NIEUW ARCHIEF VOOR WISKUNDE (4), Vol. 2, (1984) 267-280

ON THE NORMAL SUBGROUPS OF RUBIK GROUPS

J. van de CRAATS & R.J. SCHOOF

1. INTRODUCTION

Rubik's Cube and related toys like Meffert's Pyraminx or the 4×4×4 Master Cube ('Rubik's Revenge') provide examples of nontrivial finite groups, and thus are important didactical tools in a first course on group theory. Concepts like group, subgroup, coset, normal subgroup, conjugation, factor group, commutator subgroup, center, generator, transitivity, direct product, homomorphism, isomorphism, are vividly illustrated with a cube at hand.

In this note we shall concentrate upon normal subgroups, and among other results, we shall give a proof of the fact, first discovered by the second author in 1981, that the group of Rubik's Cube has exactly 13 normal subgroups.

2. RUBIK GROUPS

Rubik's Cube has three kinds of pieces: six *center pieces*, having fixed locations relative to each other, twelve *edge pieces*, and eight *corner pieces*. The six center pieces form a natural reference frame. With respect to this frame, every edge piece and every corner piece has a well-defined *home-location* and *home-orientation*.

Any state of the cube may be described by a quadruplet (ρ, v, σ, w) where the permutation $\rho \in S_{12}$ describes the location of the twelve edge pieces, the 12-tuple $v = (v_1, \ldots, v_{12}) \in C_2^{12}$ characterizes the orientations of the edge pieces, the permutation $\sigma \in S_8$ describes the location of the corner pieces and the 8-tuple $w = (w_1, \ldots, w_8) \in C_3^8$ their orientations (S_n denotes the *symmetric group* of all permutations on n objects, A_n will be the *alternating group* of all *even* permutations and C_q the cyclic group with q elements).

To be specific, we number the edge pieces and the corner pieces in an arbitrary way, and mark one of the faces of every piece. This induces a numbering and marking of every home-location, determined by START, the state of the 'clean' cube. In a state described by (ρ, v, σ, w), $\rho(i)$ is the number of the actual location of edge piece i; $v_j = 0$ or 1 means that the edge piece now on location j (i.e. piece number $\rho^{-1}(j)$) has a marking that does or does not coincide with the home-marking of location j. Similarly, $\sigma(i)$ defines the location of corner piece i, and $w_j = +1$, -1 or 0 describes a clockwise twist, an anticlockwise twist, or no twist at all of the cornerpiece on location j.

It is well-known (see, e.g. SINGMASTER, 1980; VAN DE CRAATS, 1981, ch. 5; FREY & SINGMASTER, 1982, ch.7, or BERLEKAMP, CONWAY & GUY, 1982, p. 760-768) that for any state (ρ, v, σ, w) of the cube

(i) $\operatorname{sgn} \rho = \operatorname{sgn} \sigma$,

(ii) $\sum_{i=1}^{12} v_i = 0$,

(iii) $\sum_{i=1}^{8} w_i = 0$.

Conversely, any quadruplet (ρ, v, σ, w) satisfying (i), (ii) and (iii) can be realized by turning a cube in an appropriate way.

A quadruplet (ρ, v, σ, w) also may be interpreted as a *transformation* of the set of states of the cube. A state is transformed by (ρ, v, σ, w) in the following way: the edge piece on location i is brought to location $\rho(i)$ with orientation flipped iff $v_{\rho(i)} = 1$, and similarly for the cornerpieces. The two interpretations of (ρ, v, σ, w) are connected by the effect of the transformation on START.

Considered as transformations, the quadruplets form a *group* R. We shall use the convention that the composition

$$(1) \qquad (\rho, v, \sigma, w)\,(\bar\rho, \bar v, \bar\sigma, \bar w)$$

means that *first* $(\bar\rho, \bar v, \bar\sigma, \bar w)$ is taken, and *then* (ρ, v, σ, w). When (1) is applied to START, then edge piece i first goes to location $\bar\rho(i)$ with orientation $\bar v_{\bar\rho(i)}$, and then to $\rho\bar\rho(i)$ with orientation $\bar v_{\bar\rho(i)} + v_{\rho\bar\rho(i)}$. If we put $\rho\bar\rho(i) = j$ and define $\rho\bar v \in C_2^{12}$ by $(\rho\bar v)_j = \bar v_{\rho^{-1}(j)}$, then

$$\bar v_{\bar\rho(i)} + v_{\rho\bar\rho(i)} = \bar v_{\rho^{-1}(j)} + v_j = (\rho\bar v + v)_j ,$$

so the new orientation vector is $\rho\bar v + v$.

In a similar way the corner pieces are affected, and we see that

$$(\rho, v, \sigma, w)\,(\bar\rho, \bar v, \bar\sigma, \bar w) = (\rho\bar\rho,\ \rho\bar v + v,\ \sigma\bar\sigma,\ \sigma\bar w + w).$$

Note that if 1 is the identity permutation, the neutral element of the group (also denoted by 1) is (1, 0, 1,0) and

$$(\rho, v, \sigma, w)^{-1} = (\rho^{-1}, -\rho^{-1}v, \sigma^{-1}, -\sigma^{-1}w).$$

The black edges group

With Rubik's Cube modified, other interesting groups may be obtained. For example, if we color all edge pieces black, so that they cannot be distinguished from each other, the group becomes

$$G(8,3) = \left\{(\sigma, w) \mid \sigma \in S_8;\ w = (w_1, \ldots, w_8) \in C_3^8,\ \sum_{i=1}^{8} w_i = 0\right\}.$$

(The notation G(8,3) will be explained later). Note that in this group no limitation on the parity of σ occurs: any $\sigma \in S_8$ can be realized!

The black corners group

Another interesting group occurs when the corners are colored black:

$$G(12,2) = \left\{(\rho, v) \mid \rho \in S_{12},\ v = (v_1, \ldots, v_{12}) \in C_2^{12},\ \sum_{i=1}^{12} v_i = 0\right\}.$$

The black centers group

When all center pieces are colored black, our reference frame disappears. However, with respect to *one* particular corner piece, the other seven corner pieces and the twelve edge pieces again have well-defined home-locations and home-orientations, and the group becomes

$$G(12,2) \times G(7,3) = \left\{(\rho, v, \sigma, w) \mid \rho \in S_{12},\ \sigma \in S_7,\ v = (v_1, \ldots, v_{12}) \in C_2^{12},\ w = (w_1, \ldots, w_7) \in C_3^7,\ \sum_{i=1}^{12} v_i = \sum_{i=1}^{7} w_i = 0\right\}.$$

It is interesting to note that indeed there are no limitations on the parity of the permutations, and therefore this group is a direct product of the action on the corners and the action on the edges.

The 2×2×2 group

If the edges *and* the centers are colored black, a simulated 2×2×2 cube results, and, again taking one corner piece as point of reference, its group is

$$G(7,3) = \left\{(\sigma,w) \mid \sigma \in S_7 , w = (w_1,\dots,w_7) \in C_3^7 , \sum_{i=1}^{7} w_i = 0\right\}.$$

Meffert's Pyraminx

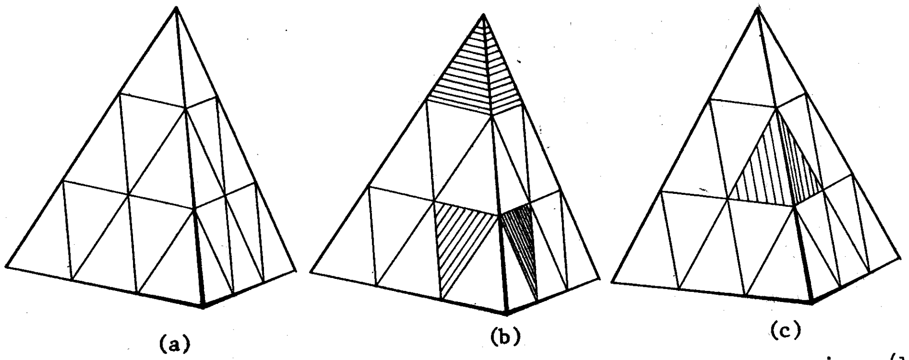

fig.1 Meffert's Pyraminx (a), with corner piece, subcorner piece (b) and edge piece (c)

This object has four corner pieces, four subcorner pieces and six edges pieces. In turning, the corner- and subcorner pieces keep their locations relative to each other, and any orientation of these eight pieces can be realized without affecting the edges by a suitable sequence of moves. So the only interesting part is formed by the possible locations and orientations of the six edge pieces. Any move of the pyraminx engenders a 3-cycle on edges, so only *even* permutations can be realized. Furthermore, as with Rubik's Cube, the orientations are such that in any state the total number of 'flipped' edges is even. The edge group, denoted by H(6,2), thus is

$$H(6,2) = \left\{(\rho,v) \mid \rho \in A_6 , v = (v_1,\dots,v_6) \in C_2^6 , \sum_{i=1}^{6} v_i = 0\right\},$$

and the complete group of Meffert's Pyraminx is the direct product $H(6,2) \times C_3^8$.

The 4×4×4 Master Cube

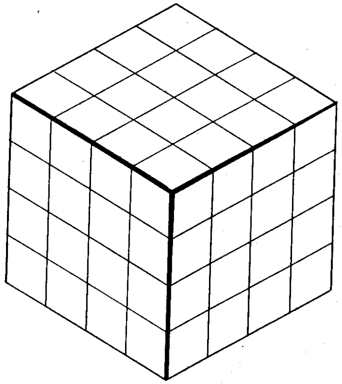

fig.2 The Master Cube

This most astonishing toy has eight corner pieces, 24 edge pieces (two on every edge), and 24 center pieces (four on every face). The edge pieces appear with equal colors in pairs , but since the side of such a piece that is adjacent to a *middle plane* of the cube always keeps such a position, the two pieces are *mirror images* and in any state of the cube they can be distinguished from each other. Consequently, such a piece cannot be flipped on its place: each piece can occupy each edge position *in only one orientation*! Similarly, the center pieces always keep their innermost corner in the center of a face, and thus every center piece also has only one possible orientation on every center location: centers cannot be twisted on their place!

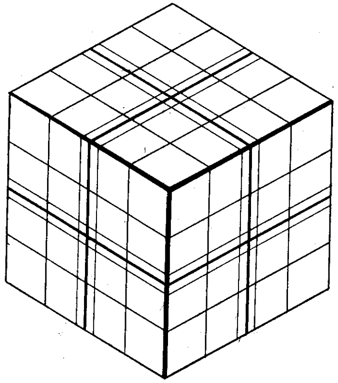

fig.3 Edge pieces and center pieces of the Master Cube have only one possible orientation

However, it is impossible to distinguish between four equally colored center pieces, and this means that the different states of the Master Cube do *not* generated a group! Two sequences of moves that yield the same result when applied to START, may give *distinct* results when applied to another state!

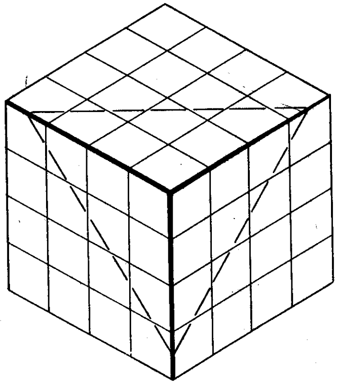

fig.4 A pattern to give each center piece a well-defined home-location

If we provide the faces with patterns to distinguish the center pieces from each other, however, we do get a group; let us call it the *quadro-super-group* Q. Again, we take one particular corner piece as point of reference. Then with suitable patterns on the faces, the seven other corner pieces, the 24 edge pieces and the 24 center pieces all have a well-defined home-location and (only for the corner pieces) home-orientation. Keen cubologists may have discovered that *any* permutation of the 24 edges can be obtained without affecting the other pieces. Thus Q is the direct product of S_{24} (the action on the edges) and the action on corners and centers.

Any quarterturn of a face not containing the chosen reference corner, yields a 4-cycle on corners and centers, and every quarterturn of a middle slice yields *two* 4-cycles on centers (and one 4-cycle on edges). Therefore, the permutations on corners and centers always have the same parity. Persistent players will discover that any 3-cycle on corners or centers can be obtained without affecting the rest of the cube, so the quadro-super-group Q can be described as

$$Q = \left\{(\varepsilon, \sigma, \kappa, v) \mid \varepsilon, \sigma \in S_{24}, \kappa \in S_7, \right.$$
$$\left. v = (v_1,\dots,v_7) \in C_3^7, \sum_{i=1}^{7} v_i = 0, \text{ sgn } \sigma = \text{sgn } \kappa\right\}.$$

Now we shall treat all these kinds of groups (let us call them *Rubik Groups*) in a unified way, and determine their normal subgroups.

3. GROUPS AND NORMAL SUBGROUPS

For natural numbers n, p with p prime, we define

$$G(n,p) = \left\{(\sigma,v) \mid \sigma \in S_n, v = (v_1,\dots,v_n) \in C_p^n, \sum_{i=1}^{n} v_i = 0\right\},$$

$$H(n,p) = \left\{(\sigma,v) \in G(n,p) \mid \sigma \in A_n\right\},$$

$$V(n,p) = \left\{(1,v) \in G(n,p)\right\}$$

$$Z(n,p) = \left\{(1,v) \in G(n,p) \mid v = (v_1,\dots, v_n) \text{ with } v_1 = v_2 = \dots\dots = v_n\right\}$$

If $(\sigma,v) \in G(n,p)$ then we define $\sigma v \in C_p^n$ by
$(\sigma v)_i = v_{\sigma^{-1}(i)}$ for $i = 1,\dots,n$.
$G(n,p)$ is a *group* by $(\sigma,v)(\bar\sigma,\bar v) = (\sigma\bar\sigma, \sigma\bar v + v)$.
Note that $1 = (1,0)$ and $(\sigma,v)^{-1} = (\sigma^{-1}, -\sigma^{-1}v)$.

It will be convenient to define
$G(n,1) = S_n$,
$H(n,1) = A_n$,
$V(n,1) = Z(n,1) = \{1\}$.

Sometimes we shall write $(\sigma,0)$ instead of σ if $\sigma \in S_n = G(n,1)$ to obtain a unified treatment of $G(n,1)$ and $G(n,p)$ for $p > 1$.

Examples:

$G(8,3)$ is the group of the black edges cube, $G(7,3)$ is the group of the 2×2×2 cube, $G(12,2)$ is the group of the black corners cube, and $H(6,2)$ is the edge group of Meffert's Pyraminx. Note that in each case $V(n,p)$ is the subgroup of transformations that change orientations while keeping every piece on its location. Note also that $Z(8,3) = Z(7,3) = \{1\}$ by the condition that $\Sigma_{i=1}^{n} v_i = 0$, and that $Z(12,2)$ and $Z(6,2)$ consist of the neutral element 1 and the element that flips *every* piece on its place.

In general, we have $Z(n,p) \neq \{1\}$ iff $p > 1$ and $p \mid n$.

Normal subgroups

In the following chain of subgroups

$$\{1\} \subset Z(n,p) \subset V(n,p) \subset H(n,p) \subset G(n,p)$$

each subgroup is *normal* in G(n,p). Recall that a subgroup N is normal in G iff $gNg^{-1} = N$ for all $g \in G$. We shall use the notation $N \triangleleft G$ to express that N is a normal subgroup of G. Beginners often fail to realize that if we have a chain of subgroups $N \subset M \subset G$ and $N \triangleleft G$ then also $N \triangleleft M$, but if $N \triangleleft M$ then *not* necessarily $N \triangleleft G$ holds! This is illustrated by the fact that every subgroup of V(n,p) is normal in V(n,p) (since V(n,p) is abelian), but only {1}, Z(n,p) and V(n,p) are normal in H(n,p) or in G(n,p), as will be shown below.

In the sequel, we shall frequently use the fact that for $n \geq 5$ the alternating group A_n is *simple*, i.e. its only normal subgroups are A_n itself (see, e.g., VAN DER WAERDEN, 1971, p. 163-165).

Normal subgroups of H(n,p)

In theorems 1 and 2 we shall determine all normal subgroups of H(n,p). It may be helpful for the reader to realise the contents of theorem 1 in a concrete case, e.g. the edge group H(6,2) of Meffert's Pyraminx. Then theorem 1 states that if a normal subgroup N contains a transformation that flips some, but not all edge pieces, then $N \supset V(6,2)$, i.e., by conjugation and composition *any* (even) number of flips can be obtained. In the black edges group G(8,3) theorem 1 states that the existence in $N \triangleleft H(8,3)$ of *one* twisting transformation $(1,v) \in V(8,3)$ with $v \neq 0$, forces *all* twisting transformations to be contained in N.

THEOREM 1. *Let* $N \triangleleft H(n,p)$, $p > 1$, $n \geq 5$. *If there is an element* $v = (v_1,\dots,v_n) \in C_p^n$ *such that* $(1,v) \in N$ *and* $v_i \neq v_j$ *for some* i, j *then* $V(n,p) \subset N$.

PROOF. If $(1,w) \in N$ then also $(1,\sigma w) = (\sigma,0)(1,w)(\sigma,0)^{-1} \in N$ for all $\sigma \in A_n$. Thus we may suppose that $v_1 \neq v_2$. Define $e_i = (1,0,\dots,0,-1,0,\dots,0) \in C_p^n$ for $i = 2,\dots,n$ (the i^{th} component of e_i is -1). The elements $(1,e_i)$ generate V(n,p). It thus is sufficient to prove that $(1,e_{i_0}) \in N$ for *one* value $i_0 \in \{2,\dots,n\}$, for then also $(1,\sigma e_{i_0}) \in N$ for all $\sigma \in A_n$.

Take $\rho = (132) \in A_n$, $\tau = (154) \in A_n$, then $(1,v)$, $(1,\rho v)$, $(1,\tau v)$, $(1,\tau\rho v) \in N$ and also $(1, v - \rho v - \tau v + \tau\rho v) \in N$.
But $v - \rho v - \tau v + \tau\rho v = (v_1-v_2,0,0,0,v_2-v_1,\dots,0)$ and since $v_1-v_2 \neq 0$ also $(1,e_5) \in N$. □

THEOREM 2. *Let* $N \triangleleft H(n,p)$, $n \geq 5$.
Then N = {1}, Z(n,p), V(n,p) *or* H(n,p).

PROOF. Since A_n is simple, we may suppose that $p > 1$.

Consider
$$\begin{tikzcd} H(n,p) \arrow[r] & A_n \\ N \arrow[u, hook] \arrow[ur] & \end{tikzcd}$$
(canonical).

Again, since A_n is simple, we have im(N) = {1} or A_n.

Case 1: im(N) = {1}.
Then $N \subset V(n,p)$. If $N \neq \{1\}$ or Z(n,p), then N = V(n,p) by theorem 1.

Case 2: im(N) = A_n.
Take $\sigma = (132) \in A_n$, $w = (1,-1,0,\dots,0) \in C_p^n$. Since im(N) = A_n, there exists a $(\sigma,v) \in N$, so also $(1,w)\,(\sigma,v)\,(1,w)^{-1}\,(\sigma,v)^{-1} = (1,w-\sigma w) \in N$. But $w - \sigma w = (2,-1,-1,0,\dots,0)$, so by theorem 1, $V(n,p) \subsetneq N$.
Consider
$$\{1\} \neq {}^{N}/_{V(n,p)} \triangleleft {}^{H(n,p)}/_{V(n,p)} \xrightarrow{\sim} A_n.$$
Since A_n is simple, it follows that N = H(n,p). □

It will follow from theorem 3 that in fact with theorem 2 we have determined all nontrivial normal subgroups of G(n,p).

Direct products

Consider $G = G(n_1,p_1) \times \dots\dots \times G(n_k,p_k)$.
For each $g = (g_1,\dots,g_k) = ((\sigma_1,v^1),\dots,(\sigma_k,v^k)) \in G$ we shall write $\sigma_i = \text{perm}_i(g)$. Furthermore, we shall frequently write g_i for $(1,\dots,1,g_i,1,\dots,1)$ and G_i, H_i, V_i, Z_i for $G(n_i,p_i)$, $H(n_i,p_i)$, $V(n_i,p_i)$ (n_i,p_i), respectively, and $H = H_1 \times \dots\dots \times H_k$.
Note that the groups
$$R = \left\{(\rho,v,\sigma,w) \mid \rho \in S_{12},\ \sigma \in S_8,\ \text{sgn}\,\rho = \text{sgn}\,\sigma,\ v \in C_2^{12},\ w \in C_3^{8},\ \sum_{i=1}^{12} v_i = \sum_{i=1}^{8} w_i = 0\right\}$$
of Rubik's Cube, and
$$Q = \left\{(\varepsilon,\sigma,\kappa,v) \mid \varepsilon, \sigma \in S_{24},\ \kappa \in S_7,\ \text{sgn}\,\sigma = \text{sgn}\,\kappa,\ v \in C_3^7,\ \sum_{i=1}^{7} v_i = 0\right\}$$
of the modified Master Cube are normal subgroups of $G(12,2) \times G(8,3)$ and $G(24,1) \times G(24,1) \times G(7,3)$, respectively.

THEOREM 3. *Let* $N \triangleleft M$, *where* M *is a subgroup of* $G = G_1 \times \ldots \times G_k$ *and suppose that* $H_1 \subset M$ *and* $n_1 \geq 5$.

(i) *If there is an element* $g \in N$ *with* $\mathrm{perm}_1(g) \neq 1$ *then* $H_1 \subset N$.

(ii) *If there is an element* $g = (g_1,\ldots,g_k) \in N$ *with* $g_1 \in V_1$, $g_1 \notin Z_1$, *then* $V_1 \subset N$.

PROOF. (i) Let $\sigma = \mathrm{perm}_1(g) \in S_{n_1}$. Since $n_1 \geq 5 > 2$, the center of S_{n_1} is trivial, so there exists a $\tau \in A_{n_1}$ with $\tau\sigma\tau^{-1}\sigma^{-1} \neq 1$.
Take $h = (\tau,0) \in H_1$, then $hgh^{-1}g^{-1} = (hg_1h^{-1}g_1^{-1}, 1,\ldots,1) \in H_1 \cap N$ and $\mathrm{perm}_1(hgh^{-1}g^{-1}) = \tau\sigma\tau^{-1}\sigma^{-1} \neq 1$. On account of $H_1 \cap N \triangleleft H_1$ and theorem 2 it follows that $H_1 \cap N = H_1$, so $H_1 \subset N$.
(ii) Let $g_1 = (1,v)$. As in the proof of theorem 1, there exist $\rho, \tau \in A_{n_1}$ such that $(1, v - \rho v - \tau v + \tau\rho\, v) \notin Z_1$.
With $h_\rho = (1,\rho v) = (\rho,0)\ (1,v)\ (\rho,0)^{-1}$,
$h_\tau = (1,\tau v)$ and $h_{\tau\rho} = (1,\tau\rho v)$ we have that
$(h_\rho, g_2,\ldots,g_k)$, $(h_\tau, g_2,\ldots,g_k)$ and $(h_{\tau\rho}, g_2,\ldots,g_k)$ are elements of N, so
$(g_1,\ldots,g_k)(h_\rho, g_2,\ldots,g_k)^{-1}(h_\tau, g_2,\ldots,g_k)^{-1}(h_{\tau\rho}, g_2,\ldots,g_k) =$
$= (g_1h_\rho{}^{-1}h_\tau{}^{-1}h_{\tau\rho}, 1,\ldots,1) \in N \cap H_1$,
thus by theorem 1 we have $V_1 \subset N \cap H_1 \subset N$. □

COROLLARY. *If* $N \triangleleft G(n,p)$ *and* $n \geq 5$ *then* $N = \{1\}$, $Z(n,p)$, $V(n,p)$, $H(n,p)$ *or* $G(n,p)$.

PROOF. This follows from theorem 2, theorem 3 (i) with $k = 1$ and $M = G(n,p)$, and the fact that $H(n,p)$ has index 2 in $G(n,p)$. □

THEOREM 4. *Let* $N \triangleleft H = H_1 \times\ldots\times H_k$, $n_i \geq 5$ *for all* i *and* $p_1 \neq p_i$ *for all* $i > 1$.

If there exists an element $g = (g_1,\ldots,g_k) \in N$ *with* $g_1 \neq 1$ *and* $g_1 \in Z_1$ *then* $Z_1 \subset N$.

PROOF. Note that $p_1 > 1$ for otherwise $\{1\} = Z_1$.
If $g_j \notin Z_j$ for some $j > 1$ then by theorem 3 we have $g_j \in N$, so also $gg_j^{-1} = (g_1,\ldots,1,\ldots g_k) \in N$. Thus we may suppose that $g \in Z_1 \times\ldots\ldots\times Z_k$.
But then

$$g^{p_2\cdots p_k} = (g_1^{p_2\cdots p_k}, 1,\ldots, 1) \in N \cap Z_1$$

and since $g_1 \neq 1$, $g_1 \in Z_1$ and $p_i \neq p_1$ for all $i > 1$, p_1 does not divide the product $p_2\cdots p_k$. Consequently

$g_1^{p_2\cdots p_k} = g^{p_2\cdots p_k} \neq 1$, so $Z_1 \subset N$. □

THEOREM 5. *Let* M *be a subgroup of* $G = G_1\times\ldots\times G_k$ *and* $H = H_1 \times\ldots\times H_k \subset M$. *Suppose* $n_i \geq 5$ *for all* i *and* $(p_i,p_j) = 1$ *if* $i \neq j$.
If $N \triangleleft M$ *and for some* m, $1 \leq m \leq k$,
$N \subset H_1 \times\ldots\times H_m \times G_{m+1} \times\ldots\times G_k$
then $N = N_1 \times\ldots\times N_m \times \bar{N}$, *where*
$N_i = N \cap H_i$ $(i = 1,\ldots,m)$ *and* $\bar{N} = N \cap (G_{m+1}\times\ldots\times G_k)$.

PROOF. Let g is $(g_1,\ldots,g_k) \in N$. If for some i, $1 \leq i \leq m$, $g_i \neq 1$ holds, then from theorems 3 and 4 it follows that $g_i \in N$. □

Finally, we treat the case that $N \triangleleft M$ where $H = H_1\times\ldots\times H_k \subset N$. Then automatically $N \triangleleft G$ since G/H is abelian.

For any $g = (g_1,\ldots,g_k) \in G$ we define $\mathrm{sgn}(g) \in \mathbb{F}_2^k$ by

$$(\mathrm{sgn}(g))_i = \begin{cases} 0 & \text{if } \mathrm{perm}_i(g) \in A_{n_i} \\ 1 & \text{otherwise} \end{cases}$$

Then by the homomorphism $g \mapsto \mathrm{sgn}(g)$ we have $G/_H \simeq \mathbb{F}_2^k$ so any normal subgroup N, $H \subset N \subset G$, corresponds uniquely with a linear subspace of $\mathbb{F}_2^k$.
From this we also see that the number $I(k)$ of normal subgroups N with $H \subset N \subset G$ only depends on k and not on the special nature of the groups $G(n_i,p_i)$.
This number is equal to

$$I(k) = 1 + \sum_{i=1}^{k} \frac{(2^k-1)(2^k-2)\ldots.(2^k-2^{i-1})}{(2^i-1)(2^i-2)\ldots.(2^i-2^{i-1})}.$$

Indeed, for $1 \leq i \leq k$, there are $(2^k-1)(2^k-2)\ldots(2^k-2^{i-1})$ ordered sets of i independent vectors in $\mathbb{F}_2^k$ and each i-dimensional subspace contains $(2^i-1)(2^i-2)\ldots(2^i-2^{i-1})$ of these sets. For instance, we have $I(1) = 1+1 = 2$, $I(2) = 1+3+1 = 5$ and $I(3) = 1+7+7+1 = 16$.

4. EXAMPLES AND FINAL REMARKS

Rubik's Cube

In $G_1 = G(12,2)$ we have the normal subgroups

$\{1\} \subset Z(12,2) \subset V(12,2) \subset H(12,2) \subset G(12,2)$,

and in $G_2 = G(8,3)$

$$\{1\} \subset V(8,3) \subset H(8,3) \subset G(8,3)$$

(note that $3 \nmid 8$, so $Z(8,3) = \{1\}$).

Thus in $G = G_1 \times G_2$ we have $5 \times 4 = 20$ normal subgroups N of the form $N = N_1 \times N_2$ with $N_1 \triangleleft G_1$ and $N_2 \triangleleft G_2$. Since $I(2) = 5$, there are 5 normal subgroups N with $H \subset N$, but four of these, viz. $H_1 \times H_2$, $H_1 \times G_2$, $G_1 \times H_2$ and $G_1 \times G_2$, are among the 20 mentioned above. The remaining one is R, the group of Rubik's Cube: $R = \{g \in G_1 \times G_2 | \mathrm{sgn}(\mathrm{perm}_1(g)) = \mathrm{sgn}(\mathrm{perm}_2(g))\}$. Its image in $\mathbb{F}_2^2$ is $\{(0,0), (1,1)\}$.

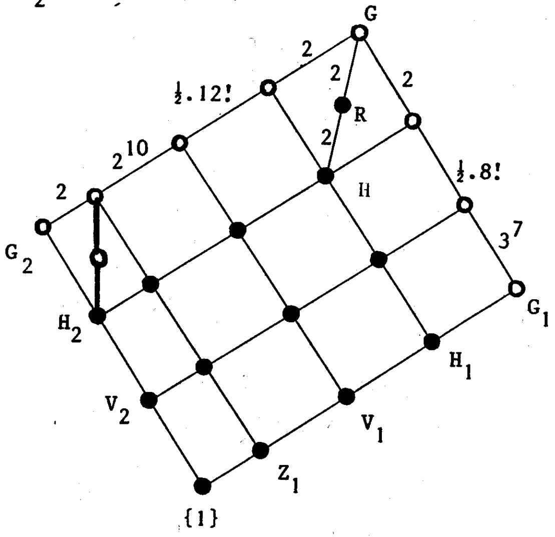

fig.5 The 21 normal subgroups of G(12,2) x G(8,3); the black vertices are the 13 normal subgroups of the group R of Rubik's Cube

The 21 normal subgroups of $G_1 \times G_2$ are shown in fig. 5, where two normal subgroups are connected by an ascending path iff the lower one is contained in the upper one. The black vertices show the 13 normal subgroups of R. This part of the diagram is also shown (without proof) in VAN DE CRAATS, 1981, p. 86.

The Master Cube

Let $G_1 = G_2 = G(24,1) = S_{24}$, $G_3 = G(7,3)$, then we have

$$\{1\} \subset H_1 = H_2 \subset G_1 = G_2 \text{ and}$$

$$\{1\} \subset V_3 \subset H_3 \subset G_3$$

(note that $Z_1 = Z_2 = V_1 = V_2 = Z_3 = \{1\}$). Thus in $G = G_1 \times G_2 \times G_3$ we have $3 \times 3 \times 4 = 36$ normal subgroups of the form $N = N_1 \times N_2 \times N_3$ with $N_i \triangleleft G_i$.

Furthermore, with the notations

$$D_{ij} = \{g_i g_j | g_i \in G_i, g_j \in G_j, \mathrm{sgn}(\mathrm{perm}_i(g_i)) = \mathrm{sgn}(\mathrm{perm}_j(g_j))\} (i \neq j),$$

$$D_{123} = \{g \in G| \mathrm{sgn}(\mathrm{perm}_1(g)) = \mathrm{sgn}(\mathrm{perm}_2(g)) = \mathrm{sgn}(\mathrm{perm}_3(g))\},$$

$$E_{123} = \{g \in G| \text{ if } g \notin H, \text{ then exactly } \underline{\text{two}} \text{ of the } \mathrm{perm}_i(g) \text{ are odd}\},$$

we have the following 'mixed' normal subgroups of G:

$\{1\} \times D_{23}$, $H_1 \times D_{23}$, $G_1 \times D_{23}$,

$\{1\} \times D_{13}$, $H_2 \times D_{13}$, $G_2 \times D_{13}$,

$D_{12} \times \{1\}$, $D_{12} \times V_3$, $D_{12} \times H_3$, $D_{12} \times G_3$,

D_{123} and E_{123},

adding to a total of $36 + 12 = 48$ normal subgroups of G. Among these, $Q = G_1 \times D_{23}$ is the quadro-super-group. This group has 22 normal subgroups, as shown in fig. 6.

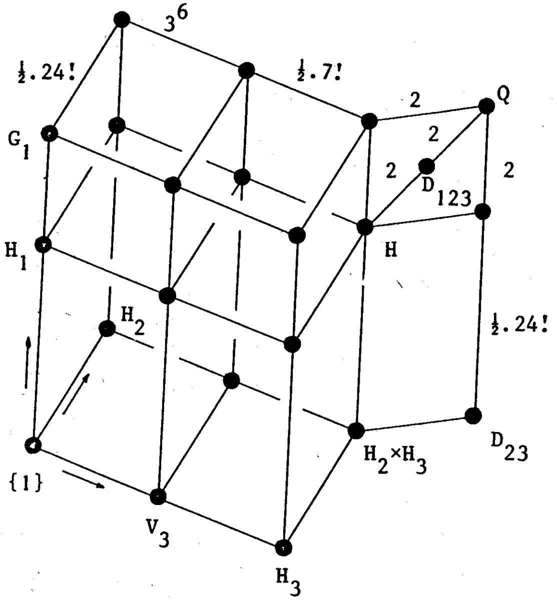

fig.6 The 22 normal subgroups of the quadro-super-group, the group of the modified Master Cube of fig.4

The setting of section 3 is general enough for our main purpose: to get a complete list of the normal subgroups of R and Q. Of course, similar methods also can be applied under less restrictive conditions, but then the results mostly will be less simple. If, for instance, in theorem 5 we drop the condition that all primes $p_i > 1$ be distinct, then more 'mixed' normal subgroups will arise. The same is true if not all n_i are ≥ 5. The reader might like to verify that theorem 1 remains true if $n = 2$ or $n = 4$, but is false if $n = 3$ and $p \equiv 1 \bmod 3$. Also, if in $G(n,p)$ the integer p is not a prime, complications will arise.

We did not strive for the utmost generality. Instead, we tried to illustrate various concepts and methods from an attractive part of elementary group theory. From our theorems other results can be obtained easily. For example, the commutator subgroup of $G = G_1 \times \ldots \times G_k$ is $H = H_1 \times \ldots \times H_k$, being the smallest normal subgroup with an abelian factor group. Also, if $H \subset M \subset G$ then it is easy to see that $Z = Z_1 \times \ldots \times Z_k$ is the *center* of M, i.e. the collection of all z for which $zm = mz$ for all $m \in M$.

REFERENCES

BERLEKAMP, E.R., J.H. CONWAY & R.K. GUY, 1982, *Winning Ways*, Academic Press, London.

FREY, A. & D. SINGMASTER, 1982, *Handbook of Cubik Math*, Enslow Publ., Hillside, NJ.

SINGMASTER, D. 1980, *Notes on Rubik's Magic Cube*, Fifth Edition, London.

VAN DE CRAATS, J. 1981, *De Magische Kubus van Rubik*, De Muiderkring, Bussum.

VAN DER WAERDEN, B.L. 1971, *Algebra I*, Achte Auflage, Springer Verlag.