Theorem. If A be an additive subgroup of Euclidean space $\mathbf{R}^n$ such that every bounded region of space contains only finitely many elements of A, then A is a lattice of dimension $\leq n$.

Proof. Let $\{v_1, \ldots, v_m\}$ be a maximal $\mathbf{R}$-linearly independent set of elements from A (if $A = \{0\}$, take the empty set; otherwise, add linearly independent vectors until no new elements from A can be added). Let m be the maximum possible size of such a set, since any such set has size $\leq n$. We will prove the statement by induction on m. Clearly, if $m = 0$ then $A = \{0\}$, hence is a lattice of dimension 0.

Let $A_0 = A \cap \operatorname{span}\{v_1, \ldots, v_{m-1}\}$. Then $\{v_1, \ldots, v_{m-1}\}$ is a maximal linearly independent subset of A_0, so by induction A_0 is a lattice with some basis $\{u_1, \ldots, u_k\}$, where $k \leq m-1$. However, $\{v_1, \ldots, v_{m-1}\} \subseteq A_0$, thus $\{v_1, \ldots, v_{m-1}\}$ is in the vector space spanned by $\{u_1, \ldots, u_k\}$ over $\mathbf{R}$. Since $\{v_1, \ldots, v_{m-1}\}$ is linearly independent over $\mathbf{R}$, this means that $k \geq m-1$. Therefore, we know $k = m-1$.

Let $S = A \cap \{a_1u_1 + \cdots + a_{m-1}u_{m-1} + a_mv_m \mid 0 \leq a_i < 1 \text{ for } 1 \leq i \leq m-1, 0 \leq a_m \leq 1\}$. By the triangle inequality, S is contained within a ball of radius $|u_1| + \cdots + |u_{m-1}| + |v_m|$ about the origin, hence is finite. Now, $\{u_1, \ldots, u_{m-1}, v_m\}$ must be linearly independent, since if v_m were in the span of the u_is, then $\operatorname{span}\{u_1, \ldots, u_{m-1}\}$ would contain $\operatorname{span}\{v_1, \ldots, v_m\}$, contradicting that this latter set is linearly independent. So every element of S has a unique representation of the form

$$a_1u_1 + \cdots + a_{m-1}u_{m-1} + a_mv_m$$

with $0 \leq a_i < 1$ for $1 \leq i \leq m-1$ and $0 \leq a_m \leq 1$. So there is some $v'_m \in S$ which has a minimal but nonzero coefficient a_m when expanded as

$$v'_m = a_1u_1 + \cdots + a_{m-1}u_{m-1} + a_mv_m.$$

We know this because these expansions are unique and S is finite.

Replacing v_m with v'_m, we now see that $\{u_1, \ldots, u_{m-1}, v'_m\}$ is still linearly independent because $\{u_1, \ldots, u_{m-1}\}$ is linearly independent and, due to the uniqueness of the representations we just discussed, v'_m is not a linear combination of $\{u_1, \ldots, u_{m-1}\}$. Also, $\{u_1, \ldots, u_{m-1}, v'_m\}$ spans A over $\mathbf{R}$: if there were some $v \in A \setminus \operatorname{span}(\{u_1, \ldots, u_{m-1}, v'_m\})$ then v would be linearly independent of $\{u_1, \ldots, u_{m-1}, v'_m\}$, meaning that $\{u_1, \ldots, u_{m-1}, v'_m, v\}$ is a linearly independent set, contradicting that m is the largest possible size of a linearly independent set in A.

Let $v \in A$. Then v can be expressed uniquely as a linear combination $v = b_1u_1 + \cdots + b_{m-1}u_{m-1} + b_mv'_m$. Letting $v'_m = a_1u_1 + \cdots + a_{m-1}u_{m-1} + a_mv_m$ be the expansion of v'_m given previously, we have

$$\begin{aligned} v &= b_1u_1 + \cdots + b_{m-1}u_{m-1} + b_mv'_m \\ &= b_1u_1 + \cdots + b_{m-1}u_{m-1} + b_m(a_1u_1 + \cdots + a_{m-1}u_{m-1} + a_mv_m) \\ &= (b_1 + b_ma_1)u_1 + \cdots + (b_{m-1} + b_ma_{m-1})u_{m-1} + (b_ma_m)v_m. \end{aligned}$$

Let $c_m = \lfloor b_m \rfloor$. Note that the coefficient of v_m in $v - c_mv'_m$ is $(b_m - c_m)a_m$, which satisfies $0 \leq (b_m - c_m)a_m < a_m$ since $0 \leq b_m - c_m < 1$. Next, for each $i = 1, \ldots, m-1$ let c_i be the floor of the coefficient of u_i in $v - c_mv'_m$. Let

$$v' = v - c_1u_1 - \cdots - c_{m-1}u_{m-1} - c_mv'_m$$

Each u_i is in A, v'_m is in A, and each c_i is an integer. So v' is a $\mathbf{Z}$-linear combination of elements in A, hence $v' \in A$. Furthermore, the coeffecients of $u_1, \ldots, u_{m-1}, v_m$ in v' are all less than 1 and at least 0 by construction; therefore, $v' \in S$. The coefficient of v_m in v' is the same as the coefficient of v_m in v, which we previously noted is strictly less than a_m. By the minimality of a_m (recall how a_m was defined), we realize that this coefficient must be 0. Therefore, v' is a $\mathbf{Z}$-linear combination of $\{u_1, \ldots, u_{m-1}\}$. But also, $w' = c_1u_1 + \cdots + c_{m-1}u_{m-1} + c_mv'_m$ is in the span of $\{u_1, \ldots, u_{m-1}, v'_m\}$ over $\mathbf{Z}$. Thus, $v = v' + w$ is in the span of $\operatorname{span}\{u_1, \ldots, u_{m-1}, v'_m\}$ over $\mathbf{Z}$, and so this set generates A. We have already shown this set to be linearly independent over $\mathbf{R}$, and that $m \leq n$. Therefore, A is a lattice of dimension $\leq n$. $\square$

Proposition. Let $\mathcal{M} \subseteq \mathbf{R}^n$ be such that $0 \in \mathcal{M}$ and $[\alpha - \beta] \in \mathbf{Z}$ for all $\alpha, \beta \in \mathcal{M}$. Then the additive group $\mathbf{Z}[\mathcal{M}]$ generated by $\mathcal{M}$ also satisfies $[\alpha - \beta] \in \mathbf{Z}$ for all $\alpha, \beta \in \mathbf{Z}[\mathcal{M}]$, and contains finitely many points in any bounded region of $\mathbf{R}^n$. Therefore, $\mathbf{Z}[\mathcal{M}]$ is a lattice in $\mathbf{R}^n$.

Proof. Let $\alpha \in \mathbf{Z}[\mathcal{M}]$, so that $\alpha = \sum_{t=1}^m \alpha_t$ for some $\alpha_1, \dots, \alpha_m \in \mathcal{M}$. We have

$$[\alpha] = \left[\sum_{t=1}^m \alpha_t\right] = \left[\sum_{t=1}^m \alpha_t, \sum_{t=1}^m \alpha_t\right] = \sum_{s=1}^m \sum_{t=1}^m [\alpha_s, \alpha_t] = \sum_{t=1}^m [\alpha_t] + \sum_{1 \le s < t \le m} 2\,[\alpha_s, \alpha_t]\,.$$

Since $[\alpha_s] = [\alpha_s - 0] \in \mathbf{Z}$, and $[\alpha_s - \alpha_t] = [\alpha_s] + [\alpha_t] - 2\,[\alpha_s, \alpha_t] \in \mathbf{Z}$ for all $s, t \in \mathbf{Z}$, we know $2\,[\alpha_s, \alpha_t] \in \mathbf{Z}$ for all $s, t \in \mathbf{Z}$. Therefore, $[\alpha] \in \mathbf{Z}$. Since $\mathbf{Z}[\mathcal{M}]$ is a subgroup, we know that $\alpha - \beta \in \mathbf{Z}[\mathcal{M}]$ for any $\beta \in \mathbf{Z}[\mathcal{M}]$, thus $[\alpha - \beta] \in \mathbf{Z}$ as well.

Let R be any bounded region of $\mathbf{R}^n$. We aim to show that $\mathbf{Z}[\mathcal{M}] \cap R$ is finite. We may assume R is closed, since R is certainly contained within its closure and hence so is $\mathbf{Z}[\mathcal{M}] \cap R$. Let $\mathcal{C}$ be the set of all open balls in $\mathbf{R}^n$ of radius $\frac{1}{2}$. $\mathcal{C}$ is an open cover of the compact set R, hence it has a finite subcover $\mathcal{C}' \subset \mathcal{C}$ containing $N \in \mathbf{Z}_{>0}$ elements. If $B \in \mathcal{C}'$, then B may contain at most one point of $\mathbf{Z}[\mathcal{M}]$, since we have $[\alpha - \beta] \in \mathbf{Z}$, and thus $|\alpha - \beta| \ge 1 > \frac{1}{2}$, for any distinct $\alpha, \beta \in \mathbf{Z}[\mathcal{M}]$. Therefore, $\mathbf{Z}[\mathcal{M}] \cap R$ contains at most N points. By the previous theorem, we see that $\mathbf{Z}[\mathcal{M}]$ must be a lattice in $\mathbf{R}^n$. $\square$