NISTIR 88-3777

Finite Unions of Closed Subgroups of the n-Dimensional Torus

Jim Lawrence

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
(Formerly National Bureau of Standards)
Center for Computing and Applied Mathematics
Mathematical Analysis Division
Gaithersburg, MD 20899

August 1988

National Bureau of Standards became the National Institute of Standards and Technology on August 23, 1988, when the Omnibus Trade and Competitiveness Act was signed. NIST retains all NBS functions. Its new programs will encourage improved use of technology by U.S. industry.

U.S. DEPARTMENT OF COMMERCE
C. William Verity, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Ernest Ambler, Director

NISTIR 88-3777

Finite Unions of Closed Subgroups of the n-Dimensional Torus

Jim Lawrence

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
(Formerly National Bureau of Standards)
Center for Computing and Applied Mathematics
Mathematical Analysis Division
Gaithersburg, MD 20899

August 1988

FINITE UNIONS OF CLOSED SUBGROUPS OF THE N-DIMENSIONAL TORUS

by Jim Lawrence

Center for Applied Mathematics
National Bureau of Standards

and

George Mason University

Abstract

Let U be an open subset of the torus group T^n. We show that the set of maximal subgroups of T^n which miss U is of finite cardinality. This result is applied to show that the lattice of finite unions of closed subgroups of T^n is a complete distributive lattice, and to show that, up to unimodular equivalence, there are only finitely many convex polytopes $P \subseteq \mathbb{R}^n$ having vertices in $\mathbb{Z}^n$ but no interior points in $\mathbb{Z}^n$ and such that each subgroup G of the additive group $\mathbb{R}^n$ which properly contains $\mathbb{Z}^n$ does have points in common with the interior of P.

FINITE UNIONS OF CLOSED SUBGROUPS
OF THE N-DIMENSIONAL TORUS

by Jim Lawrence

1. Introduction.

Let $x = (x_1, \ldots, x_n)$ be an element of $\mathbb{R}^n$ and let $U \subseteq \mathbb{R}^n$ be an open neighborhood of 0. A classical theorem of Dirichlet asserts that there exist a positive integer m and a point $z = (z_1, \ldots, z_n) \in \mathbb{Z}^n$ such that $mx - z \in U$. The numbers $x_1, \ldots, x_n$ and 1 are independent over the rational numbers if there is no $w \in \mathbb{Z}^n \sim \{0\}$ such that $\langle w, x \rangle \in \mathbb{Z}$. A classical theorem of Kronecker asserts that the numbers $x_1, \ldots, x_n$, and 1 are independent over the rational numbers if and only if for every open set $U \subseteq \mathbb{R}^n$ there exist a positive integer m and $z \in \mathbb{Z}^n$ such that $mx - z \in U$. (These are Theorems 201 and 442 of [4]. See also Chapter VII of [1].)

In this paper we consider, for open sets $U \subseteq \mathbb{R}^n$, the nature of the sets $\tilde{\tau}(U) = \{x \in \mathbb{R}^n :$ there exist $m \in \mathbb{Z}$ and $z \in \mathbb{Z}^n$ such that $mx - z \in U\}$. (Alternatively, $\tilde{\tau}(U) = \{x \in \mathbb{R}^n :$ the (additive) group generated by $\{x\} \cup \mathbb{Z}^n$ intersects $U\}$.) We show that $\mathbb{R}^n \sim \tilde{\tau}(U)$ is a finite union of closed subgroups of $\mathbb{R}^n$; and moreover, the set $M(\mathbb{R}^n, U)$ of maximal subgroups G of $\mathbb{R}^n$ such that $G \cap U = \emptyset$ and $\mathbb{Z}^n \subseteq G$, is finite. This is Corollary 1.A, below.

As an example, let $n = 2$ and let $U = \{(x, y) \in \mathbb{R}^2 : 0 < x, 0 < y, \text{ and } x + y < 1\}$. Then the subgroups H of $\mathbb{R}^2$ such that $\mathbb{Z}^2 \subseteq H$ and $H \cap U = \emptyset$ are precisely the subgroups of the following four groups:

$$H_1 = \{(x, y) \in \mathbb{R}^2 : x \in \mathbb{Z}\},$$
$$H_2 = \{(x, y) \in \mathbb{R}^2 : y \in \mathbb{Z}\},$$
$$H_3 = \{(x, y) \in \mathbb{R}^2 : x + y \in \mathbb{Z}\}, \text{ and}$$
$$H_4 = \{(x, y) \in \mathbb{R}^2 : 2x \in \mathbb{Z} \text{ and } 2y \in \mathbb{Z}\}.$$

One of several interesting consequences of the general finiteness result concerns subsets of the n-dimensional torus group T^n. It is obvious that these subsets form a finitely distributive lattice under the operations of intersection and union. It follows from the finiteness result that they actually form a complete lattice: The intersection of an arbitrary family of finite unions of closed subgroups of T^n is again a finite union of closed subgroups of T^n. (We will have occasion in this paper to use the word "lattice" in two different senses: We will use it as we have in this paragraph, to mean a partially ordered set with certain properties; we will also use it in its sense in the geometry of numbers, to mean a discrete, full-dimensional subgroup of $\mathbb{R}^n$. The useage must be ascertained from the context.)

In Section 3 we present some consequences of these results concerning finiteness of certain sets of unimodular equivalence classes of polytopes with integer vertices.

This paper uses standard results concerning additive subgroups of $\mathbb{R}^n$. The best reference for this topic for our purposes is Chapter VII of [1].

2. Preliminaries.

Let $\mathscr{G}$ be the lattice of closed subgroups G of $\mathbb{R}^n$ such that $\mathbb{Z}^n \subseteq G$. (We could equivalently work with closed subgroups of the torus group $T^n = \mathbb{R}^n/\mathbb{Z}^n$ in view of the bijective correspondence $G \to \pi(G)$ mapping the set of such subgroups to the set of subgroups of T^n, where $\pi : \mathbb{R}^n \to T^n$ is the canonical map. We prefer to remain in $\mathbb{R}^n$ in order to make easy use of results from the geometry of numbers.)

Let $\overline{\mathscr{G}}$ be the lattice of closed subgroups of $\mathbb{R}^n$. For $G \in \overline{\mathscr{G}}$, let $G^* = \{ x \in \mathbb{R}^n : \langle x, u\rangle \in \mathbb{Z}$ for each $u \in G\}$. Then G^* is also in $\overline{\mathscr{G}}$ and the map $G \to G^*$ is an anti-automorphism of $\overline{\mathscr{G}}$. (See [1].)

The lattice $\mathscr{G}$ satisfies the descending chain condition; that is, each non-empty subset of $\mathscr{G}$ possesses a minimal element. Equivalently, any chain $H_1 \supseteq H_2 \supseteq \ldots$ of distinct elements of $\mathscr{G}$ must be finite. To see this note that $H_1^* \subseteq H_2^* \ldots$ would be an ascending chain of subgroups of $(\mathbb{Z}^n)^* = \mathbb{Z}^n$, which satisfies the ascending chain condition, since it is a finitely generated abelian group.

For $S \subseteq \mathbb{R}^n$, let $\mathrm{pol}(S) = \{x \in \mathbb{R}^n : \langle x, y\rangle \leq 1$ for each $y \in S\}$. Then $\mathrm{pol}(S)$ is a closed, convex set which contains the origin; $\mathrm{pol}(\mathrm{pol}(S))$ is the smallest closed, convex set which contains $S \cup \{0\}$; and pol is a dual automorphism of the partially ordered set of closed, convex sets containing the origin.

Our objective now is to establish a lemma (Lemma 3) which will be used in the proof in the next section of the main result.

LEMMA 1. Suppose that U is a convex subset of $\mathbb{R}^n$ and that $p \in U$. If H is a subgroup of $\mathbb{R}^n$ such that $H \cap (1/n\ (U - p))$ contains a basis for $\mathbb{R}^n$ then $H + U = \mathbb{R}^n$.

Proof. Let $\{b_1, \ldots b_n\}$ be a basis for $\mathbb{R}^n$ contained in $H \cap (1/n\ (U - p))$. Let $P = \{\sum \alpha_i b_i : 0 \leq \alpha_i \leq 1$ for $i = 1, \ldots, n\}$. Then $P \subseteq \text{conv}\{0, nb_1, \ldots, nb_n\} \subseteq U - p$. Any $x \in \mathbb{R}^n$ can be expressed in terms of the basis: $x = \sum \alpha_i b_i$, $i = 1, \ldots, n$. We then have:

$$x = \sum \lfloor \alpha_i \rfloor b_i + \sum (\alpha_i) b_i \in H + P,$$

so $H + P = \mathbb{R}^n$. (Here $\lfloor \alpha \rfloor$ denotes the greatest integer less than or equal to α and $(\alpha) = \alpha - \lfloor \alpha \rfloor$ is the fractional part of α.) It follows that $H + (U - p) = \mathbb{R}^n$; i.e., $H + U = \mathbb{R}^n$. □

In the proof of Lemma 2 we will use a result of Mahler belonging to the theory of successive minima. Recall that for a lattice $L \subseteq \mathbb{R}^n$, and a full-dimensional, compact, convex set K symmetric about the origin, the successive minima $\lambda_1, \ldots, \lambda_n$ of L with respect to K are the smallest real numbers such that (for each i) $(\lambda_i K) \cap L$ contains a set of i linearly independent points.

Let $\lambda_1, \ldots,$ and λ_n be the successive minima of L with respect to K (as above) and let $\lambda_1^*, \ldots,$ and λ_n^* be the successive minima of L^* with respect to pol(K). Mahler's result is that (for each i) one has

$$1 \le \lambda_i \lambda_{n-i+1}^* \le n!.$$

(In Mahler's original result, the right-hand bound was $(n!)^2$. The statement as we have it is Theorem VI of Chapter VIII, Section 5, of [2]. The right-hand bound has been spectacularly improved by Lagarias, Lenstra, and Schnorr in [5].)

LEMMA 2. *Let K be a full-dimensional, convex, compact set with $K = -K$. Let H be a closed subgroup of $\mathbb{R}^n$ such that $H \cap K$ does not contain a basis for $\mathbb{R}^n$. Then $H^* \cap (n!\ \mathrm{pol}(K))$ contains a non-zero element.*

Proof. Suppose that there is a convex, full-dimensional, compact set K symmetric about 0 and a closed subgroup H such that $H \cap K$ contains no basis for $\mathbb{R}^n$ and $H^* \cap (n!\ \mathrm{pol}(K)) = \{0\}$. We may choose a basis $\{x_1, \ldots, x_n\}$ for $\mathbb{R}^n$ such that

$$H = \{ \sum_{i=1}^{n} \alpha_i x_i : \alpha_i \in \mathbb{Z} \text{ for } i = a+1, \ldots, b,$$
$$\text{and } \alpha_i = 0 \text{ for } i = b+1, \ldots, n\}.$$

Let L_m be the lattice generated by $\{x_1/m, \ldots, x_a/m, x_{a+1}, \ldots, x_b, mx_{b+1}, \ldots, mx_n\}$. It is clear that we may choose m sufficiently large that $L_m \cap K$ contains no basis for $\mathbb{R}^n$, and $L_m^* \cap (n!\ \mathrm{pol}(K)) = \{0\}$. Let $\lambda_1, \ldots, \lambda_n$, $\lambda_1^*, \ldots$, and λ_n^* be the successive minima for L_m with respect to K and for L_m^* with respect to $\mathrm{pol}(K)$, respectively. Since $L_m \cap K$ contains no basis for $\mathbb{R}^n$, we have $\lambda_n > 1$. Also $L_m^* \cap (n!\ \mathrm{pol}(K)) = \{0\}$, so $\lambda_1^* > n!$. This contradicts Mahler's Theorem, since then $\lambda_n\lambda_1^* > n!$. □

LEMMA 3. <u>Let G be a closed subgroup of $\mathbb{R}^n$. Let U be a subset of G which contains a non-empty relatively open set. Then there is a bounded set $X \subseteq \mathbb{R}^n$ such that if H is a closed subgroup of G for which $H + U \neq G$ then $H^* \cap X$ is not contained in G^*.</u>

Proof. It is clear that, if $\lambda : \mathbb{R}^n \to \mathbb{R}^n$ is a nonsingular linear transformation, then the statement holds for a given group G and open set $U \subseteq G$ if and only if it holds for the images $\lambda(G)$ and $\lambda(U)$. We may therefore suppose that

$$G = \{ (x_1, \ldots, x_n) \in \mathbb{R}^n : x_{a+1}, \ldots, x_b \in \mathbb{Z} \text{ and } x_{b+1} = \ldots = x_n = 0\},$$

where a and b are integers for which $0 \leq a \leq b \leq n$.

Let

$$A = \{ (x_1, \ldots, x_n) \in \mathbb{R}^n : x_i = 0 \text{ unless } i \leq a\},$$

$$B = \{ (x_1, \ldots, x_n) \in \mathbb{R}^n : x_i = 0 \text{ unless } a < i \leq b\},$$

and

$$C = \{ (x_1, \ldots, x_n) \in \mathbb{R}^n : x_i = 0 \text{ unless } b < i\};$$

and let $\alpha : \mathbb{R}^n \to A$, $\beta : \mathbb{R}^n \to B$, and $\gamma : \mathbb{R}^n \to C$ be the obvious projections. Then we may write

$$G = \{ x \in \mathbb{R}^n : \beta(x) \in \mathbb{Z}^n \text{ and } \gamma(x) = 0\}, \text{ and}$$

$$G^* = \{ x \in \mathbb{R}^n : \alpha(x) = 0 \text{ and } \beta(x) \in \mathbb{Z}^n\}.$$

Let $P = \{ x \in \mathbb{R}^n : \alpha(x) = \gamma(x) = 0 \text{ and } 0 \leq \beta(x) < 1\}$. Note that $P \cap G^* = \{0\}$. If G is a discrete group, so that $a = 0$, then we may take $X = P$. Otherwise, let W be the unit ball in A: $W = \{ x \in A : \|x\| \leq 1\}$. Let $p \in U$ and choose ϵ sufficiently small that $\epsilon W \subseteq \frac{U - p}{a}$. Finally, let $X = (a!/\epsilon).W + P$. Clearly X is bounded.

Suppose H is a closed subgroup of G such that $H + U \neq G$. We will show that $(H^* \cap X) \sim G^* \neq \emptyset$.

Suppose $\beta(H)$ is properly contained in $\beta(G) = \mathbb{Z}^n \cap B$. It follows that $H + A + C$ $(= \beta^{-1}(\beta(H))$) is properly contained in $G + A + C$, so that $H^* \cap B = (H + A + C)^*$ properly contains $(G + A + C)^* = G^* \cap B = \mathbb{Z}^n \cap B$. Choose $x \in (H^* \cap B) \sim (G^* \cap B)$; say,

$x = (0, \ldots, 0, x_{a+1}, \ldots, x_b, 0, \ldots, 0)$. Then $\tilde{x} = (0, \ldots, 0, \lfloor x_{a+1} \rfloor, \ldots, \lfloor x_b \rfloor, 0, \ldots, 0) \in \mathbb{Z}^n \cap B \subseteq H^* \cap B$, so $x - \tilde{x}$ is a nonzero element of P which is in H^*. Therefore $x - \tilde{x} \in (H^* \cap X) \sim G^*$.

Finally, suppose $\beta(H) = \beta(G)$. If $a\epsilon W + (H \cap A) = A$ then $a\epsilon W + H = G$ so $U + H \supseteq (a\epsilon W + p) + H = G$, contrary to our assumption. Therefore $a\epsilon W + (H \cap A) \neq A$, and we see by invoking Lemma 1 that $\epsilon W \cap H$ contains no basis for A. By Lemma 2 applied to A there is a nonzero vector in

$$(n!/\epsilon)W \cap (H \cap A)^* = (n!/\epsilon)W \cap (H^* + B + C);$$

i.e., we may find $x \in H^*$ such that $\alpha(x) \in (n!/\epsilon)W$, $\alpha(x) \neq 0$. Suppose $x = (x_1, \ldots, x_n)$. Then $\tilde{x} = (0, \ldots, 0, \lfloor x_{a+1} \rfloor, \ldots, \lfloor x_b \rfloor, x_{b+1}, \ldots, x_n) \in H^*$ (since H^* contains G^*), and $x - \tilde{x}$ is the required element of $(H^* \cap X) \sim G^*$. □

3. Main Results and Corollaries.

Let G be a closed subgroup of $\mathbb{R}^n$. Suppose $U \subseteq G$. We shall call U full if its intersection with each closed subgroup H of G is empty or contains a relatively open, non-empty subset of H. In particular, open sets are full.

THEOREM 1. *Suppose G is a closed subgroup of $\mathbb{R}^n$ and U is a full subset of G. Let $M(G, U)$ be the set of maximal subgroups $H \subseteq G$ such that $\mathbb{Z}^n \subseteq H$ and $H \cap U = \emptyset$. Then $M(G, U)$ is of finite cardinality.*

Proof. Let Γ denote the set of all closed subgroups G of $\mathbb{R}^n$ containing $\mathbb{Z}^n$ for which there exists a full subset $U \subseteq G$ $M(G, U)$ is infinite. Suppose $G \in \Gamma$ and U is a corresponding full subset. Clearly $U \neq \emptyset$. By Lemma 3 there is a bounded set $X \subseteq \mathbb{R}^n$ such that if H is a closed subgroup of G such that $H + U \neq G$ then $H^* \cap X \not\subseteq G^*$. If $H \in M(G, U)$ then $H + U \neq G$ (since $0 \notin H + U$), so for such H there is $b \in (H^* \cap X) \sim G^*$. It follows that

$$M(G, U) \subseteq \bigcup_b M(G_b, U_b),$$

where the union is taken over $b \in (H^* \cap X) \sim G^*$, $G_b = \{ x \in G : \langle x, b\rangle \in \mathbb{Z}\}$, and $U_b = U \cap G_b$. Notice that, for each such b, G_b is a proper subgroup of G (since $b \notin G^*$). Also, since $\mathbb{Z}^n \subseteq H$, it follows that $H^* \subseteq \mathbb{Z}^n$, so $H^* \cap X$ is finite. It follows that $M(G_b, U)$ is of infinite cardinality for some $b \in (H^* \cap X) \sim G^*$, so that $G_b \in \Gamma$.

We have shown that Γ has no minimal element. By the descending chain condition on $\mathcal{G}$, $\Gamma = \emptyset$. □

We present some corollaries of Theorem 1.

COROLLARY 1.A. _If_ U _is a full subset of_ T^n _then there are only finitely many maximal closed subgroups_ H _of_ T^n _such that_ $H \cap U = \emptyset$.

COROLLARY 1.B. _Let_ S _be a closed subset of_ T^n _such that if_ $x \in S$ _and_ m _is a positive integer then_ $mx \in S$. _Then_ S _is a finite union of closed subgroups of_ T^n.

We now consider an order relation on open subsets of the torus T^n. For open subsets U and V of T^n we write $U \prec V$ if for each $x \in U$ there is a positive integer m such that $mx \in V$. We write $U \approx V$ if $U \prec V$ and $V \prec U$. Then $\approx$ is an equivalence relation on the set of open subsets of T^n and $\prec$ induces a partial ordering on the set $\mathcal{E}$ of equivalence classes. We wish to study this partially ordered set.

For open subsets U of T^n let $\tau(U)$ denote the complement of the union of the closed subgroups G of T^n such that $G \cap U = \emptyset$. We see from Theorem 1 that $\tau(U)$ is open. Perhaps it is easier to derive this fact as a consequence of the following lemma.

LEMMA 4. $\tau(U) = \{ x \in T^n :$ <u>there is</u> $m \in \mathbb{Z}$, $m > 0$, <u>such that</u> $mx \in U \}$.

Proof. Certainly if there is a positive integer m such that $mx \in U$ then each subgroup $G \subseteq T^n$ such that $x \in G$ intersects U nontrivially, so $x \in \tau(U)$. Suppose no such m exists. The closure of the set $\{ mx : m \in \mathbb{Z}, m > 0\}$ is then a closed subgroup G of T^n which misses U. Since $x \in G$, $x \notin \tau(U)$. □

We see that τ is an algebraic closure operator on the collection of all open subsets of T^n : $U \subseteq \tau(U)$ for each open set U; if $U \subseteq V$ then $\tau(U) \subseteq \tau(V)$; and $\tau(\tau(U)) = \tau(U)$, for each open set U. Also from the lemma it is immediate that $\tau(U)$ is the largest open set such that $\tau(U) \prec U$. The following theorem, which is now immediate, characterizes the partial ordering of $\mathcal{E}$ induced by $\prec$.

THEOREM 2. *If* U *and* V *are open subsets of* T^n *then* $U \prec V$ *if and only if* $\tau(U) \subseteq \tau(V)$, *and* $U \approx V$ *if and only if* $\tau(U) = \tau(V)$. *The partially ordered set* $\mathcal{E}$ *is dually isomorphic to the partially ordered set of finite unions of closed subgroups of* T^n *(under inclusion). This partially ordered set is a finitely distributive complete lattice.*

Finally we wish to establish a chain condition for this lattice.

THEOREM 3. *Let* $U_1 \subseteq U_2 \subseteq \ldots$ *be an ascending sequence of open subsets of* T^n. *Then there is an integer* M *such that* $\tau(U_M) = \tau(U_{M+1}) = \ldots.$

Proof. Let Γ denote the set of closed subgroups G of T^n such that there exists an infinite ascending chain $\tau(U_1) \subseteq \tau(U_2) \subseteq \ldots$ of distinct τ-closed open sets $\tau(U_i) \supseteq T^n \sim G$. We may write $\tau(U_1) = T^n \sim (G_1 \cup \ldots \cup G_m)$ $= \bigcap_{j=1}^{m} (T^n \sim G_j)$ for some closed subgroups $G_1, \ldots, G_m$. Then $\tau(U_i) = \tau(U_i) \cup \tau(U_1) = \bigcap_{j=1}^{m} (\tau(U_i) \cup (T^n \sim G_j))$. It is clear that for some j the sequence of sets $\tau(U_i) \cup (T^n \sim G_j) \supseteq T^n \sim G_j$ must contain an infinite subsequence of distinct τ-closed open sets. Since G_j properly contains G, we see that Γ contains no maximal element. By the chain condition on the closed subgroups of T^n, it follows that $\Gamma = \emptyset$. □

4. Some Consequences and Related Results.

LEMMA 5. *Let* $U^n = \{ (x_1, \ldots, x_n) \in \mathbb{R}^n : x_i > 0$ *for* $i = 1, \ldots, n$ *and* $x_1 + \ldots + x_n < 1 \}$. *There is a number* $\chi < 1$ *such that if* G *is a group for which* $\mathbb{Z}^n \subseteq G \subseteq \mathbb{R}^n$ *and* $G \cap U^n \neq \emptyset$ *then there is a point* $(x_1, \ldots, x_n) \in G \cap U^n$ *for which* $x_1 + \ldots + x_n \leq \chi$.

Proof. Consider the sequence

$$\tau(1/2\ U^n) \subseteq \tau(2/3\ U^n) \subseteq \tau(3/4\ U^n) \subseteq \ldots.$$

By Theorem 3 there is an m such that

$$\tau(m/(m+1)\ U^n) = \tau((m+1)/(m+2)\ U^n) = \ldots.$$

We may set $\chi = m/(m+1)$. □

In general it seems difficult to find a value for χ. We know that for $n = 1$ we can take $\chi = 1/2$; for $n = 2$, $\chi = 5/6$. Any value for $n = 3$ must satisfy $\chi \geq 41/42$, but we do not know a value even in this case.

Let χ_n denote the least value for χ satisfying Lemma 5. It is easy to see that $\chi_n \leq \chi_{n+1}$ for n = 1, 2, . . ., for if $G \subseteq \mathbb{R}^n$ is a group such that $G \cap U^n \neq \emptyset$ and $G \cap (\alpha U^n) = \emptyset$ then $G \times \mathbb{R}$ has the analogous properties in $\mathbb{R}^{n+1}$. For $S \subseteq \mathbb{R}^n$ denote by S^o its interior. For a convex polytope $K \subseteq \mathbb{R}^n$ denote by vert(K) its vertex set.

LEMMA 6. <u>Let</u> $k = \lceil \frac{1}{1 - x_{2n-2}} \rceil$. <u>Suppose the convex polytope</u> K, <u>having</u> $\mathrm{vert}(K) \subseteq \mathbb{Z}^n$, <u>contains at least</u> $(1 + k)^n + 1$ <u>points of</u> $\mathbb{Z}^n$, <u>and</u> $K^o \cap \mathbb{Z}^n = \emptyset$. <u>Then there is a linear function</u> $A : \mathbb{R}^n \to \mathbb{R}^{n-1}$ <u>such that</u> $A(\mathbb{Z}^n) = \mathbb{Z}^{n-1}$ <u>and</u> $A(K)^o \cap \mathbb{Z}^{n-1} = \emptyset$.

Proof. Clearly some pair of points of $K \cap \mathbb{Z}^n$ must be congruent modulo $1 + k$; the line L containing these satisfies $|L \cap K \cap \mathbb{Z}^n| \geq k + 2$. Let $u, w \in \mathbb{Z}^n$ be such that $u, u + w, u + 2w, . . ., $ and $u + (k+1)w$ are consective points of $L \cap K \cap \mathbb{Z}^n$. We may choose a basis $\{w, b_2, b_3, . . ., b_n\}$ for $\mathbb{Z}^n$ which contains w. For $x = \alpha_1 w + \alpha_2 b_2 + . . . + \alpha_n b_n \in \mathbb{Z}^n$, let $A(x) = (\alpha_2, . . ., \alpha_n) \in \mathbb{R}^{n-1}$. Then $A : \mathbb{R}^n \to \mathbb{R}^{n-1}$ is a linear function such that $A(\mathbb{Z}^n) = \mathbb{Z}^{n-1}$.

We will complete the proof by showing that if $A(K)^o \cap \mathbb{Z}^{n-1} \neq \emptyset$ then $K^o \cap \mathbb{Z}^n \neq \emptyset$. Suppose $p \in A(K)^o \cap \mathbb{Z}^{n-1}$. Then by a theorem of Steinitz ([6]; see also Exercise 2.3.5 of [3]) we may choose a set of $m \leq 2(n - 1)$ vertices of A(K), say, $\{A(v_1), . . ., A(v_m)\}$, where $v_1, . . .,$ and v_m are vertices of K, such that p is in the interior of $\mathrm{conv}\{A(v_1), . . ., A(v_m)\}$. We may find $\alpha_1, . . ., \alpha_m$, and β, where $\alpha_i > 0$ $(i = 1, . . ., m)$, $\beta > 0$, $(\sum_{i=1}^{m} \alpha_i) + \beta = 1$, and $p = (\sum_{i=1}^{m} \alpha_i A(v_i)) + \beta (A(u))$.

Let $G \subseteq \mathbb{R}^m$ be the subgroup

$$G = \{ (\nu_1, \ldots, \nu_m) : \sum_{i=1}^{m} \nu_i (A(v_i) - A(u)) \in \mathbb{Z}^{n-1} \}.$$

Clearly $G \supseteq \mathbb{Z}^m$, and $(\alpha_1, \ldots, \alpha_m) \in G$. By Lemma 5 it is possible to choose $(\tilde{\alpha}_1, \ldots, \tilde{\alpha}_m) \in G$ such that $\tilde{\alpha}_i > 0$ for $1 \leq i \leq m$ and $\tilde{\alpha}_1 + \ldots + \tilde{\alpha}_m \leq x_m \leq x_{2(n-1)}$. Let $\tilde{\beta} = 1 - \tilde{\alpha}_1 - \ldots - \tilde{\alpha}_m \geq 1 - x_{2(n-2)} > 1/(k+1)$. Consider

$$x = \sum_{i=1}^{m} \tilde{\alpha}_i v_i + \tilde{\beta} u \quad \text{and} \quad y = \sum_{i=1}^{m} \tilde{\alpha}_i v_i + \tilde{\beta}(u + (k+1)w)$$

$= x + \tilde{\beta}(k+1)w$. Suppose $x = \tau_1 w + \tau_2 b_2 + \ldots \tau_n b_n$, so that $A(x) = (\tau_2, \ldots, \tau_n)$. Since $(\tilde{\alpha}_1, \ldots, \tilde{\alpha}_m) \in G$, $\tau_2, \ldots,$ and τ_n are integers. Since $\tilde{\beta}(k+1) > 1$, there is an integer $\tilde{\tau}_1$ such that $\tau_1 < \tilde{\tau}_1 < \tau_1 + \beta(k+1)$. Then $z = \tau_1 w + \tau_2 b_2 + \ldots + \tau_n b_n \in \mathbb{Z}^n$ is in the relative interior of the line segment connecting x and y, so $z \in K^o \cap \mathbb{Z}^n$. □

THEOREM 4. <u>There are, up to unimodular equivalence, only finitely many convex polytopes</u> P <u>satisfying</u>:

(i) $\text{vert}(P) \subseteq \mathbb{Z}^n$;

(ii) $P^o \cap \mathbb{Z}^n = \emptyset$; <u>and</u>

(iii) $P^o \cap G \neq \emptyset$, <u>for each group</u> $G \subseteq \mathbb{R}^n$ <u>which properly contains</u> $\mathbb{Z}^n$.

Proof. After Lemma 6, we need only show that there are only finitely many equivalence classes of such P for which

$|P \cap \mathbb{Z}^n| < m$ (where $m = (1 + k)^n + 1$ as in Lemma 6). Indeed, if $|P \cap \mathbb{Z}^n| \geq m$ and if P satisfies (i) and (ii) then $A^{-1}(\mathbb{Z}^{n-1})$ is a subgroup G of $\mathbb{R}^n$ for which (iii) fails, where A is the linear function guaranteed by the lemma.

Suppose that P and Q are convex polytopes, each satisfying conditions (i), (ii), and (iii), and neither having m or more elements in common with $\mathbb{Z}^n$. Let

$$U^n = \{(x_1, \ldots, x_{m-2}) \in \mathbb{R}^{m-2} : x_i > 0 \text{ for } 1 \leq i \leq m - 2 \text{ and } x_1 + \ldots + x_{m-2} < 1\}.$$

Let $B : \mathbb{R}^{m-2} \to \mathbb{R}^n$ and $C : \mathbb{R}^{m-2} \to \mathbb{R}^n$ be affine functions mapping $cl(U^n)$ onto P and Q respectively and mapping $\mathbb{Z}^{m-2}$ onto $\mathbb{Z}^n$. The subgroups $G = B^{-1}(\mathbb{Z}^n)$ and $H = C^{-1}(\mathbb{Z}^n)$ then miss U, and are maximal such subgroups. If $G = H$ then there is an affine unimodular function $D : \mathbb{R}^n \to \mathbb{R}^n$ such that $B = DC$. In particular, $DQ = P$.

By Theorem 1, the number of maximal subgroups $G \supseteq \mathbb{Z}^{m-2}$ such that $G \cap U = \emptyset$ is finite. We see from the preceding paragraph that this number is an upper bound on the cardinality of any collection of unimodularly inequivalent convex polytopes P satisfying (i), (ii), (iii), and $|vert(P)| < m$. □

5. Unanswered Questions.

In this final section we present some problems and questions that seem natural but with which we have not dealt.

A. Is there a reasonable method for computing the finitely many groups of Theorem 1 -- say, when the dimension n is small and the set U is the interior of a convex polytope?

B. Compute χ_n; or at least find numbers that can serve as the χ's of Lemma 5. (We know $\chi_1 = 1/2$, $\chi_2 = 5/6$, $\chi_3 \geq 41/42$, ...)

C. Find the convex polytopes P of Theorem 4, when (say) $n = 3$. (For $n = 1$, there is, up to unimodular equivalence, only the interval $[0, 1]$; for $n = 2$, only $\mathrm{conv}\{\begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}2\\0\end{bmatrix}, \begin{bmatrix}0\\2\end{bmatrix}\}$.

Acknowledgement. We are indebted to Mark Hartmann for a careful reading of and several improvements over a preliminary version of this paper.

References.

1. Bourbaki, N., General Topology, Part 2. Hermann, 1966.

2. Cassels, J. W. S., An Introduction to the Geometry of Numbers, Springer-Verlag, 1971.

3. Grünbaum, B., Convex Polytopes. Interscience, 1967.

4. Hardy, G. H., and E. M. Wright, The Theory of Numbers, Oxford University Press, 1968.

5. Lagarias, J. C., H. W. Lenstra, Jr., and C. P. Schnorr, "Korkine-Zolotarev Bases and Successive Minima of a Lattice and its Reciprocal Lattice." (Preprint.)

6. Steinitz, E., "Bedingt Konvergente Reihen und Konvexe System." J. reine angew. Math. 143 (1913), 128-175; 144 (1914), 1-40; 146 (1916), 1-52.

NBS-114A (REV. 2-80)

U.S. DEPT. OF COMM.

BIBLIOGRAPHIC DATA SHEET *(See instructions)*

1. PUBLICATION OR REPORT NO.
NISTIR 88-3777

2. Performing Organ. Report No.

3. Publication Date
AUGUST 1988

4. TITLE AND SUBTITLE

Finite Unions of Closed Subgroups of the n-Dimensional Torus

5. AUTHOR(S)

Jim Lawrence

6. PERFORMING ORGANIZATION *(If joint or other than NBS, see instructions)*

NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
WASHINGTON, D.C. 20234

7. Contract/Grant No.

8. Type of Report & Period Covered

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS *(Street, City, State, ZIP)*

10. SUPPLEMENTARY NOTES

☐ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

11. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here)*

Let U be an open subset of the torus group T^n. We show that the set of maximal subgroups of T^n which miss U is of finite cardinality. This result is applied to show that the lattice of finite unions of closed subgroups of T^n is a complete distributive lattice, and to show that, up to unimodular equivalence, there are only finitely many convex polytopes P R^n having vertices in Z^n but no interior points in Z^n and such that each subgroup G of the additive group R^n which properly contains Z^n does have points in common with the interior of P.

12. KEY WORDS *(Six to twelve entries; alphabetical order; capitalize only proper names; and separate key words by semicolons)*

torus; lattice; convex polytope; successive minima

13. AVAILABILITY

- [X] Unlimited
- [ ] For Official Distribution. Do Not Release to NTIS
- [ ] Order From Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.
- [X] Order From National Technical Information Service (NTIS), Springfield, VA. 22161

14. NO. OF PRINTED PAGES
23

15. Price
$9.95