ALGEBRAIC TILING

S. K. STEIN

A variety of problems concerning number theory, tiling Euclidean space by cubes or by cross-shaped clusters of cubes, coding theory, and gambling, have led to questions in group theory, usually involving finite, or at least finitely generated, abelian groups. We shall discuss some of these problems, their history, and, when convenient, some details of their algebraic solutions. A reader who is familiar with vector spaces and with the quotient groups and homomorphisms of abelian groups will be able to follow the presentation without trouble. It is hoped, in particular, that the discussion will be accessible to upper-division students.

1. Preliminaries. The words "tiling" or "tesselation" usually call to mind congruent copies of a triangle or of a convex quadrilateral tiling the plane. Perhaps "tiling" may remind us of the herringbone pattern composed of translates of an L-shaped set in brick pavements. In any case, copies of some set by some collection of motions fill up another set without overlap (except perhaps along common borders).

Several types of tiling will concern us. In one case, we consider tilings of Euclidean n-space R^n by translates of a cube or by translates of a certain union of a finite number of cubes. The union of these translates will be R^n and the interiors of distinct translates will not intersect.

Secondly, we shall be involved with a group G and two subsets of G: A and B, such that each element of G is uniquely expressible in the form ab, $a \in A$, $b \in B$. We may think of G as being tiled by copies of B or, symmetrically, by copies of A. We shall write $G = (A, B)$, and speak of a **factoring** of G by subsets A and B.

Another important type of tiling is the following: Let G be an abelian group written additively, and $\{s_1, s_2, \cdots, s_k\}$ a set of integers. Each s_i determines a function $\bar{s}_i\colon G \to G$ by $\bar{s}_i(g) = s_i g = g + g + \cdots + g$, s_i times if s_i is positive, and $(-g) + (-g) + \cdots + (-g)$, $|s_i|$ times if s_i is negative. If each non-zero element of G is uniquely expressible in the form $\bar{s}_i b$ for b in some fixed set $B \subseteq G$ and some i, we write

$$G - \{0\} = \{s_1, s_2, \cdots, s_k\} : B$$

and say "$\{s_1, s_2, \cdots, s_k\}$ **splits** $G - \{0\}$". In this case, $G - \{0\}$ is tiled by k copies of B.

In special cases, the splitting of a group is equivalent to the factoring of a different group. To be specific, let p be a positive prime integer and let $C(p)$ be the additive group of the integers modulo p. Assume that $\{s_1, s_2, \cdots, s_k\}$ splits $C(p) - \{0\}$. Let Z_p be the field of integers modulo p and let G_p be its multiplicative group. Then we have the factoring

$$G_p = (\{s_1, s_2, \cdots, s_k\}, B).$$

For instance, since $C(13) - \{0\} = \{\pm 1, \pm 2\} : \{1, 3, 4\}$, we have

$$G_{13} = (\{\pm 1, \pm 2\}, \{1, 3, 4\}).$$

Before going on to the tilings that we shall treat in detail (all of which concern commutative structures), let us illustrate the notion of a tiling by showing how a purely combinatorial problem can lead to a problem concerning the tiling of a nonabelian group.

Consider the set of $n!$ linear arrangements of the integers $1, 2, \cdots, n$. Call two such arrangements **adjacent** if one is obtainable from the other by a single transposition. The question is:

Is there a set B of arrangements of $1, 2, \cdots, n$ such that each of the $n!$ arrangements is in B or adjacent to precisely one member of B?

The case $n = 2$ is the only one for which the answer is known to be "yes". Since there are $n(n-1)/2$ arrangements adjacent to a given one, the set B, if it exists, would have

$$\frac{n!}{1 + n(n-1)/2}$$

elements. So, it is necessary that $1 + n(n-1)/2$ divide $n!$. Consequently, if $1 + n(n-1)/2$ is divisible by a prime that is larger than n, then the answer is "no". Rothaus and Thompson [**1**] obtained this stronger result:

THEOREM. *If $1 + n(n-1)/2$ is divisible by a prime that is larger than $2 + \sqrt{n}$, then there does not exist a set B of arrangements of $1, 2, \cdots, n$ such that each of the $n!$ arrangements of $1, 2, \cdots, n$ is either in B or adjacent to precisely one member of B.*

As stated, the theorem is purely combinatorial. To obtain their result, Rothaus and Thompson rephrased the problem in terms of factoring the symmetric group S_n:

Let T be the set of transpositions, together with the identity permutation, in the symmetric group S_n. Is there a subset B of S_n such that (T, B) is a factoring of S_n?

Rothaus and Thompson used the theory of group representations to obtain their result. The original question has still not been completely answered.

THE MINKOWSKI-HAJÓS PROBLEM

The next five sections follow the evolution of a problem of Minkowski, from its origins in number theory, through its resolution in abelian groups, and then describes the problems that grew out of the solution.

2. Minkowski's conjecture. The most dramatic work in factoring, that of Hajós [7] in 1942, solved a problem that Minkowski [**12**] raised in 1907. Minkowski first considered a question in number theory, quickly transformed it to one about vectors, and this to a problem about tiling space with congruent cubes. Hajós expressed this problem in terms of factoring a finite abelian group and solved it. Let us follow these transitions in detail, which in total are almost as startling as the metamorphosis of a caterpillar to a butterfly.

The original problem concerns the simultaneous approximation of several real numbers by rational numbers:

Let $a_1, a_2, \cdots, a_{n-1}$ *and* $t > 1$ *be real numbers. Do there exist integers* $x_1, x_2, \cdots, x_n$ *such that* $0 < x_n < t^{n-1}$ *and*

$$\left|a_1 - \frac{x_1}{x_n}\right| < \frac{1}{x_n t}, \left|a_2 - \frac{x_2}{x_n}\right| < \frac{1}{x_n t}, \cdots, \left|a_{n-1} - \frac{x_{n-1}}{x_n}\right| < \frac{1}{x_n t}? \tag{2.1}$$

The case $n = 2$, for instance, concerns the approximation of a single real number a_1 by a rational number x_1/x_2 such that $|a_1 - x_1/x_2| < 1/x_2 t$ and $0 < x_2 < t$. (Note that these two inequalities imply that $|a_1 - x_1/x_2| < 1/x_2^2$.) If $t = 2$, and $a_1 = \frac{1}{2}$, then x_2 would have to be 1 and the inequality $|a_1 - x_1/x_2| < 1/x_2 t$ could not be satisfied. However, as will be shown later, if t is not an integer (2.1) can be satisfied.

We shall follow the evolution of the problem in terms of the specific case $n = 3$, for it illustrates the essentials for arbitrary n and is easier to describe.

Minkowski's question for $n = 3$ may be rephrased, after the clearing of denominators, as follows:

Let a_1, a_2, *and* $t > 1$ *be real numbers. Do there exist integers* x_1, x_2, x_3, *not all* 0, *such that*

$$\begin{aligned} &|tx_1 + 0x_2 - a_1 t x_3| < 1 \\ &|0x_1 + tx_2 - a_2 t x_3| < 1 \\ &|0x_1 + 0x_2 + (1/t^2)x_3| < 1? \end{aligned} \tag{2.2}$$

The determinant of the 3-by-3 matrix formed from (2.2) by removing x_1, x_2, x_3 has the value 1. So, Minkowski raised this more general question:

Let

$$\begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix} \tag{2.3}$$

be a real matrix with determinant 1. *When do there exist integers* x_1, x_2, x_3, *not all* 0, *such that*

$$\begin{aligned} &|b_{11}x_1 + b_{12}x_2 + b_{13}x_3| < 1 \\ &|b_{21}x_1 + b_{22}x_2 + b_{23}x_3| < 1 \\ &|b_{31}x_1 + b_{32}x_2 + b_{33}x_3| < 1? \end{aligned} \tag{2.4}$$

Such integers x_1, x_2, x_3 do not always exist. For example, the only integral solution of

$$\begin{aligned} |1x_1 + b_{12}x_2 + b_{13}x_3| &< 1 \\ |0x_1 + \phantom{b_{12}}1x_2 + b_{23}x_3| &< 1 \\ |0x_1 + \phantom{b_{12}}0x_2 + \phantom{b_{13}}1x_3| &< 1 \end{aligned}$$

is $(0,0,0)$. Clearly, x_3 must be 0, then $x_2 = 0$, finally $x_1 = 0$. To find the extra condition on the matrix (2.3) that would guarantee a nontrivial solution for the inequalities (2.4), Minkowski transformed the question into a geometric one.

Observe that the three column vectors

$$v_1 = \begin{bmatrix} b_{11} \\ b_{21} \\ b_{31} \end{bmatrix} \quad v_2 = \begin{bmatrix} b_{12} \\ b_{22} \\ b_{32} \end{bmatrix} \quad v_3 = \begin{bmatrix} b_{13} \\ b_{23} \\ b_{33} \end{bmatrix}$$

span a parallelepiped whose volume is 1. For convenience we shall identify a vector with the point whose coordinates are the components of the vector. The question now reads:

Let v_1, v_2, and v_3 be three vectors in R^3 that span a parallelepiped of volume 1. *When are there integers x_1, x_2, x_3, not all* 0, *such that the vector*

$$x_1v_1 + x_2v_2 + x_3v_3 \tag{2.5}$$

lies in the **interior** *of the* 2 *by* 2 *by* 2 *cube C whose edges are parallel to the axes and whose center is the origin*?

If, instead of demanding that $x_1v_1 + x_2v_2 + x_3v_3$ lie in the interior of C, we ask only that it lie in C—perhaps on the surface of C—then Minkowski showed that the answer is "always". His argument goes like this: Let D be the 1 by 1 by 1 cube whose edges are parallel to the axes and whose center is the origin. Form the set of all translates of D by vectors of the form (2.5). (Note that x_1, x_2, x_3 are integers.) Such a set of translates, we shall call a lattice of translates.

Pair off each point of the form (2.5) with the parallelepiped obtained by translating by that vector the parallelepiped P spanned by v_1, v_2, v_3. Since the volume of P is 1, the number of points of the form (2.5) in a large region of volume V (say, similar to P) is approximately V. Thus there are approximately V translates of the unit cube C in that region. Since C has volume 1, these translates cannot be disjoint—they must overlap, perhaps only at their surface. Hence there are two vectors v and v^* of the form (2.5) such that

$$(v + C) \cap (v^* + C) \neq \varnothing,$$

hence also two points c and c^* in C such that $v + c = v^* + c^*$, or

$$v - v^* = c^* - c. \tag{2.6}$$

Now $c^* - c$ is in the cube D and $v - v^*$ is a non-zero vector of the form (2.5). Thus inequalities (2.4), with $<$ replaced by $\leqq$, do have a non-trivial solution.

As observed above, if

$$v_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \quad v_2 = \begin{bmatrix} b_{12} \\ 1 \\ 0 \end{bmatrix} \quad v_3 = \begin{bmatrix} b_{13} \\ b_{23} \\ 1 \end{bmatrix},$$

inequalities (2.4) have only the trivial solution. More generally, if the vectors

$$u_1 = \begin{bmatrix} c_{11} \\ c_{21} \\ c_{31} \end{bmatrix} \quad u_2 = \begin{bmatrix} c_{12} \\ c_{22} \\ c_{32} \end{bmatrix} \quad u_3 = \begin{bmatrix} c_{13} \\ c_{23} \\ c_{33} \end{bmatrix} \tag{2.7}$$

are simply another basis for the lattice spanned by

$$v_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \quad v_2 = \begin{bmatrix} b_{12} \\ 1 \\ 0 \end{bmatrix} \quad v_3 = \begin{bmatrix} b_{13} \\ b_{23} \\ 1 \end{bmatrix}, \tag{2.8}$$

then the inequalities

$$\begin{aligned} |c_{11}x_1 + c_{12}x_2 + c_{13}x_3| &< 1 \\ |c_{21}x_1 + c_{22}x_2 + c_{23}x_3| &< 1 \\ |c_{31}x_1 + c_{32}x_2 + c_{33}x_3| &< 1 \end{aligned} \tag{2.9}$$

have no non-zero integer solution. This leads to Minkowski's conjecture, which we state for dimension 3.

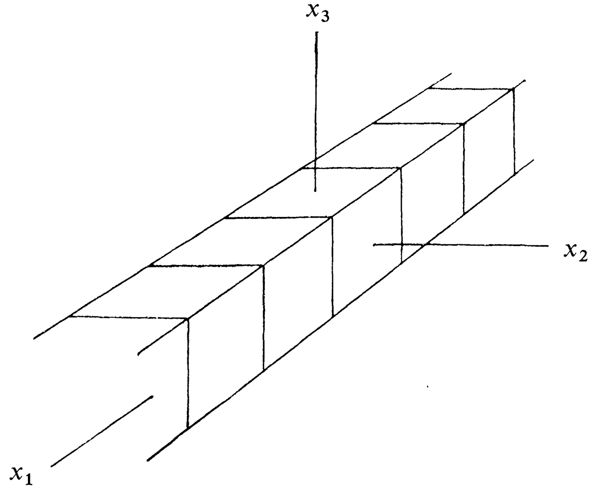
Minkowski's Conjecture. Let (c_{ij}) be a three-by-three matrix whose determinant is 1. If the only integral solution of inequalities (2.9) is $(0,0,0)$, then the lattice spanned by (2.7) can also be spanned by vectors of the form (2.8) (or vectors differing from (2.8) only by changing the role of the three axes).

The validity of this conjecture would imply that all entries in at least one row of the matrix (c_{ij}) would have to be integers. In particular, if t is not an integer, inequalities (2.2) would have a non-zero solution. In other words, Equations (2.4) have only the trivial solution $(0,0,0)$ if and only if the real matrix (2.3) of determinant 1 is unimodularly equivalent to a triangular matrix with ones on the diagonal. (For the case where t is an integer see **[11]** pp. 109–110.)

Minkowski also expressed his conjecture geometrically. The assertion that a lattice of translates of the unit cube C has a basis of, say, the form

$$v_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \quad v_2 = \begin{bmatrix} b_{12} \\ 1 \\ 0 \end{bmatrix} \quad v_3 = \begin{bmatrix} b_{13} \\ b_{23} \\ 1 \end{bmatrix},$$

implies, first of all, that the unit cube whose center is $(1, 0, 0)$ is present in the lattice of translates. This means that the two unit cubes whose centers are $(0, 0, 0)$ and $(1, 0, 0)$ *share a complete two-dimensional face.* Since a lattice is homogeneous—every cube in it playing the same role—the lattice must be composed of files of cubes, parallel to the x_1 axis: one such (endless) file is shown in this figure:



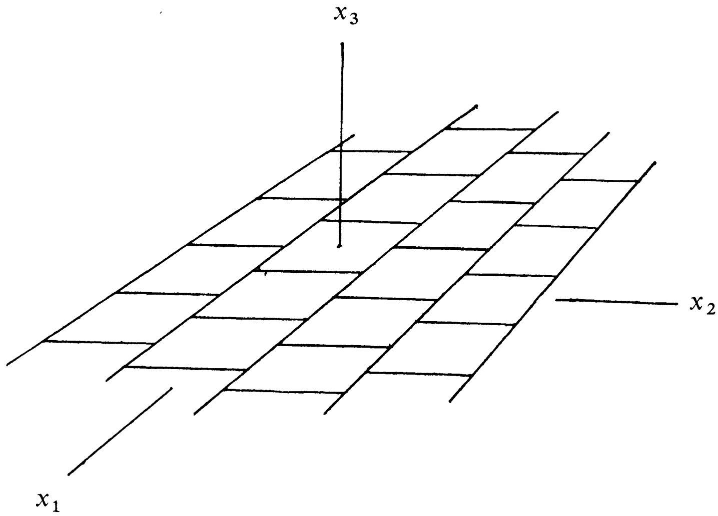
The presence of the vector

$$v_2 = \begin{bmatrix} b_{12} \\ 1 \\ 0 \end{bmatrix}$$

is then equivalent to the existence of another file of cubes at the same height, tangent to the first array, but perhaps slid along the x_1 direction. Hence the tiling of R^3 includes a tiling of the slab $|x_3| \leqq \frac{1}{2}$, as shown in the figure on page 451.

Translates of this slab make up the original tiling of R^3. In other words, the tiling of R^3 can be built step by step, cubes forming files, then files forming slabs. This is how Minkowski's conjecture for general n reads in geometric terms:

MINKOWSKI'S CONJECTURE (**geometric form**): *If a lattice of unit cubes tiles R^n, then some pair of cubes share a complete $(n-1)$-dimensional face.*

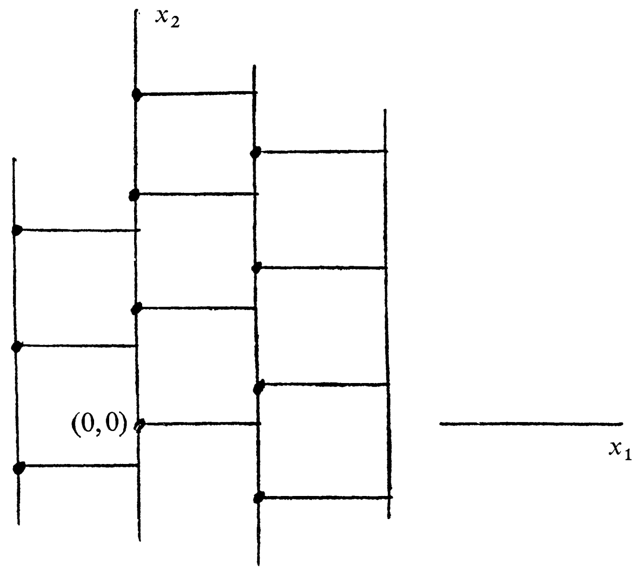


This formulation appears in [12, p. 74]. The problem, in arithmetic form, was raised eleven years earlier [11, §37].

3. Hajós' confirmation of Minkowski's conjecture. Minkowski easily settled his conjecture for $n = 2$ or 3. Jansen in 1909 [9] took care of $n = 4$, 5, and 6. In 1930, Keller [10] generalized the conjecture by removing the assumption that the cubes form a lattice. Using only the assumption that parallel unit cubes tile R^n, he proved that for any two of the cubes there is a coordinate axis such that along that axis the coordinates of their midpoints differ by an integer. Reviewing the work done up to 1940, Perron [13] remarked, "I must confess that in most of the papers I came to one or more places where I could not follow the line of reasoning. So I do not really know how far the assertions are in fact proved. Partly, but not completely, this may be because I lack the slightest intuitive picture of n-dimensional space, an insight with which the other authors seem to be endowed." In this paper, Perron verifies Keller's version of Minkowski's conjecture for $n \leqq 6$ and reduces the problem for any dimension n to a finite one concerning 2^n parallel unit cubes whose centers are located in a special way in the 2^n unit cubes that compose a cube of side 2. And there he left the problem, whose complexity grows rapidly with the dimension.

Soon after, in 1942, Hajós [7] settled Minkowski's conjecture, where it is assumed that the cubes form a lattice, after first casting it into the form of an equivalent conjecture about finite abelian groups. We shall describe this final formulation, but refer the reader to Fuchs [6, pp. 318–323] for the simplest exposition of Hajós' proof, which depends on the group ring of a finite abelian group with integer coefficients.

Let us consider only the case $n = 2$, the plane, for it illustrates the general idea and is easy to draw. Imagine, then, that the plane is tiled by a lattice of unit squares parallel to the coordinate axes. Describe the location of each square by its lower left corner. These points form a group L^*.



First of all, Hajós reduced the general case to that in which the points in L^* have rational coordinates. A linear transformation of the form $(x, y) \to (m_1 x,\ m_2 y)$, where m_1 and m_2 are positive integers, distorts L^* to a subgroup L whose points have integer coordinates and simultaneously transforms the unit squares to m_1 by m_2 rectangles, still parallel to the axes.

This is now the situation. We have the group H of all points with integer coordinates and a subgroup L, which consists of the lower left corners of a family of m_1 by m_2 rectangles that tile the plane. Hajós then expressed Minkowski's conjecture in terms of the quotient group $G = H/L$.

Let $u_1 = (1,0)$ and $u_2 = (0,1)$ be the standard unit vectors in H. Let $a_1 = u_1 + L$ and $a_2 = u_2 + L$ be the corresponding elements in $G = H/L$. (We write the elements of G multiplicatively and those of H additively.)

The assumption that the rectangles tile the plane is composed of two conditions: that they cover the plane and that they do not overlap (except at their borders).

The assumption that the m_1 by m_2 rectangles cover the plane reads, in terms of the group H, as follows:

For any element $h \in H$, there are an element $l \in L$ and integers e_1 and e_2, $0 \leqq e_i < m_i$, $i = 1, 2$, such that

$$h = l + e_1 u_1 + e_2 u_2.$$

In terms of the quotient group, this reads: Every element $g \in G$ can be written in the form

$$g = a_1^{e_1} a_2^{e_2}, \qquad 0 \leqq e_i < m_i, \qquad i = 1,2.$$

The assumption that the m_1 by m_2 rectangles do not overlap reads, in terms of H: If $l_1 \in L$ and $l_2 \in L$, and $0 \leqq e_i,\ e_i' < m_i$, $i = 1,2$, and

$$l_1 + e_1 u_1 + e_2 u_2 = l_2 + e_1' u_1 + e_2' u_2,$$

then $e_1 = e_1'$ and $e_2 = e_2'$. In terms of G this condition reads:

$$\text{If } a_1^{e_1} a_2^{e_2} = a_1^{e_1'} a_2^{e_2'},\ 0 \leqq e_i,\ e_i' < m_i,\ i = 1,2, \text{ then } e_i = e_i',\ i = 1,2.$$

The assumptions of Minkowski's conjecture are now expressed completely in terms of the group G (which, incidentally, has $m_1 m_2$ elements). How does the conclusion read?

Imagine that two rectangles share a complete edge parallel, say, to the x_2-axis. There is no loss of generality in assuming that the common edge is the right edge of the rectangle whose lower left corner is at the origin. Thus

$$m_1 u_1 \in L.$$

In terms of G, this assertion is expressed in the equation

$$a_1^{m_1} = 1.$$

This suggests Hajós' translation of Minkowski's conjecture in n-space:

(3.1) *Let G be a finite abelian group and let $a_1, a_2, \cdots, a_n$ be n elements of G. Let the order of a_i be at least m_i, $i = 1, 2, \cdots, n$. Assume that each element of G is uniquely expressible in the form*

$$a_1^{e_1} a_2^{e_2} \cdots a_n^{e_n},$$

$0 \leqq e_i < m_i$, $i = 1, 2, \cdots, n$. *Then there is at least one integer i such that $a_i^{m_i} = 1$.*

This theorem concerns the factorization of the group G into n sets,

$$G = (\{1, a_1, \cdots, a_1^{m_1 - 1}\},\ \{1, a_2, \cdots, a_2^{m_2 - 1}\}, \cdots, \{1, a_n, \cdots, a_n^{m_n - 1}\}),$$

and asserts that at least one of the factors is a group. It was in this form that Minkowski's problem was finally solved.

4. Hajós generalized. With Hajós' solution of Minkowski's problem, interest in tiling by congruent cubes disappeared. No one seems to have pursued Keller's conjecture which removes the "lattice" assumption nor his problem concerning 2^n cubes in n-space.

But Hajós' theorem did inspire new questions and new work. Perhaps the most interesting is Rédei's generalization [**15**] in 1965 of Hajós' theorem, where the factors are no longer required to be "front ends" of cyclic groups.

RÉDEI'S THEOREM. *Let G be a finite abelian group and let $A_1, A_2, \cdots, A_m$ be subsets of G, each of which contains the identity element and each has prime order. Assume that G is factored*

$$G = (A_1, A_2, \cdots, A_m)$$

in the sense that each element of G is uniquely expressible as a product

$$a_1 a_2 \cdots a_m,$$

$a_i \in A_i$. *Then at least one A_i is a group.*

(It is not hard to reduce Hajós' theorem to the case where each m_i is prime. So Rédei's is indeed a generalization of Hajós'.)

Wittman [22] in 1969 simplified part of Rédei's proof, the important case where $G = C(p) \times C(p)$, the square of a cyclic group of prime order. Both Rédei and Wittman used characters of abelian groups, the factorization of polynomials, and, as did Hajós, the group ring.

Moving in another direction, Bernstein [2] generalized Hajós' theorem to finite nonabelian groups in which every cyclic subgroup of composite order is normal.

5. Good groups. Hajós' theorem also raised questions about the form of factorizations. Let us look at just one of them, which was answered over a period of fifteen years in a series of papers by Hajós [8], Rédei [14], Sands [18, 19, 20, 21], and de Bruijn [4, 5].

Hajós calls a subset A of a finite abelian group G **periodic** if there is an element g in G, other than the identity element, such that $gA = A$. (The conclusion of Hajós' theorem is equivalent to the assertion that one of the sets

$$\{1, a_i, a_i^2, \cdots, a_i^{m_i - 1}\}$$

is periodic.) Observe that a subset A is periodic if and only if there is a subgroup H of G, $|H| > 1$, such that A has a factorization, $A = (H, B)$.

In [8] Hajós proved that if G is a cyclic group of prime power order, $C(p^n)$, and $G = (A, B)$, then at least one of the subsets A and B is periodic. Rédei [14] obtained the same conclusion when G is of the form $C(p) \times C(p)$. These papers helped initiate the search for "good" groups. A finite abelian group G is **good** if in each factorization $G = (A, B)$, at least one of A and B is periodic. Sands [20], summarizing the efforts of several mathematicians, provided this complete list of the good groups:

$$(p^n, q),\ (p^2, q^2),\ (p^2, q, r),\ (p, q, r, s)$$

$$(p^3, 2, 2),\ (p^2, 2, 2, 2),\ (p, 2^2, 2),\ (p, 2, 2, 2, 2)$$

$$(p, q, 2, 2),\ (p, 3, 3),\ (3^2, 3),\ (2^n, 2)$$

$$(2^2, 2^2),\ (p, p),$$

and their subgroups. Here, p, q, r, s denote distinct primes; in each case p may equal 2. The notation $(a, b, \cdots, c)$ is short for the direct product $C(a) \times C(b) \times \cdots \times C(c)$.

Along the way, many side results were obtained. For instance, Sands [**18**] proved that if a finite cyclic group G is factored, $G = (A, B)$, and $|A|$ is a power of a prime, then A or B is periodic. In [**19**], Sands proved that if the finite abelian group G is factored, $G = (A, B)$, $|A|$ is a power of a prime, and if $(|A|, |B|) = 1$, then there is a subgroup H in G such that $G = (A, H)$. It is not known whether the assumption that the order of A is a prime power is necessary.

6. Another relation to geometric tiling problems. The preceding section was concerned with the relation of a factor of G to some subgroup H of G. The first such theorem is Lagrange's, which asserts that any subgroup H of G is a factor of G. Similar questions and results are to be found in the theory of convex bodies. For instance, for any convex body in the plane a densest packing by translates is provided by a *lattice* packing.

Zassenhaus in [**23**] remarked, concerning a different geometric problem, "It is highly interesting to observe that one of the densest X-admissible point sets turns out to be a 'lattice with a base', i.e., a point set which is the union of a finite number of translates of a geometric lattice...the fact that (vaguely formulated) optimal discrete distributions tend to be lattices with a base has been known to every scientist interested in solid state physics since Bragg's and von Laue's discoveries. ...Is it reasonable to assume that lattices with a base form a pattern of optimal packings?" Zassenhaus was presumably referring to the fact that when a liquid solidifies it tends to form a crystal which usually is the configuration that minimizes the total internal energy.

One algebraic analog of this expectation, for tilings rather than for packings in general, runs as follows. Let $G = Z \times Z \times \cdots \times Z$, the free abelian group with n generators (the analog of n-dimensional Euclidean space) with addition coordinatewise. Let A be a finite subset of G. Assume that there is a set B such that $G = (A, B)$. Is there then a subgroup H of G and a *finite* set S in G such that $G = (A, H, S)$? The set $H + S$ is the analog of "a lattice with a base". The answer is not known. In [**33**] is an example of a symmetric star body that tiles R^{10} as a lattice with a base but not as a lattice. Robinson [**17**] exhibited 32 finite subsets of $Z \times Z$ whose translates tile $Z \times Z$ but do not tile $Z \times Z$ in any way that resembles a lattice with a base. The general question for translates of a single finite subset of $Z \times Z$ remains open.

Tiling by Certain Star Bodies

The theory of convexity contains many results on tiling, packing, and covering by translates of a convex body. If the interiors of a family of convex bodies in Euclidean space are pairwise disjoint, the family is called a **packing**; if the union of the family is all of the space, the family is called a **covering**. Thus a tiling by convex bodies is simultaneously a packing and a covering. We will also speak of lattice tilings. First of all, a family of vectors form a **lattice** if they are a group under addition and have no accumulation point. In a **lattice tiling**, the tiling family consists of the translates of a fixed convex body by the vectors of a lattice. The body is said to tile in a **lattice manner**. These definitions extend from convex bodies to star bodies. (A star body contains a point from which the entire body is "visible".) Two types of star bodies, called "crosses" and "semi-crosses", are of special interest, in part because their tiling problems, though fairly general, can be treated algebraically, and in part because of their appearance in combinatorial and coding theory. The next two sections concerns these star bodies.

7. Tiling Euclidean space by crosses or semi-crosses. Let k and n be positive integers. Any translate of the $kn+1$ unit n-dimensional cubes whose edges are parallel to the coordinate axes and whose centers are the $kn+1$ points specified by the n-tuples

$$(0,0,\cdots,0),\ (j,0,\cdots,0),\cdots,(0,0,\cdots,j),$$

$j = 1,2,\cdots,k$, is called a (k,n)-**semi-cross**. A (k,n)-semi-cross consists of n arms of length k attached at facets of a "corner" cube.

A (k,n)-**cross** is any translate of the $2kn+1$ unit cubes whose centers are at the $2kn+1$ points specified by the n-tuples

$$(0,0,\cdots,0),\ (\pm j,0,\cdots,0),\cdots,\ (0,0,\cdots,\ \pm j),$$

$j = 1,2,\cdots,k$. The (k,n)-cross is centrally symmetric.

We shall assume, unless otherwise stated, that in the tilings by crosses or semi-crosses, the centers of the cubes have integer coordinates. Essentially we are replacing R^n by Z^n. The next few theorems, which suggest the type of algebraic problems such tilings raise, are taken from Stein [**32**].

Theorems 7.1 and 7.3 show why lattice tilings by semi-crosses or crosses are specially amenable to algebraic treatment.

THEOREM 7.1. *The (k,n)-semi-cross tiles R^n in a lattice manner if and only if the set $\{1,2,\cdots,k\}$ splits an abelian group G of order $kn+1$, that is*

$$G-\{0\} = \{1,2,\cdots,k\}:\{g_1,g_2,\cdots,g_n\}, \tag{7.2}$$

where $\{g_1,g_2,\cdots,g_n\} \subseteq G$.

Proof. Let Z^n be the free abelian group with n generators. If the (k,n)-semi-cross tiles Z^n in a lattice manner, let H be the subgroup of Z^n occupied by the centers of the corners of the semi-crosses. Let G be the quotient group Z^n/H. Let $f\colon Z^n \to G$ be the natural homomorphism and let $g_j = f(E_j)$ where E_j is the basic unit vector in the jth direction, $E_j = (0,\cdots,0,1,0,\cdots,0)$, a 1 in the jth coordinate. Note that Z^n is the union of the $kn+1$ cosets of the form $c+H$, where c is a center of a cube in the semi-cross whose corner is at the origin. Thus, as c runs through the $kn+1$ points iE_j, $1 \leqq i \leqq k$, $1 \leqq j \leqq n$, together with the origin, $f(c)$ runs through the elements of G. Thus we have the splitting,

$$G - \{0\} = \{1, 2, \cdots, k\} : \{g_1, g_2, \cdots, g_n\}.$$

Conversely, assume that G is an abelian group of order $kn+1$ and that each non-zero element is of the form ig_j, $1 \leqq i \leqq k$, $1 \leqq j \leqq n$. Define $f: Z^n \to G$ to be the unique homomorphism such that $f(E_j) = g_j$ and let H be the kernel of f. Then, as may be checked directly, the set of semi-crosses whose corner cubes have their center in H constitute a tiling of R^n.

In a similar manner, it can be shown that the (k,n)-cross tiles R^n in a lattice manner if and only if the set $\{\pm 1, \pm 2, \cdots, \pm k\}$ splits an abelian group of order $2kn+1$. In both these results, call G "the quotient group of the tiling". In particular, since $C(13) - \{0\} = \{\pm 1, \pm 2\} : \{1, 3, 4\}$, the $(2,3)$-cross tiles R^3.

So the question, "when does a (k,n)-semi-cross or cross tile R^n in a lattice manner," is reduced to a question concerning the splitting of finite abelian groups. Either question is far from being answered. The following two theorems represent only the first steps toward a complete solution.

THEOREM 7.3. ([**32**, Theorem 4.8]). *If p is a prime, then the $(p-1, n)$-semi-cross tiles R^n in a lattice manner for an infinitude of n such that $(p-1)n+1$ is prime.*

The next theorem shows that a semi-cross or cross can tile a given space in many geometrically distinct ways. Preprints are available from the authors.

THEOREM 7.4. (W. Hamaker-S.K. Stein). *Let p be an odd prime, b an integer greater than 1, and $n = (p^b - 1)/(p-1)$. Then the $(p-1, n)$-semi-cross tiles R^n and the $((p-1)/2, 2n)$-cross tiles R^{2n} in a lattice manner. Moreover, any abelian group of order p^b can be prescribed as the quotient group of either tiling.*

Theorem 7.4 shows, for instance, that the $(2,4)$-semi-cross tiles R^4 with quotient group $C(9)$ and also $C(3) \times C(3)$. There are in fact at least two geometrically inequivalent lattice tilings with quotient group $C(9)$. One has its corners at

$$\{(x_1, x_2, x_3, x_4) \mid x_1 + 4x_2 + 7x_3 + 3x_4 \equiv 0\,(9)\}$$

and the other at

$$\{(x_1, x_2, x_3, x_4) \mid x_1 + 4x_2 + 7x_3 - 3x_4 \equiv 0\,(9)\}.$$

With the aid of Theorem 7.1 and its companion for crosses, it is easy to show that the $(1,n)$-semi-cross tiles R^n with any abelian group of order $n+1$ as quotient group and that the $(1,n)$-cross tiles R^n with any abelian group of order $2n+1$ as quotient group.

Among the many questions suggested by these theorems, we state just two. In a geometric tiling of R^n by crosses (parallel to the axes), one of which has its center at the origin, must the centers of all the crosses have integer coordinates? (For the $(1,3)$-semi-cross in R^3, the answer is "no".)

Secondly, if a (k,n)-semi-cross tiles R^n, $n \geqq 3$, is k bounded in terms of n? In [**32**] it was shown that in the case of a lattice tiling, where $kn+1$ is prime, then $k < 2n-2$. Hamaker [**26**] removed the assumption that $kn+1$ is prime. For crosses, a bound is known for any tiling, [**32**, Theorem 3.2].

8. Combinatorial and coding problems. Problems in packing, covering, or tiling by figures closely related to semi-crosses or crosses have appeared independently in such separate fields as combinatorics and coding theory.

The combinatorial case goes back to a gambling problem first investigated by Taussky and Todd [**34**] in 1948. This is their description of the problem: "A bettor tries to forecast the results of 13 games (win, loss, or tie). He 'knows' the results of 9, say. But the remaining 4 are uncertain. To make sure of getting the remaining 4 right, he would have to make 3^4 entries. But if he thinks 12 right will be the best submitted, he asks what is the smallest number of entries which will ensure that no matter what happens he will have at least 3 right out of 4."

This question suggested a general combinatorial problem:

Let X be a set with q elements and let n be a positive integer. Let S be the n-fold cartesian product, $X \times X \times \cdots \times X$. How small a subset $B \subseteq S$ can be found such that each element of S differs from some element of B in at most one coordinate?

(The gambler's problem is the case $q = 3$ and $n = 4$.) The minimal size of B is usually denoted $\sigma(n,q)$. Since a given point in S differs in exactly one coordinate from $n(q-1)$ points, clearly

$$\sigma(n,q) \geqq \frac{q^n}{n(q-1)+1}.$$

If S is pictured as an n-dimensional chess board of side q, then the set B can be interpreted as a minimal set of castles that attack or occupy every cube of the board.

At the outset, the combinatorial question was cast in algebraic terms. Let

$$G = C(q) \times C(q) \times \cdots \times C(q), \ n \text{ times}.$$

Let $A \subseteq G$ be the $n(q-1)+1$ elements

$$(0,0,\cdots,0),\ (i,0,\cdots,0),\ (0,i,0,\cdots,0),\cdots,(0,\cdots,0,i) \tag{8.1}$$

$1 \leqq i \leqq q-1$. Then the combinatorial question now reads:

How small a subset B can be found in G such that $A + B = G$?

The symbol $A + B$ denotes the set of elements of the form $a + b$, a in A and b in B.

Since it is *not* assumed that each element of G is uniquely of the form $a + b$, this question concerns covering, not tiling. However, most of the early work was devoted to the special case of finding a factoring; in this case $n(q-1)+1$ must divide q^n. The first general result in this direction is due independently to Zaremba [**35**] and Mauldon [**31**] in 1951:

THEOREM 8.2. *Let p be a prime number, let a be an integer larger than* 1, *and let $n = (p^a - 1)/(p-1)$. Then the group $G = [C(p)]^n$ has a tiling $G = (A, B)$, where A is prescribed in* (8.1).

Proof. Each non-zero element of $H = [C(p)]^a$ has order p. Select a non-zero element g_1. It generates a group G_1 of order p. Select g_2 not in G_1. It generates a group G_2 of order p that meets G_1 only in the element 0. Continuing in this way, select elements $g_1, g_2, \cdots, g_n$ such that

$$H - \{0\} = \{1, 2, \cdots, p-1\} : \{g_1, g_2, \cdots, g_n\}.$$

Next define a homomorphism

$$f: [C(p)]^n \to [C(p)]^a$$

by mapping $(0, \cdots, 1, \cdots, 0)$—where 1 is the ith place—onto g_i. Then $(A, f^{-1}(0))$ is a factoring of $G = [C(p)]^n$.

Theorem 8.2 includes the particular problem of the gambler when $p = 3$, $a = 2$, and $n = (p^2 - 1)/(p-1) = 4$, showing that $3^4/[4(3-1)+1] = 9$ forecasts suffice.

Zaremba [**36**] also treated the case where q is a power of a prime. For convenience, we include the short proof published in 1969 by Losey [**30**].

THEOREM 8.3. *Let q be a power of a prime p, let a be an integer larger than* 1, *and let $n = (q^a - 1)/(q-1)$. Then the group $G = [C(q)]^n$ has a tiling (A, B) where A is prescribed in* (8.1).

Proof. The vector space V^a of dimension a over the Galois field GF(q) is the union of $n = (q^a - 1)/(q-1)$ lines through the origin. On each line, select a point g_i other than the origin. Let V^n be the vector space of dimension n over GF(q) and define a linear map

$$T: V^n \to V^a$$

by setting

$$T(0, \cdots, 1, \cdots, 0) = g_i,$$

(where a 1 is in the ith place and 0's elsewhere). Then it can be shown directly that

$$G = (A, T^{-1}(0)),$$

where G is considered as the additive group of V^n.

Note that G in the preceding proof is *not* $[C(q)]^n$. The additive structure of V^n is the n-fold sum of the additive group of GF(q), hence the sum of copies of $C(p)$. The set $T^{-1}(0)$ is *not* a subgroup of $[C(q)]^n$ (unless q is itself a prime). This is a consequence of the following theorem, due to Zaremba [**36**].

THEOREM 8.4. *If q is composite, the group $G = [C(q)]^n$ has no factoring of the type (A,B), where A is prescribed in* (8.1) *and B is a group.*

Proof. Assume that in such a factorization B is a group. Let

$$f: G \to G/B$$

be the natural homomorphism. The ith axis of G,

$$\{(0,\cdots,x,\cdots,0) \mid x \in C(q),\ x \text{ in the } i\text{th place}\},$$

is a subgroup of G. Let $H_i \subseteq G/B$ be the image of the ith axis under the homomorphism f. Then

$$G/B = H_1 \cup H_2 \cup \cdots \cup H_n$$

and any pair of the H_i's meet only at the element 0 in G/B. Each H_i is isomorphic to $C(q)$.

As Baer observes in [**24**, p. 337], if a finite abelian group H is expressed as the union of at least two subgroups, any two of which meet only at $\{0\}$, then every non-zero element of H has the same order.

[To show this, assume $H = A \cup B \cup C \cup \cdots$. Let $a \in A - \{0\}$ and $b \in B - \{0\}$. Assume $mb = 0$. We shall show $ma = 0$. Clearly, $a + b \notin A \cup B$, hence is in a subgroup C that meets A and B only at $\{0\}$. Hence $m(a + b) \in C$. But $m(a + b) = ma \in A$. Thus $ma = 0$. From this it follows that all non-zero elements of A and of B have the same order, which, being non-zero, must be a prime.]

The factorings of $[C(q)]^n$ in Theorems 8.2 and 8.3 provide tilings of R^n by $(q-1,n)$-semi-crosses and, if q is odd, by $((q-1)/2, 2n)$-crosses). If q is prime the tiling is by a lattice. If q is a power of a prime, but not prime, the tiling is by a lattice with a base.

The problem of tiling $[C(q)]^n$ arose, as we saw, from a combinatorial covering problem. The same problem is of importance in coding theory, where it grew out of a packing, rather than covering, problem.

In the coding case, X is a set of q "symbols" and X^n is the set of q^n "messages" of length n that can be written with those symbols. Assume that when a message of length n is transmitted, at most one of the n symbols is received erroneously. Therefore, when a message m is sent, any of $1 + n(q - 1)$ sequences can be received. Call this set of possibilities $A(m)$. Because of the possible ambiguity, the sender and the receiver must agree in advance on a list of possible messages, called "code words," $m_1, m_2, \cdots, m_k$ such that for $i \neq j$, $A(m_i)$ and $A(m_j)$ are disjoint. When each m_i is again interpreted as the position of a castle, no two of the k castles must attack the same point. Instead of a (minimal) covering problem, we have come to a (maximal) packing problem. The two problems become identical if we insist that the covering have no overlap and the packing fill X^n. Codes that meet this stringent demand are called "perfect single-error correcting codes." For a survey of the construction of such codes, see van Lint [**28**, **29**].

References

1. O. Rothaus and J. G. Thompson, A combinatorial problem in the symmetric group, Pacific J. Math., 18 (1966) 175–178.

Minkowski-Hajós

2. H. J. Bernstein, Extension of Hajós' factorization theorem to some non-abelian groups, Comm. Pure Appl. Math., 21 (1968) 289–311.

3. H. Davenport, Recent progress in the geometry of numbers, Proc. Int. Congr. Math., (1950) 166–174.

4. N. G. de Bruijn, On the factorization of finite abelian groups, Indag. Math. Kon. Ned. Akad. Wetensch. Amsterdam, 15 (1953) 258–264.

5. ———, On the factorization of cyclic groups, *ibid.*, 370–377.

6. L. Fuchs, Abelian Groups, Pergamon Press, 1967.

7. G. Hajós, Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einen Würfelgitter, Math. Zeit., 47 (1942) 427–467.

8. ———, Sur la factorisation des groupes abéliens, Časopis Pěst. Mat. Fys., 74 (1949) 157–162.

9. H. Jansen, Lückenlose Ausfüllung des R_n mit gitterförmig angeordneten n-dimensionalen Quadern, Dissertation Kiel, 1909.

10. O. H. Keller, Über die lückenlose Einfüllung des Raumes mit Würfeln, J. Reine Angew. Math., 163 (1930) 231–248.

11. H. Minkowski, Geometrie der Zahlen, Leipzig, 1896.

12. ———, Diophantische Approximationen, Leipzig, 1907.

13. O. Perron, Über lückenlose Ausfüllung des n-dimensionalen Raumes durch kongruente Würfel, Math. Zeit., 46 (1940) 1–26, 161–180.

14. L. Rédei, Zwei Lücken Sätze über Polynome in endlichen Primkörpern mit Anwendung auf die endlichen Abelschen Gruppen und die Gausseschen Summen, Acta Math., 79 (1947) 273–290.

15. ———, Die neue Theorie der endlichen abelschen Gruppen und Verallgemeinerung des Hauptsatzes von Hajós, Acta Math. Acad. Sci. Hung., 16 (1965) 329–373.

16. ———, Berichtigung zu meiner Arbeit, "Die neue Theorie der endlichen abelschen Gruppen und Verallgemeinerung des Hauptsatzes von Hajós", Acta Math. Acad. Sci. Hung., 17 (1966) 46.

17. R. M. Robinson, Undecidability and nonperiodicity for tilings of the plane, Invent. Math., 12 (1971) 177–209.

18. A. D. Sands, On the factorization of finite abelian groups, Acta Math., 8 (1957) 65–86.

19. ———, On a problem of L. Fuchs, J. Lond. Math. Soc., 37 (1962) 277–284.

20. ———, On the factorizations of finite abelian groups, II, Acta Math., 13 (1962).

21. ———, Factorization of cyclic groups, Proc. Colloq. Abelian Groups, Hungary, Sept. 1963, (1964).

22. E. Wittman, Einfacher Beweis des Hauptsatzes von Hajós-Rédei für elementare Gruppen von Primzahlquadratordnung, Acta Math. Sci Acad. Hung., 20 (1–2) (1969) 227–230.

23. H. Zassenhaus, Modern developments in the theory of numbers, Bull. Amer. Math. Soc., 67 (1961) 426–439.

Tiling by Certain Star Bodies

24. R. Baer, Partitionen endlichen Gruppen, Math. Zeitschr., 75 (1961) 333–372.

25. J. P. Conlan, Tiling space with the aid of the holomorph, J. Comb. Theory, 14 (1973) 167–172.

26. W. Hamaker, Factoring groups and tiling space, Aequationes Math., to appear.

27. M. Herzog and J. Schönheim, Group partition, factorization, and the vector covering problem, Canad. Math. Bull., 15 (1972) 207–214.

28. J. H. van Lint, Coding Theory, Lecture Notes in Mathematics, 201, Springer, 1971.

29. ———, A survey of perfect codes, Rocky Mountain Jour. Math., to appear.

30. G. Losey, Note on a theorem of Zaremba, J. Comb. Theory, 6 (1969) 208–209.

31. J. G. Mauldon, Covering theorems for groups, Quart. J. Math. Oxford (2), 1 (1950) 284–287.

32. S. K. Stein, Factoring by subsets, Pacific J. Math., 22 (1967) 523–541.

33. ———, A symmetric star body that tiles but not as a lattice, Proc. Amer. Math. Soc., 36 (1972) 543–548.

34. O. Taussky and J. Todd, Covering theorems for groups, Ann. Soc. Polonaise de Math., 21 (1948) 303–305.

35. S. K. Zaremba, A covering theorem for abelian groups, J. London Math. Soc., 26 (1951) 71–72.

36. ———, Covering problems concerning abelian groups, J. London Math. Soc., 27 (1952) 242–246.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, DAVIS, CALIFORNIA 95616.

FOLIATIONS OF 3-MANIFOLDS

MAURICE COHEN

The theory of foliations has its roots in the study of differential equations in the nineteenth century and has recently been a very active area of topology. The modern theory started in 1944 and until 1969 the most striking examples and theorems were all concerning foliations of codimension one on the 3-sphere and other 3-manifolds. The statements of these results of G. Reeb, A. Haefliger, S. Novikov and J. Wood, all of which will be discussed, are very geometric and within reach of the imagination and our usual 3-dimensional intuition (together with a few drawings). The definition of foliation will be vague at first and made gradually precise. We shall begin with a few words about ordinary differential equations in the plane and the statement of the Poincaré-Bendixson theorem, so that it later becomes clear how foliations generalize differential equations and how questions about foliations arise naturally from the study of the qualitative behavior of solutions of ordinary differential equations.

For our purposes, a differential equation in the plane is given by a system