match no. 10 pp. 55-63 1981

AN ALGORITHM FOR FINDING THE SUBGROUPS OF n-DIMENSIONAL CRYSTALLOGRAPHIC GROUPS

Klaus-Joachim Köhler
Lehrstuhl für Informatik I
RWTH Aachen
5100 Aachen

1. Introduction

This is the last in a series of three papers on the construction of n-dimensional crystallographic groups and their subgroups. In the first paper [3] we proposed an algorithm for the construction of partially periodic groups from the point groups. Subgroup-relations of space groups and partially periodic groups were treated in the second paper [4]. There we showed in particular that the problem of finding all subgroups can be reduced to the determination of

type I-subgroups ("zellengleich", translation equivalent),
type II-subgroups ("klassengleich", class-equivalent), and
type III-subgroups.

Sometimes one is not interested in the complete subgroup lattice of a crystallographic group but rather in the affine types of the subgroups. Therefore, we propose in the present paper dimension-independent algorithms which for each pair (C,C^*) of n-dimensional crystallographic groups

1) decide whether or not C^* can be embedded into C, i.e. C contains a subgroup U with linear constituent $P(U) = P(C)$ such that U is affinely equivalent to C^*,

and if so,

2) calculate all embeddings of C^* into C.

In particular, all type II- and type III-subgroups are calculated. As the algorithm for problem 1) is essentially a simplification of that of problem 2), we first treat problem 2) in Chapter 2 and then problem 1) in Chapter 3.

The algorithm for problem 1) was implemented on a computer, and the affine classes of subgroups of all two- and three-dimensional space groups and partially periodic groups were calculated at the "Rechenzentrum der RWTH Aachen".

Moreover, crystallographic equivalence instead of affine equivalence can be treated by slight modifications of the algorithm. For $n \leqslant 3$ or n odd this leads to the same subgroup-relations ([5]).

I like to thank Professor J. Neubüser and Dr. W. Plesken for reading this paper and supplying helpful criticism.

2. Finding All Subgroups of a Given Affine Type

Whenever possible, we use definitions and notations from the preceeding papers [3] and [4]. Throughout this paper let

$C=\{(v_p+t,p)\mid p\in P,\ t\in\mathbb{Z}^r\}$ and $C^*=\{(v^*_{p^*}+t^*,p^*)\mid p^*\in P^*,t^*\in\mathbb{Z}^{r^*}\}$

be crystallographic groups with linear constituents

$P<GL(r,\mathbb{Z})\times GL(n-r,\mathbb{Z})$ and $P^*<GL(r^*,\mathbb{Z})\times GL(n-r^*,\mathbb{Z}), |P|=|P^*|$,

and vector systems

$v: P\rightarrow |P|^{-1}\cdot\mathbb{Z}^r$ and $v^*: P^*\rightarrow |P^*|^{-1}\cdot\mathbb{Z}^{r^*}$,

respectively. We shall derive necessary and sufficient conditions that C^* can be embedded into C, i.e. C contains a subgroup U affinely equivalent to C^*.*) These conditions are formulated as systems of rational and diophantic equations, which can be checked by a computer. The set of all solutions of the equations describe all embeddings of C^* into C.

To reduce the number of candidates C^* which can be embedded into C, we note:

2.1 Proposition. If the (n,r)-group C contains a subgroup U affinely equivalent to the (n,r^*)-group C^*, then

a) $r\geq r^*$,

b) the linear constituents P and P^* are $\mathbb{Q}$-equivalent, i.e. they belong to the same geometric crystal class,

c) the order $|v|$ of the vector system v of C divides the order $|v^*|$.

Proof: a) and b) are obvious.

c) We can assume that v is also a vector system of the subgroup U, i.e.

$U=\{(v_p+t,p)\mid p\in P,t\in M\},\quad M<\mathbb{Z}^r.$

As C^* and U are affinely equivalent, $|v^*|$ is the least positive integer such that

$U'=\{(|v^*|\cdot v_p+t,p)\mid p\in P,t\in M\}$

is a split extension of M by P. Therefore,

$C'=\{(|v^*|\cdot v_p+t,p)\mid p\in P,t\in\mathbb{Z}^r\}$

also splits, and thus $|v|$ divides $|v^*|$. □

2.2 Remark. The necessary conditions b) and c) of Proposition 2.1 can be considerably sharpened. As far as b) is concerned, this is done in the next proposition, and in the case of c) it would not simplify the announced algorithm.

2.3 Theorem. C contains a subgroup affinely equivalent to C^*, i.e. $(u,x)\cdot C^*\cdot(u,x)^{-1}<C$ for a suitable affine mapping $(u,x)\in A(n,\mathbb{R})$, if and only if there exist

$u\in\mathbb{Q}^r$ and $x=\begin{pmatrix}x' & x^*\\ 0 & x''\end{pmatrix}\in GL(n,\mathbb{Q})$ with $x'\in\mathbb{Z}^{r\times r^*}$

(and with $x^*=0$ for $r=r^*$) such that

---

*) Since we have required the linear constituents P and P^* to have the same order, $P(U)=P(C)=P$. The subgroup U need not be of type II or of type III, it can be a type II-subgroup of a type III-subgroup of C.

(1) $xP^*x^{-1} = P$,

(1') $v_p \equiv x \cdot v^*_{x^{-1}px} + (e-p) \cdot u \bmod \mathbb{Z}^r$ for all $p \in P$.

All subgroups $(u,x) \cdot C^* \cdot (u,x)^{-1}$ of C can be found as solutions of (1) and (1').

Proof: Let C^* be affinely equivalent to a subgroup of C. Then there exist $\bar{x} \in GL(n,\mathbb{R})$ and $\bar{u} = \begin{bmatrix} u' \\ u'' \end{bmatrix} \in \mathbb{R}^n$ such that $(\bar{u},\bar{x}) \cdot C^* \cdot (\bar{u},\bar{x})^{-1} < C$. Since translations are transformed into translations,

$$\bar{x} \cdot \mathbb{Z}^{r^*} < \mathbb{Z}^r, \text{ and thus } \bar{x} = \begin{pmatrix} x' & x^* \\ 0 & x'' \end{pmatrix}, \quad x' \in \mathbb{Z}^{r \times r^*}.$$

Let

$$u := \begin{bmatrix} u' \\ 0 \end{bmatrix} \quad \text{and} \quad x := \begin{cases} \bar{x} & \text{for } r \neq r^* \\ \begin{pmatrix} x' & 0 \\ 0 & x'' \end{pmatrix} & \text{for } r = r^* \end{cases} .$$

From

$$\bar{x}p^*\bar{x}^{-1} = xp^*x^{-1} \quad \text{for all } p^* \in P^*$$

and

$$\begin{aligned}
&(\bar{u},\bar{x}) \cdot C^* \cdot (\bar{u},\bar{x})^{-1} \\
&= (\bar{u},\bar{x}) \cdot \{(v^*_{p^*} + t^*, p^*) \mid p^* \in P^*, t^* \in \mathbb{Z}^{r^*}\} \cdot (-\bar{x}^{-1} \cdot \bar{u}, \bar{x}^{-1}) \\
&= \{(\bar{u} + \bar{x} \cdot v^*_{p^*} + \underbrace{\bar{x} \cdot t^*}_{t} - \underbrace{\bar{x}p^*\bar{x}^{-1}}_{p} \cdot \bar{u}, \underbrace{\bar{x}p^*\bar{x}^{-1}}_{p}) \mid p^* \in P^*, t^* \in \mathbb{Z}^{r^*}\} \\
&= \{(\bar{x} \cdot v^*_{\bar{x}^{-1}p\bar{x}} + (e-p) \cdot \bar{u} + t, p) \mid p \in \bar{x}P^*\bar{x}^{-1}, t \in \bar{x} \cdot \mathbb{Z}^{r^*}\} \\
&< C = \{(v_p + t, p) \mid p \in P, t \in \mathbb{Z}^r\}
\end{aligned}$$

we derive that

$$(\bar{u},\bar{x}) \cdot C^* \cdot (\bar{u},\bar{x})^{-1} = (u,x) \cdot C^* \cdot (u,x)^{-1},$$

and the stated formulas (1) and (1') follow immediately. Moreover, we can assume without loss of generality that x and u are rational instead of real because they are solutions of the systems of the rational linear equations

$$x \cdot p^* = p \cdot x \text{ for } p^* \in P^* \text{ and suitable } p \in P$$

and

$$(e-p) \cdot u = v_p - x \cdot v^*_{x^{-1}px} + t_p \text{ for } p \in P \text{ and suitable } t_p \in \mathbb{Z}^r,$$

respectively. Since $\mathbb{Q}^{n \times n}$ is a dense subset of $\mathbb{R}^{n \times n}$ and the determinant is a continuous function, there is a solution $x \in GL(n,\mathbb{Q})$ if there is one in $GL(n,\mathbb{R})$ ([2,p.200], see also [3, Theorem 3.3]).

The converse follows directly from the above computations. □

2.4 Corollary. Let

$$xP^*x^{-1} = P \text{ for a matrix } x = \begin{pmatrix} x' & x^* \\ 0 & x'' \end{pmatrix} \in GL(n,\mathbb{Q}), \quad x' \in \mathbb{Q}^{r \times r^*}.$$

(For $r = r^*$ this means that P and P^* are $\mathbb{Q} \times \mathbb{Q}$-equivalent.)

a) If C is symmorphic, i.e. a split extension of $\mathbb{Z}^r$ by P, then C contains a subgroup affinely equivalent to C^*.

b) If C^* is symmorphic, then C contains a subgroup affinely equivalent to C^* if and only if C is symmorphic, too.

Proof: a) We can assume that $v_p = 0$ for all $p \in P$. Multiplying x with a suitable integer, we can assume that $x \in |P| \cdot \mathbb{Z}^{n\times n}$. Now the conditions (1) and (1') in Theorem 2.3 are fulfilled.

b) If C^* can be embedded into C, then $|v|$ divides $|v^*| = 1$ by Proposition 2.1 c), and hence $|v| = 1$. The converse follows from a). □

Theorem 2.3 yields an algorithm for determining the subgroups of C that are affinely equivalent to C^*. The matrix x of Theorem 2.3 induces an isomorphism

$\varphi : P \to P^*$ defined by $\varphi(p) := x^{-1}px$

that leaves invariant the determinant and the trace of the matrices. Therefore, we can formulate the first version of our algorithm as follows:

- Determine the set

$$I'(P,P^*) := \{\varphi : P \to P^* \mid \varphi \text{ isomorphism, } \det\varphi(p) = \det p, \operatorname{trace}\varphi(p) = \operatorname{trace} p \text{ for } p \in P\}$$

- For each $\varphi \in I'(P,P^*)$ determine the set of all $x \in GL(n,\mathbb{Q})$, $u \in \mathbb{Q}^r$ which for all $p \in P$ fulfill the conditions

$$(2) \quad x \cdot \varphi(p) = p \cdot x,\ x = \begin{pmatrix} x' & x^* \\ 0 & x'' \end{pmatrix},\ x' \in \mathbb{Z}^{r\times r^*} \text{ (and } x^* = 0 \text{ for } r = r^*)$$

$$(2') \quad v_p \equiv x \cdot v^*_{\varphi(p)} + (e - p) \cdot u \mod \mathbb{Z}^r.$$

Let $\varphi : P \to P^*$ be a fixed isomorphism induced by a rational matrix. Then

$$I'(P,P^*) = \{\psi : P^* \to P^* \mid \psi \text{ automorphism, } \det\psi(p) = \det p, \operatorname{trace}\psi(p) = \operatorname{trace} p \text{ for } p \in P\} \circ \varphi;$$

and the automorphisms can be determined by a slight modification of an existing computer program ([6]).

Obviously, (2) and (2') have only to be checked for a set of generators $p_1,\dots,p_k$ of P, and $I'(P,P^*)$ can be replaced by

$$I(P,P^*) := \{\psi : P^* \to P^* \mid \psi \text{ automorphism, } \det\psi(p_i) = \det p_i, \operatorname{trace}\psi(p_i) = \operatorname{trace} p_i \text{ for } i = 1,\dots,k\} \circ \varphi$$

Since (2) is a system of homogeneous linear equations, one can easily calculate a $\mathbb{Q}$-basis

$$x_1 = \begin{pmatrix} x_1' & x_1^* \\ 0 & x_1'' \end{pmatrix}, \dots, x_b = \begin{pmatrix} x_b' & x_b^* \\ 0 & x_b'' \end{pmatrix} \in \mathbb{Q}^{n\times n}$$

of the rational solutions of (2) such that for a suitable $t \leq b$

$x_1',\dots,x_t' \in \mathbb{Z}^{r\times r^*}$

is a $\mathbb{Z}$-basis of the integral upper blocks $x' \in \mathbb{Z}^{r\times r^*}$ occurring in the rational solutions $x \in \mathbb{Q}^{n\times n}$ of (2).

Using the methods of the generalized Zassenhaus algorithm ([3]) and setting

$x' = \lambda_1 \cdot x_1' + \dots + \lambda_t \cdot x_t',\ \lambda_i \in \mathbb{Z},$

we can transform (2') into a system of diophantic equations

$F \cdot \lambda \equiv W \mod \mathbb{Z}^s,\quad \lambda \in \mathbb{Z}^t.$

The set of solutions

$\Lambda := \{\lambda \in \mathbb{Z}^t \mid F \cdot \lambda \equiv W \mod \mathbb{Z}^s\}$

can be calculated by methods similar to those of the Zassenhaus algorithm (see [1], [3]).

Therefore, the solutions x of (2) and (2') can be parametrized by

$$x = \lambda_1 \cdot x_1 + \dots + \lambda_b \cdot x_b \ , \ (\lambda_1,\dots,\lambda_t)^{tr} \in \Lambda, \ \lambda_{t+1},\dots,\lambda_b \in \mathbb{Q}, \ \det x \neq 0.$$

As the set Λ and the polynomial det x can be calculated by a computer, it is usually very easy to describe x explicitely. For each fixed $x \in GL(n,\mathbb{Q})$ the solutions $u \in \mathbb{Q}^r$ of (2') can easily be calculated, and hence all subgroups $(u,x) \cdot C^* \cdot (u,x)^{-1}$ of C can be calculated.

Different solutions (u,x) and $(\bar{u},\bar{x})$ of (2) and (2') yield the same subgroup

$$(u,x) \cdot C^* \cdot (u,x)^{-1} = (\bar{u},\bar{x}) \cdot C^* \cdot (\bar{u},\bar{x})^{-1}$$

of C if and only if $(\bar{u},\bar{x})$ lies in the coset $(u,x) \cdot N_{A(n,\mathbb{R})}(C^*)$ of the normalizer of C^* in the affine group $A(n,\mathbb{R})$.

The whole algorithm for the determination of the subgroups of C affinely equivalent to C^* is described by the following refinement of our first version. The algorithm is formulated for the case $r > r^*$, but the modification (and simplification) for the case $r = r^*$ is obvious.

2.5 <u>Algorithm</u> for determining all subgroups of C which are affinely equivalent to C^*.
If $r > r^*$ and P is $\mathbb{Q}$-equivalent to P^* and $|v|$ divides $|v^*|$ then
- determine the group of isomorphisms $I(P,P^*)$,
- for each $\varphi \in I(P,P^*)$
  - calculate a $\mathbb{Q}$-basis $x_1 = \begin{pmatrix} x_1' & x_1^* \\ 0 & x_1'' \end{pmatrix}$, ..., $x_b = \begin{pmatrix} x_b' & x_b^* \\ 0 & x_b'' \end{pmatrix}$ of the solutions of $x \cdot \varphi(p_i) = p_i \cdot x$, $i = 1,\dots,k$, such that $x_1',\dots,x_t'$ forms a $\mathbb{Z}$-basis of $\mathbb{Z}^{r \times r^*} \cap \langle x_1',\dots,x_b' \rangle_{\mathbb{Q}}$
  - if $\det(\lambda_1 \cdot x_1 + \dots + \lambda_b \cdot x_b)$ is not the zero polynomial, then
    - determine $v^*_{\varphi(p_1)},\dots,v^*_{\varphi(p_k)}$,
    - transform the congruences
      $(*)$ $v_{p_i} \equiv (\lambda_1 \cdot x_1' + \dots + \lambda_t \cdot x_t') \cdot v^*_{\varphi(p_i)} + (e' - p_i') \cdot u \bmod \mathbb{Z}^r$, $i = 1,\dots,k$,
      into a system of diophantic equations $F \cdot \lambda \equiv W \bmod \mathbb{Z}^s$, $\lambda \in \mathbb{Z}^t$,
    - determine the set $\Lambda = \{\lambda \in \mathbb{Z}^t \mid F \cdot \lambda \equiv W \bmod \mathbb{Z}^s\}$,
    - determine the (empty or infinite) set of matrices
      $X = \{x = \lambda_1 \cdot x_1 + \dots + \lambda_b \cdot x_b \mid (\lambda_1,\dots,\lambda_t)^{tr} \in \Lambda, \ \det x \neq 0\}$,
    - for each $x \in X$
      - calculate all solutions u of $(*)$ and form the corresponding subgroups $(u,x) \cdot C^* \cdot (u,x)^{-1}$ of C.

2.6 <u>Example</u>: We determine such subgroups of the space group

$$C = \left\langle \left(\begin{bmatrix} 1/2 \\ 0 \\ 0 \end{bmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \right), \ (t,e) \ \middle| \ t \in \mathbb{Z}^3 \right\rangle$$

(Hermann-Maughin-symbol $P4_2$) that are affinely equivalent to the (3,1)-group

$$C^* = \left\langle \left(\begin{bmatrix} 1/4 \\ 0 \\ 0 \end{bmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \right) \right\rangle .$$

Let $P := P(C) = P^* := P(C^*) = \left\langle p := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \right\rangle$,

$$v_p := \begin{bmatrix} 1/2 \\ 0 \\ 0 \end{bmatrix}, \quad v_p^* := [1/4].$$

The group $I(P,P^*)$ consists of the isomorphisms

$\varphi_1 : P \to P^*$ with $\varphi_1(p) = p$

$\varphi_2 : P \to P^*$ with $\varphi_2(p) = p^3$.

Let $\varphi := \varphi_1$. Then

$$x_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad x_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad x_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$$

forms a $\mathbb{Q}$-basis for the solutions of $x \cdot \varphi(p) = p \cdot x$, and

$$x_1' = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad \text{forms a } \mathbb{Z}\text{-basis of } \mathbb{Z}^{3\times 1} \cap \langle x_1', x_2', x_3' \rangle_{\mathbb{Q}} .$$

Congruence $(*)$ becomes

$$\begin{bmatrix} 1/2 \\ 0 \\ 0 \end{bmatrix} \equiv \lambda_1 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \cdot [1/4] + \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \right) \cdot \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} \mod \mathbb{Z}^3$$

i.e. $1/2 \equiv 1/4 \cdot \lambda_1 \mod \mathbb{Z}$, $(F \cdot \lambda \equiv W \mod \mathbb{Z}^s,\ \lambda \in \mathbb{Z}^t)$

$0 \equiv u_2 + u_3 \mod \mathbb{Z}$, $0 \equiv -u_2 + u_3 \mod \mathbb{Z}$.

Therefore, $\Lambda = \{\lambda_1 \in \mathbb{Z} \mid \lambda_1 \equiv 2 \mod 4\} = 4\mathbb{Z} + 2$, and the set X consists of the matrices

$$x = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & -\lambda_3 \\ 0 & \lambda_3 & \lambda_2 \end{pmatrix}, \quad \lambda_1 \in 4\mathbb{Z} + 2, \quad \lambda_2, \lambda_3 \in \mathbb{Q},$$

$0 \neq \det x = \lambda_1 \cdot (\lambda_2^2 + \lambda_3^2)$, i.e. $\lambda_2 \neq 0$ or $\lambda_3 \neq 0$.

The solutions u of $(*)$ belonging to x are

$u_1 \in \mathbb{Q}$, $u_2, u_3 \in \frac{1}{2}\mathbb{Z}$,

and the subgroups of C belonging to x and u are

$$\left\langle \left(\begin{bmatrix} \lambda_1/4 \\ a \\ b \end{bmatrix} + t, p \right) \;\middle|\; t \in \begin{pmatrix} \lambda_1 \\ 0 \\ 0 \end{pmatrix} \cdot \mathbb{Z}^1 \right\rangle, \ \lambda_1 \in 4\mathbb{Z} + 2, \ a = u_2 + u_3 \in \mathbb{Z}, \ b = -u_2 + u_3 \in \mathbb{Z}.$$

They are mutually different.

Now let $\varphi = \varphi_2$. Then

$$x_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad x_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad x_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

forms a $\mathbb{Q}$-basis of the solutions of $x \cdot \varphi(p) = p \cdot x$, and

$x_1' = \begin{pmatrix}1\\0\\0\end{pmatrix}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}^{3\times 1} \cap \langle x_1', x_2', x_3'\rangle_{\mathbb{Q}}$.

As $v^*_{\varphi(p)} = [3/4]$, congruence (*) becomes

$1/2 \equiv 3/4 \cdot \lambda_1 \mod \mathbb{Z}$,

$0 \equiv u_2 + u_3 \mod \mathbb{Z}$, $0 \equiv -u_2 + u_3 \mod \mathbb{Z}$.

Therefore, $\Lambda = \{\lambda_1 \in \mathbb{Z} \mid 3\lambda_1 \equiv 2 \mod 4\} = 4\mathbb{Z} + 2$ and

$$X = \left\{ x = \begin{pmatrix}\lambda_1 & 0 & 0\\ 0 & \lambda_2 & \lambda_3\\ 0 & \lambda_3 & -\lambda_2\end{pmatrix} \;\middle|\; \lambda_1 \in 4\mathbb{Z}+2,\ \lambda_2,\lambda_3 \in \mathbb{Q},\ \det x = -\lambda_1 \cdot (\lambda_2^2 + \lambda_3^2) \neq 0 \right\},$$

and the mutually different subgroups of C belonging to $\varphi = \varphi_2$ are

$$\left\langle \left(\begin{bmatrix} 3/4 \cdot \lambda_1 \\ a \\ b \end{bmatrix} + t, p \right) \;\middle|\; t \in \begin{pmatrix}\lambda_1\\0\\0\end{pmatrix} \cdot \mathbb{Z}^1 \right\rangle, \quad \lambda_1 \in 4\mathbb{Z}+2,\ a,b \in \mathbb{Z}.$$

The subgroups belonging to φ_1 are mutually different from those belonging to φ_2. (They are affinely but not crystallographically equivalent, i.e. enantiomorphic). □

3. Deciding whether or not a Crystallographic Group Contains Subgroups of a Given Affine Type

Theorem 2.3 yields an algorithm for deciding whether C* can be embedded into C. This algorithm essentially checks for each isomorphism $\varphi: P \to P^*$ whether there is a matrix $x = \begin{pmatrix}x' & x^*\\ 0 & x''\end{pmatrix} \in GL(n,\mathbb{Q})$ with $\varphi(p) = x^{-1} p x$ for all $p \in P$ such that the (n,r^*)-group $(0,x) \cdot C^* \cdot (0,x)^{-1}$ is translationally equivalent to a subgroup U of C (see Algorithm 2.5). Let ψ be an automorphism of P* induced by a matrix y^{-1}, $y = \begin{pmatrix}y' & 0\\ 0 & y''\end{pmatrix} \in N_{\mathbb{Z}\times\mathbb{Q}}(P^*)$. Then $(0,x) \cdot C^* \cdot (0,x)^{-1}$ is translationally equivalent to U for a matrix $x \in GL(n,\mathbb{Q})$ inducing φ if and only if there is a matrix $z = \begin{pmatrix}z' & z^*\\ 0 & z''\end{pmatrix} \in GL(n,\mathbb{Q})$ inducing $\psi \circ \varphi$ so that $(0,z) \cdot (0,y) \cdot C^* \cdot (0,y)^{-1} \cdot (0,z)^{-1}$ is translationally equivalent to U (choose $z := x \cdot y^{-1}$). Therefore, we need not consider all isomorphisms $\varphi: P \to P^*$ if we take into account the (n,r^*)-groups

$(0,y) \cdot C^* \cdot (0,y)^{-1}$, $y \in N_{\mathbb{Z}\times\mathbb{Q}}(P^*)$

instead of C* only.

This trade-off between the number of isomorphisms φ and the number of groups $(0,y) \cdot C^* \cdot (0,y)^{-1}$ reduces the amount of calculations consideralby since the groups $(0,y) \cdot C^* \cdot (0,y)^{-1}$ are already calculated in the generalized Zassenhaus algorithm ([3]).

To fomulate this result more precisely, we call isomorphisms $\varphi, \bar{\varphi}: P \to P^*$ induced by matrices $x = \begin{pmatrix}x' & x^*\\ 0 & x''\end{pmatrix}$, $\bar{x} = \begin{pmatrix}\bar{x}' & \bar{x}^*\\ 0 & \bar{x}''\end{pmatrix} \in GL(n,\mathbb{Q})$ equivalent if $\bar{\varphi} \circ \varphi^{-1}$ is an automorphism of P* induced by a matrix $y = \begin{pmatrix}y' & 0\\ 0 & y''\end{pmatrix} \in N_{\mathbb{Z}\times\mathbb{Q}}(P^*)$. Let $I_{rep}(P,P^*) \subset I(P,P^*)$ be a set of representatives of the so defined equivalence classes. Then

$$I_{rep}(P,P^*) = A_{rep}(P^*) \circ \varphi,$$

where $A_{rep}(P^*)$ is a set of representatives of the cosets of the automorphism group induced by $N_{\mathbb{Z}\times\mathbb{Q}}(P^*)$ in the automorphism group induced by $N_{\mathbb{Q}\times\mathbb{Q}}(P^*)$. Since $N_{\mathbb{Z}\times\mathbb{Q}}(P^*)$ has already to be known for the generalized Zassenhaus algorithm, $A_{rep}(P^*)$ can easily be determined.

3.1 Theorem. Let

$$C_j^* = \{(v_p^j + t^*, p^*) \mid p^* \in P^*, t^* \in Z^{r^*}\},\ v_p^j \in |P^*|^{-1} \cdot Z^{r^*},\ j = 1,\dots,d,$$

be representatives of such classes of translationally equivalent (n,r^*)-groups which are affinely equivalent to C^*. Then C contains a subgroup affinely equivalent to C^* if and only if there exist a group C_j^*, an isomorphism $\varphi \in I_{rep}(P,P^*)$, a vector $u \in \mathbb{Q}^r$, and a matrix

$$x = \begin{pmatrix} x' & x^* \\ 0 & x'' \end{pmatrix} \in \mathbb{Q}^{n\times n} \text{ with } x' \in \mathbb{Z}^{r\times r^*} \text{ (and } x^* = 0 \text{ for } r = r^*)$$

(we do not require x to be regular) such that for all $p \in P$

$$(*) \qquad \begin{aligned} & x \cdot \varphi(p) = p \cdot x \\ & v_p \equiv x \cdot v_{\varphi(p)}^j + (e - p) \cdot u \bmod \mathbb{Z}^r \end{aligned}$$

Proof: Since $C_j^* = (u_j, y_j) \cdot C^* \cdot (u_j, y_j)^{-1}$ for suitable $u_j \in \mathbb{Q}^{r^*}$ and $y_j \in N_{\mathbb{Z}\times\mathbb{Q}}(P^*)$, the assertion would follow immediately from the corresponding Theorem 2.3 and the above remarks if we had required that x be regular. So we only have to show that, if there is a solution x of $(*)$, then there is one with $\det x \neq 0$, as well.

Let $(*)$ be fulfilled by φ, u, and x and let φ be induced by
$y = \begin{pmatrix} y' & y^* \\ 0 & y'' \end{pmatrix} \in GL(n,\mathbb{Q}) \cap \mathbb{Z}^{n\times n}$ (with $y^* = 0$ for $r = r^*$). Then $(*)$ is also fulfilled by φ, u, and

$$\bar{x} := x + z \cdot |P| \cdot y,\ z \in \mathbb{Z},$$

and

$$\det \bar{x} = z^n \cdot \det\left(\frac{1}{z} \cdot x + |P| \cdot y\right) \neq 0$$

for sufficiently large $z \in \mathbb{Z}$ since the determinant is a continuous function of the entries of the maxtrix. □

We formulate the resulting algorithm for $r = r^*$. The modification for the case $r \geqslant r^*$ is obvious.

3.2 Algorithm for the test of whether or not C contains as subgroup affinely equivalent to C^*.

If $r = r^*$ and P is $\mathbb{Q}$-equivalent to P^* and $|v|$ divides $|v^*|$, then

- determine the set $\mathcal{V}^* = \{v^1,\dots,v^d\}$ of vector systems which represent the classes of translationally equivalent (n,r^*)-groups with linear constituent P^* (generalized Zassenhaus algorithm),

- determine the set of isomorphisms $I_{rep}(P,P^*)$
- for each $\varphi \in I_{rep}(P,P^*)$
  - calculate a $\mathbb{Z}$-basis $x_1',\ldots,x_t' \in \mathbb{Z}^{r \times r^*}$ of solutions of
    $$x' \cdot \varphi(p_i)' = p_i' \cdot x', \ i = 1,\ldots,k,$$
  - for each vector system $v^j \in \mathcal{V}^*$
    - transform the congruences
      $v_{p_i} \equiv (\lambda_1 \cdot x_1' + \ldots + \lambda_t \cdot x_t') \cdot v^j_{\varphi(p_i)} + (e' - p_i') \cdot u \bmod \mathbb{Z}^r$
      into a system of diophantic equations
      $F \cdot \lambda \equiv W \bmod \mathbb{Z}^s, \ \lambda \in \mathbb{Z}^t$,
    - if a solution λ exists, then
      C* can be embedded into C; STOP.
- C* cannot be embedded into C.

4. Conclusion

If one applies the developed algorithms to all pairs (C,C*) of n-dimensional crystallographic groups belonging to a fixed $\mathbb{Q}$-class, then obviously all subgroup-relations between the groups of this $\mathbb{Q}$-class are known. As the methods used in the algorithms, namely solving systems of diophantic equations, are similar to those of the generalized Zassenhaus algorithm, one might hope to reduce the amount of computation by simultaneously constructing all (n,r)-groups of a $\mathbb{Q}$-class and determining the subgroup-relations between them. Further investigations may show whether this is practicable or not.

References

[1] Brown,H., An algorithm for the determination of space groups, Math.Comp. 23 (1969), 499 - 514.

[2] Curtis,C.W., Reiner,J., Representation theory of finite groups and associative algebras, Wiley (Interscience), New York, 1962.

[3] Köhler,K.-J., On the Structure and the Determination of n-Dimensional Partially Periodic Crystallographic Groups, to appear.

[4] Köhler,K.-J., Subgroup-Relations between Crystallographic Groups, to appear.

[5] Köhler,K.-J., Untergruppen kristallographischer Gruppen, Dissertation, Aachen, 1977.

[6] Roberts,H., Eine Methode zur Berechnung der Automorphismengruppe einer endlichen Gruppe, Diplomarbeit, Aachen, 1976.