* These we will not discuss although the performance of the more specific algorithms will also depend on the quality of the implementation of these frequently used procedures. In this section, we want to comment on the three working horses of the whole package, namely on the lattice automorphism algorithm, which is closely connected with the lattice isometry algorithms, on the sublattice (or centering) algorithm, and finally on the more classical Zassenhaus algorithm to compute H^1. It will be the lattice automorphism algorithm that will be the essential ingredient from the algorithmic side for Opgenorth's normalizer algorithm to be described later on. Fig. 1 shows which (major) algorithm makes use of which other (major) algorithm.

Most interrelations in the diagram have already been explained in §3. The most classical part of the diagram is the right-hand side: The two boxes are conventially taken together and called the Zassenhaus algorithm. In Zassenhaus (1948), everything is explained in detail, *cf.* also Holt & Plesken (1989) for a more recent account. We do not comment here on the algorithms we use to get a presentation for the point group, which is needed for the H^1-computation.

Secondly, a rough description of the sublattices (or centering) algorithm might be in place. It dates back to Plesken (1974) and has been used in the determination of maximal finite subgroups of $GL_n(\mathbb{Z})$ for $n \leq 10$, *cf.* Plesken & Pohst (1977, 1980) and Souvignier (1994), of the Bravais groups up to degree 6, *cf.* Plesken (1981) and Plesken & Hanrath (1984), and of the maximal finite subgroups of $GL_n(\mathbb{Q})$ for $n \leq 31$, *cf.* Plesken (1991), Nebe & Plesken (1995) and Nebe (1995, 1996*a*,*b*). The algorithm starts with a finite unimodular group $G \leq GL_n(\mathbb{Z})$ and starts to compute the G-sublattices of the natural G-lattice $L_0 = \mathbb{Z}^{n\times 1}$ layer by layer after some preprocessing. In the preprocessing phase, the action of G on L is taken modulo a prime p. (For the purposes of this paper, p divides $|G|$.) The irreducible consituents of the resulting representation $G \to GL_n(\mathbb{Z}/p\mathbb{Z})$ are then computed or, in the language of linear actions, the G-composition factors of L_0/pL_0 are determined. Note that any G-sublattice of finite index of L_0 would yield isomorphic composition factors.

After the preprocessing, the algorithm starts computing sublattices. It keeps a list of certain (to be explained below) lattices, which usually starts with L_0. For each G-lattice L in this list, it computes the maximal G-sublattices X of L with index $|L : X|$ dividing $|G|^l$ for some $l \in \mathbb{N}$ as follows: Each such X is the kernel of a surjective G-module homomorphism (additive G-map) $\varphi : L \to S$, where S is one of the composition factors computed in the preprocessing phase (*i.e.* a simple $\mathbb{Z}/p\mathbb{Z}G$-module). Note that computing such a homomorphism φ and computing the kernel of φ both amount to solving linear equations over the residue class field $\mathbb{Z}/p\mathbb{Z}$. In the first case, these equations are $\overline{\varphi} : \Delta_L(g) = \Delta_S(g)\overline{\varphi}$ with g running through a set of generators of G. Here, $\overline{\varphi}$ represents the matrix of the (unknown) φ and Δ_L is the matrix representation for the action of G on L/pL and Δ_S for the action on S. That the computation of the kernel of φ amounts to solving linear equations is clear. However, to get a good lattice basis for the kernel, one usually invokes the *LLL* algorithm or some other reduction routine. (This is essential to keep numbers small.)

A word about which lattices are kept and which are discarded ought to be said. This greatly depends on the circumstances. At the minimum, one checks whether a

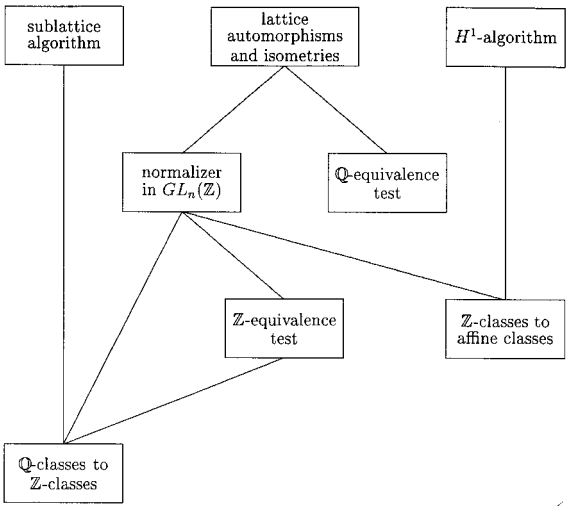

Fig. 1. Diagram to show main algorithms.

newly found lattice is in fact identical with an earlier find. One also discards multiples of earlier found lattices. But in the context of splitting $\mathbb{Q}$-classes into $\mathbb{Z}$-classes, two other conditions also play a role which were described in §3.2.2, and which can be formulated in terms of the primitive idempotents of the centre of $\overline{\mathbb{Q}G}$.

The third basic algorithm computes lattice automorphism and isometries. The algorithm was first designed by Plesken & Pohst (1985) and much refined and improved by Plesken & Souvignier (1997). The present implementation by B. Souvignier is very powerful indeed, *e.g.* it computes generators for the automorphism group of the 24-dimensional Leech lattice in less than 20 min [the lattice has 196 560 vectors of shortest length and the automorphism group, which is the covering group of the Conway group Co has order $2^{22}3^9 5^4 7^2 11 \times 13 \times 23$, *cf.* Conway & Sloane (1988)]. The program has been used for the classification of the maximal finite subgroups of $GL_n(\mathbb{Q})$ for $n \leq 31$, *cf.* above and various other projects.

We first describe the automorphism version. It starts from a set of integral matrices $F_1, F_2, \ldots, F_k \in \mathbb{Z}^{n\times n}$, where F_1 has to be symmetric and positive definite. It then computes generators for the strict Bravais group $B := B_I(\{F_1, \ldots, F_k\}) := \{g \in GL_n(\mathbb{Z}) | g^{\mathrm{tr}} F_i g = F_i \quad \text{for } i = 1, \ldots, k\}$ as follows:

Let m be the maximum of the diagonal entries of F_1. Then the finite set $C := \{x \in \mathbb{Z}^{n\times 1} | x^{\mathrm{tr}} F_1 x \leq m\}$ is computed. Note that $g \in B$ implies $ge_i \in C$, where $e_1, \ldots, e_n$ is the standard basis of $\mathbb{Z}^{n\times 1}$, *i.e.* the candidates for the columns of g lie in C. Now there follows a rather sophisticated backtrack search for n-tuples $g = (c_1, \ldots, c_n) \in C^n \subset \mathbb{Z}^{n\times n}$ satisfying $g^{\mathrm{tr}} F_i g = F_i$ for $i = 1, \ldots, k$. For an individual g, the search tries to complete k-tuples already have the correct scalar products to n-tuples in a systematic way, and that tries to predict as early as possible whether or not such a completion exists. The whole search is set up in such a way that one ends up with rather few generators of B.

For the isometry version, one starts with two sets of integral matrices $F_1, F_2, \ldots, F_k \in \mathbb{Z}^{n\times n}$ and $F_1', F_2', \ldots, F_k' \in \mathbb{Z}^{n\times n}$, where F_1 and F_1' have to be symmetric and positive definite. It then decides whether there exists a $g \in GL_n(\mathbb{Z})$ with $g^{\mathrm{tr}} F_i g = F_i'$ for $i = 1, \ldots, k$. In case of existence, such a g is given. The algorithm proceeds by first computing generators for $B_i(\{F_1, \ldots, F_k\})$ and uses them to shorten the backtrack search for g, which is similar to the automorphism version.

From this very rough description, one can see that it is essential to have the set C as small as possible, *i.e.* to keep the maximum m of the diagonal entries of F_1 as small as possible. This can usually be achieved by finding some sort of reduced basis for $\mathbb{Z}^{n\times 1}$ with respect to the scalar product induced by F_1. The algorithm can be used to compute Bravais groups, and at least its idea and basic ingredients can be used for testing $\mathbb{Q}$-equivalence, as we shall sketch next. In §4.2, we shall see how it is used for computing normalizers and test $\mathbb{Z}$-equivalence.

An outline on how one can decide whether two finite subgroups G, H of $GL_n(\mathbb{Q})$ are rationally equivalent was given in §3.3.3. In the light of the isometry routine described above, this can now be better understood: One has at least two scalar products on the enveloping $\mathbb{Z}$-order $\overline{\mathbb{Z}G}$, namely

$$\phi : \overline{\mathbb{Z}G} \times \overline{\mathbb{Z}G} \to \mathbb{Z} : \left(\sum_{g\in G} a_g g, \sum_{h\in G} b_h h \right) \mapsto \sum_{g,h} a_g b_{h^{-1}} \mathrm{tr}(gh^{-1})$$

and

$$\psi : \overline{\mathbb{Z}G} \times \overline{\mathbb{Z}G} \to \mathbb{Z} : \left(\sum_{g\in G} a_g g, \sum_{h\in G} b_h h \right) \mapsto \sum_{g,h} a_g b_h \mathrm{tr}(gh).$$

Now, there are still a few more simplifications: The set C in the automorphism program can be chosen to be G itself or G and H for the isometry program. Furthermore, one knows that I_n must be mapped onto I_n and minimal polynomials and orders of elements have to be preserved. Sometimes, one can also use idempotents of the center of the rational enveloping algebra to form more scalar products to be preserved. How to proceed from here was discussed in §3.

4.2. *The normalizer algorithm*

The algorithm is due to Opgenorth (1997), which is his second normalizer algorithm, *cf.* Opgenorth (1996) for the first one. It was explained in §§3.2.2 and 3.3.2 and Remark 5 that the essential part of the computation of the normalizer $N_{GL_n(\mathbb{Z})}(G)$ of a finite unimodular group G of degree n consists in computing the normalizer of its Bravais group $B(G)$. Also, testing $\mathbb{Z}$-equivalence reduces essentially to this task, namely to checking Bravais equivalence, *i.e.* $\mathbb{Z}$-equivalence for the Bravais groups. Therefore, we shall assume now that $G = B(G)$ is a Bravais group and also for the other group H, which has to be checked to be $\mathbb{Z}$-equivalent to G, we assume $H = B(H)$. To understand the basic idea behind Opgenorth's algorithms, assume for a moment that both G and H have a one-dimensional space of invariant forms. Then each of these spaces has a canonical basis: It consists of the unique integral positive-definite form $F \in \mathcal{F}(G)$, respectively, in $\mathcal{F}(H)$, where the greatest common divisor of entries is 1. Hence the normalizer fixes this form, *i.e.* is equal to the Bravais group, and for the $\mathbb{Z}$-equivalence test this means that one only has to compute an isometry. In general, the form space will not have such special form, not even a unique orbit of certain forms under the normalizer, which are in some sense special. But the G-perfect forms to be defined

and used below come close to this desirable property: There are only finitely many up to normalizer action in the form space, *cf.* Jaquet-Chiffelle (1995) and Opgenorth (1996, 1997). We now need some preparation from the classical theory of perfect forms and the Voronoi algorithm, *cf.* Martinet (1996).

Definition 7. Let $F \in \mathbb{R}^{n\times n}_{\text{sym},\,>0}$.

(i) $m(F) := \min\{x^{\text{tr}}Fx | 0 \neq x \in \mathbb{Z}^{n\times 1}\}$ is called the *minimum* of F.

(ii) $M_v(F) := \{x \in \mathbb{Z}^{n\times 1} | x^{\text{tr}}Fx = m(F)\}$ is called the set of *minimum vectors* of F.

(iii) $M_f(F) := \{xx^{\text{tr}} | x \in M_v(F)\}$ is called the *associated set of forms* of $M_v(F)$.

(iv) $V(F) := \left\{ \sum_{f\in M_f(F)} a_f f | a_f \in \mathbb{R}, a_f \geq 0 \right\} \cap \mathbb{R}^{n\times n}_{\text{sym},\,>0}$ is called the *Voronoi domain* of F.

(v) F is called *perfect* if $V(F)$ has non-empty interior in $\mathbb{R}^{n\times n}_{\text{sym}}$ or, equivalently, if $M_f(F)$ contains $n(n+1)/2$ linearly independent matrices.

Though it is not relevant in our context, we mention Voronoi's well known theorem from the geometry of numbers that F gives rise to a local maximum for the density of lattice sphere packings if and only if F is perfect and eutactic, *cf.* Martinet (1996). What is more relevant for us is the elementary fact that the action of $GL_n(\mathbb{Z})$ on $\mathbb{R}^{n\times n}_{\text{sym},\,>0}$ described in Example 1(ii) transforms perfect forms in perfect forms with the same minimum. Moreover, Voronoi's theorem says that the number of orbits on the perfect forms of degree n with minimum 1, say, is finite. Here is Voronoi's idea to construct a first perfect form from a given form:

Remark 7.

(i) $\text{tr} : \mathbb{R}^{n\times n}_{\text{sym}} \times \mathbb{R}^{n\times n}_{\text{sym}} \to \mathbb{R} : (F_1, F_2) \mapsto \text{trace}(F_1 \cdot F_2)$ is a nondegenerate symmetric bilinear form on $\mathbb{R}^{n\times n}_{\text{sym}}$ satisfying $\text{tr}(F, xx^{\text{tr}}) = x^{\text{tr}}Fx$ for all $F \in \mathbb{R}^{n\times n}_{\text{sym}}$ and all $x \in \mathbb{R}^{n\times 1}$, in particular for all $F \in \mathbb{R}^{n\times n}_{\text{sym},\,>0}$ and all $x \in M_v(F)$.

(ii) If $F \in \mathbb{R}^{n\times n}_{\text{sym},\,>0}$ is not perfect, for any non-zero $Y \in \mathbb{R}^{n\times n}_{\text{sym}}$ trace orthogonal to $M_f(F)$ there exists a $\lambda \in \mathbb{R}$ with $F + \lambda Y$ positive definite, $M_f(F + \lambda Y)$ containing $M_f(F)$ properly with more linearly independent matrices.

Clearly, iterating (ii) leads to a perfect form. Two perfect forms F_1 and F_2 in $\mathbb{R}^{n\times n}_{\text{sym},\,>0}$ are called neighbors if their Voronoi domains $V(F_1)$ and $V(F_2)$ share a face of co-dimension 1. Such a face spans a hyperplane of the form $H(Y) := \{X \in \mathbb{R}^{n\times n}_{\text{sym}} | \text{tr}(X, Y) = 0\}$ for some non-zero $Y \in \mathbb{R}^{n\times n}_{\text{sym}}$. The Y's describing co-dimension 1 faces of the Voronoi domain of F_1 are called directions of F_1 if $V(F_1) \subseteq \{X \in \mathbb{R}^{n\times n}_{\text{sym}} | \text{tr}(X, Y) \geq 0\}$ and can easily be found by omitting vectors from the maximal linearly independent subsets of $M_f(F)$ and computing the trace orthogonal spaces. In particular, each perfect $F \in \mathbb{R}^{n\times n}_{\text{sym},\,>0}$ has only finitely many neighbors. Moreover, the neighboring relation is respected by the $GL_n(\mathbb{Z})$ action.

We are now ready to discuss G-perfect forms. Together with the finite subgroup G of $GL_n(\mathbb{Z})$, we have to consider the transposed group G^{tr} consisting of the transposed matrices of G.

Remark 8.

(i) $\pi_G : \mathbb{R}^{n\times n}_{\text{sym}} \to \mathcal{F}(G^{\text{tr}}) : F \mapsto (1/|G|) \sum_{g\in G} gFg^{\text{tr}}$ is a linear projection of $\mathbb{R}^{n\times n}_{\text{sym},\,>0}$ onto $\mathcal{F}_{>0}(G^{\text{tr}})$.

(ii) $\text{tr}_G : \mathcal{F}(G) \times \mathcal{F}(G^{\text{tr}}) \to \mathbb{R} : (F_1, F_2) \mapsto \text{tr}(F_1, F_2)$ is a nondegenerate bilinear pairing satisfying $\text{tr}(F, \pi_G(xx^{\text{tr}})) = x^{\text{tr}}Fx$ for all $F \in \mathcal{F}_{>0}(G)$ and all $x \in M_v(F)$.

This easily verified remark suggests the following definition.

Definition 8. Let $F \in \mathcal{F}_{>0}(G)$.

(i) $M^G_f(F) := \pi_G(M_f(F))$.

(ii) $V_G(F) := \left\{ \sum_{f\in M^G_f(F)} a_f f | a_f \in \mathbb{R}, a_f \geq 0 \right\} \cap \mathbb{R}^{n\times n}_{\text{sym},\,>0} = \pi_G(V(F))$ is called the *G Voronoi domain* of F.

(iii) F is called *G-perfect*, if $V_G(F)$ has non-empty interior in $\mathcal{F}(G^{\text{tr}})$ or equivalently if $M^G_f(F)$ contains $\dim(\mathcal{F}(G))$ linearly independent matrices.

Again, the Voronoi construction for producing G-perfect forms works and one can define the corresponding neighboring relation for G-perfect forms (*cf.* Bergé & Martinet, 1992; Bergé *et al.*, 1992; Opgenorth, 1997). The role of $GL_n(\mathbb{Z})$ is taken over by $N_{GL_n(\mathbb{Z})}(G)$ and one has only finitely many orbits on G-perfect forms (*cf.* Jaquet-Chiffelle, 1995; Opgenorth, 1997). However, the G-Voronoi domain of a G-perfect form $F \in \mathcal{F}(G)$ may have co-dimension 1 faces which are not faces of another G-Voronoi domain but may lie on the boundary of $\mathcal{F}_{>0}(G^{\text{tr}})$ in $\mathcal{F}(G^{\text{tr}})$. The directions of the G-Voronoi domain of a G-perfect form F are given by those $Y \in \mathcal{F}(G)$ for which $H_G(Y) := \{X \in \mathcal{F}(G^{\text{tr}}) | \text{tr}_G(Y, X) = 0\}$ spans a co-dimension 1 face of $V_G(F)$ and $V_G(F) \subseteq \{X \in \mathcal{F}(G^{\text{tr}}) | \text{tr}_G(Y, X) \geq 0\}$. A direction is only determined by a co-dimension 1 face of $V_G(F)$ up to positive multiples. There are various ways of making them unique, for instance by insisting that they lie in $\mathbb{Z}^{n\times n}$ and that their entries have 1 as greatest common divisor. Denote the set of (in this sense) normalized directions of F by $D_G(F)$. Since $G = B(G)$ and since $V_G(F)$ together with F spans $\mathcal{F}(G)$, we clearly have the following characterization of normalizing elements of G, based on Remark 5.

Remark 9. Let $G = B(G) \leq GL_n(\mathbb{Z})$ be finite, $n \in GL_n(\mathbb{Z})$, and $F \in \mathcal{F}(G)$ a G-perfect form. Then $n \in N_{GL_n(\mathbb{Z})}(G)$ if and only if $n^{\text{tr}}Fn \in \mathcal{F}(G)$, $n^{\text{tr}}Fn$ is G-perfect, and $n^{\text{tr}}D_G(F)n = D_G(n^{\text{tr}}Fn)$.

One can clearly see now how the lattice automorphism and isometry routine can be used to find elements in the normalizer. Here are the essential steps of Opgenorth's algorithm producing a set of generators of the normalizer.

Set $N := N_{GL_n(\mathbb{Z})}(G)$, assume $G = B(G) \leq GL_n(\mathbb{Z})$ is finite. All G-perfect forms F coming up are to be normalized to have $m(F) = 1$.

Step 1: Compute a G-perfect form F_0 in $\mathcal{F}_{>0}(G)$.

Step 2: Starting with F_0, compute iterated neighbors to find a maximal set $\mathcal{P}$ of G-perfect forms, no two of which are in the same N orbit by using Remark 9, any two of which are connected by a chain of G-neighbors (*i.e.* a connected subgraph of the graph of G-perfect forms, whose vertices form a set of representatives of the N orbits of the G-perfect forms).

Step 3: For any $F \in \mathcal{P}$, compute a generating set of the stabilizer N_F of F in N (using the isometry routine and Remark 9).

Step 4: For any G-perfect $F \in \mathcal{F}(G)$, which is G-neighbor of some $F(F) \in \mathcal{P}$, compute the orbit under $N_{F(F)}$. If the orbit is disjoint to $\mathcal{P}$, pick a representative F_i and compute an $n_i \in N$ with $n_i^{\mathrm{tr}} F_i n_i \in \mathcal{P}$.

Step 5: Take the generating elements of Step 3 and the n_i of Step 4 together to form a generating set of N.

At the same time, it is now clear how to test $\mathbb{Z}$-equivalence of two Bravais groups G and H: One performs the normalizer algorithm for G, finds one H-perfect form for H and tries to match (in the sense of Remark 9) this form with one of the G-perfect forms computed before. The two groups are $\mathbb{Z}$-equivalent if and only if this works with exactly one of the (representative) G-perfect forms and the isometry yields the transforming element.

We would like to thank all those who have contributed to the algorithms, implementation, and checking of *CARAT*, in particular G. Nebe, H. Brückner, S. Kühne, A. Hilgers, and those who have read the manuscript, to make it accessible to crystallographers, in particular H. Wondratschek. *CARAT* is available *via* http://samuel.math.rwth-aachen.de/~LBFM/carat/.

References

Alperin, J. L. & Bell, R. B. (1995). *Groups and Representations*. Berlin: Springer Verlag.

Bergé, A.-M. & Martinet, J. (1992). *Astérisque*, **200**, 41–66.

Bergé, A.-M., Martinet, J. & Sigrist, F. (1992). *Astérisque*, **209**, 137–158.

Bosma, W. & Cannon, J. (1996). *Handbook of MAGMA Functions*. School of Mathematics and Statistics, University of Sydney, Australia. http://www.maths.usyd.edu.au:8000/comp/magma/Overview.html.

Brown, H., Bülow, R., Neubüser, J., Wondratschek, H. & Zassenhaus, H. (1977). *Crystallographic Groups of Four-Dimensional Space*. New York: Wiley.

Brown, H., Neubüser, J. & Zassenhaus, H. (1973). *Math Comput*. **27**, 167–182.

Conway, J. H. & Sloane, N. J. A. (1988). *Sphere Packings, Lattices and Groups*. Berlin: Springer Verlag.

Curtis, N. W. & Reiner, I. (1962). *Representation Theory of Finite Groups and Associative Algebras*. New York: Wiley-Interscience.

Hahn, Th. (1995). Editor. *International Tables for Crystallography*, Vol. A, 4th ed. Dordrecht: Kluwer Academic Publishers.

Holt, D. & Plesken, W. (1989). *Perfect Groups*. Oxford University Press.

Jaquet-Chiffelle, D.-O. (1995). *J. Theor. Nombres Bordeaux*, **7**.

Janner, A. & Janssen, T. (1977). *Phys. Rev. B*, **15**, 643–658.

Janssen, T. (1986). *Acta Cryst.* A**42**, 261–271.

Janssen, T., Janner, A., Looijenga-Vos, A. & de Wolff, P. M. (1992). *International Tables for Crystallography*, Vol. C, pp. 797–835. Dordrecht: Kluwer Academic Publishers.

Martinet, J. (1996). *Le Reseaux Parfaits des Escapes Euclidiens.* Paris: Masson.

Nebe, G. (1995). Aachener Beiträge zur Mathematik 12 (Dissertation). Aachen: Verlag Augustinus Buchhandlung.

Nebe, G. (1996*a*). *Exp. Math*. **5**, No. 3.

Nebe, G. (1996*b*). *Commun. Algebra*, **24**, 2341–2397.

Nebe, G. & Plesken, W. (1995). *AMS Mem*. **556**, 1–144.

Opgenorth, J. (1996). Aachener Beiträge zur Mathematik 16 (Dissertation). Aachen: Verlag Augustinus Buchhandlung.

Opgenorth, J. (1997). *Dual Cones and the Voronoi Algorithm*. In preparation.

Plesken, W. (1974). Dissertation, RWTH Aachen, Germany.

Plesken, W. (1977). *Commun. Algebra*, **5**, 375–396.

Plesken, W. (1978). *Reine Angew. Math*. **297**, 188–210.

Plesken, W. (1981). *Match*, **10**, 97–119.

Plesken, W. (1991). *Progress in Mathematics*, Vol. 95. *Representation Theory of Finite Groups and Finite-Dimensional Algebras*, edited by G. O. Michler & C. M. Ringel, pp. 477–496. Basel: Birkhaüser.

Plesken, W. (1996). *Group Theory, Algebra, Number Theory*, edited by H. G. Zimmer, pp. 74–96. Berlin: Walter de Gruyter.

Plesken, W. & Hanrath, W. (1984). *Math Comput*. **43**, No. 168, 573–587.

Plesken, W. & Pohst, M. (1977). *Math Comput*. **31**, No. 138, 536–577.

Plesken, W. & Pohst, M. (1980). *Math Comput*. **34**, No. 149, 245–301.

Plesken, W. & Pohst, M. (1985). *Math Comput*. **45**, No. 1, 209–221.

Plesken, W. & Souvignier, B. (1997). *J. Symb. Comput*. **24**, 327–334.

Schönert, M. (1993). *Groups, Algorithms and Programming*, Lehrstuhl D für Mathematik, RWTH Aachen, Germany. Available by anonymous ftp, together with the *GAP* system, on the servers dimacs.rutgers.edu or math.rwth-aachen.de.

Serre, J.-P. (1977). *Linear Representations of Finite Groups*. Berlin: Springer Verlag.

Souvignier, B. (1994). *Math Comput*. **63**, 335–350.

Zassenhaus, H. (1938). *Abh. Math. Sem. Univ. Hamburg*, **12**, 289–312.

Zassenhaus, H. (1948). *Comm. Math. Helv*. **21**, 117–141.