Discrete subgroups of $\mathbb{R}^n$

S. Kumaresan
School of Math. and Stat.
University of Hyderabad
Hyderabad 500046
kumaresa@gmail.com

Proposition 1. *Let Γ be a discrete subgroup of $\mathbb{R}^n$. Then there exists a basis $u_1, u_2, \dots, u_n$ of $\mathbb{R}^n$ such that*

$$\Gamma = \{x \in \mathbb{R}^n : x \text{ is of the form } x = n_1 u_1 + \cdots + n_r u_r, n_j \in \mathbb{Z}\},$$

for some $r \leq n$.

Proof. The proof is an inductive construction. Let W be a vector subspace of $\mathbb{R}^n$ such that $\Gamma \cap W = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_k$ for some basis $w_1, \dots, w_k$ of W. Such W's exist, for instance $W = \{0\}$! Suppose that there exists $u \in \Gamma$ that does not lie in W. Consider the set B_W of points

$$a_1 w_1 + \cdots + a_k w_k + bu, \quad 0 \leq a_i \leq 1, 0 \leq b \leq 1. \tag{1}$$

This set is bounded in $\mathbb{R}^n$. Since Γ is discrete, this set B_W can contain only finitely many points of Γ. Hence there exists a point $v \in B_W \cap \Gamma$ such that the coefficient b of u in v will be the least positive coefficient, say β. If $a_1 w_1 + \cdots + a_k w_k + bu$ lies in Γ with $a_i, b \in \mathbb{Z}$, then b is a multiple of β. For, otherwise, by division algorithm, we write $b = m\beta + r$ where $0 < r < \beta$. Hence the element

$$a_1 w_1 + \cdots + a_k w_k + ru = (a_1 w_1 + \cdots + a_k w_k + bu) - m\beta u \in \Gamma.$$

Since $w_j \in \Gamma$, by subtracting suitable multiples of w_j, we can assume that $0 \leq a_j \leq 1$. In other words, $a_1 w_1 + \cdots + a_k w_k + ru \in B_W$. This contradicts our choice of μ. Thus we have established that

$$\Gamma \cap (W + \mathbb{R}u) = (\Gamma \cap W) + \mathbb{Z}v = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_k + \mathbb{Z}u.$$

Note that the set $\{w_1, \dots, w_k, u\}$ is a basis of $W + \mathbb{R}u$. If there exists $u' \in \Gamma$, we can proceed as above. This process has to stop in a finite number of steps. $\square$