Math 55a: Honors Advanced Calculus and Linear Algebra

Solution for Problems 3 and 4 on Problem Set #10

Lemma. *Let V be a real vector space of dimension n, and $\{v_i | 1 \le i \le n\}$ a basis. Then the set G of integer combinations $\sum_{i=1}^m a_i v_i$ ($a_i \in \mathbf{Z}$) is discrete in V.*

Proof: Since all norms on V are equivalent, it is enough to prove the Lemma for one norm. We use the basis $\{v_i\}$ to identify V with $\mathbf{R}^n$, and use the sup norm on $\mathbf{R}^n$. Then G is clearly discrete, because open balls of radius $1/2$ abound elments of G are disjoint. $\square$

Proposition 1. *Let V be a real vector space of dimension n, and let v_i ($1 \le i \le m$) be vectors in V that is linearly independent* **over Q**, *so that the integer combinations $\sum_{i=1}^m a_i v_i$ ($a_i \in \mathbf{Z}$) are all distinct. If the set G of such linear combinations is discrete, then $m \le n$.*

Proof: Again we use a sup norm on V, this time coming from an arbitrary identification of V with $\mathbf{R}^n$. Suppose $m > n$, and let $M = \sup_{i=1}^m \|v_i\|$. For each integer $N > 0$, let G_N be the set of integer combinations $\sum_{i=1}^m a_i v_i$ ($a_i \in \mathbf{Z}$) with each coefficient a_i in $[-N, N]$. Then $|G_N| = (2N+1)^m$. But each vector in G_N has norm at most mMN. So G_N is contained in a hypercube of side-length $2mMN$. We write G_N as the union of H^n hypercubes of side-length $2mMN/H$, where H is the largest integer such that $H^n < (2N+1)^m$. By the pigeonhole principle, one of these smaller hypercubes contains at least two elements of G_N. The difference between them is a nonzero element of G of norm at most $2mMN/H$. But $H = (2N+1)^{m/n} - O(1)$, so $2mMN/H \to 0$ as $N \to \infty$. Therefore we can find a nonzero element of G arbitrarily close to zero by making N larger enough. Hence every open ball about 0 contains elements of G other than 0, so that G is not discrete. $\square$

We have implicitly used the fact that the subset G of V is in fact a subgroup of the additive group $(V, +)$. We next describe all discrete subgroups:

Proposition 2. *Let V be a real vector space of dimension n, and let G be a discrete subgroup. Then there exist linearly independent vectors $v_1, \ldots, v_m$ for some $m \le n$ such that G is the set of integer combinations of the v_i.*

Proof: Here it will be convenient to give V the structure of a real inner-product space, and use the resulting norm. We prove the Lemma by induction on n, the case $n = 0$ being trivial. Assume then that $n > 0$ and the Lemma is known for vector spaces of dimension $n - 1$. If $G = \{0\}$, there is nothing to prove. Otherwise, let r be the infimum of $\|v\|$ over nonzero $v \in G$. We claim that there exists $v \in G$ of norm r. Indeed, the intersection of G with the closed hollow ball $\{v : r \le \|v\| \le 2r\}$ is finite — because that hollow ball is compact (Heine-Borel) and G is discrete — and r is the infimum of $\|v\|$ over that finite set. Let U be the orthogonal complement of $\mathbf{R}v$, and $\pi : V \to U$ the orthogonal projection. We claim that if $v' \in G$ and v' is not an integer multiple of v then $\|\pi(v')\| \ge (\sqrt{3/4})r$. Indeed we have $v' = \pi(v') + cv$ for some $c \in \mathbf{R}$; let a be an integer such that $|c - a| \le 1/2$, and observe that $v' + av \in G$ and $\pi(v' - av) = \pi(v')$, so

$$\|\pi(v')\|^2 = \|\pi(v' - av)\|^2 = \|v' - av\|^2 - \|(c-a)v\|^2 \ge r^2 - (1/2)^2 r^2 = 3r^2/4,$$

where in the next-to-last step we used the fact that $v' - av$ is a nonzero vector in G. In particular it follows that the restriction of π to G has kernel $\mathbf{Z}v$, and image a discrete subgroup of U because the norm of each nonzero element is bounded below by $(\sqrt{3/4})r$. Thus by the inductive assumption $\pi(G)$ consists of the integer combinations of $u_1, \ldots, u_{m'}$ for some linearly independent $u_1, \ldots, u_{m'} \in U$. Writing each u_i as $\pi(v_i)$ for some $v_i \in G$, we then conclude by observing that the vectors $v_1, \ldots, v_{m'}, v$ are linearly independent in V, and that G consists of the integer combinations of those $m' + 1$ vectors. $\square$

Note that Proposition 2 also yields an alternative proof of Proposition 1.

We next consider what happens when we weaken the hypothesis of discreteness, requiring only that G be closed. A discrete subgroup is automatically closed, but many closed subgroups are not discrete, for instance vector subspaces of positive dimension. The next result states in effect that this is the only possible source of non-discreteness of G.

Proposition 3. *Let V be a real vector space of dimension n, and let G be a closed subgroup that is not discrete. Then G contains a nonzero vector subspace of V.*

Proof: Use an arbitrary norm on V, and let $v_i \in G$ be nonzero vectors such that $v_i \to 0$. Then $v_i' := v_i/\|v_i\|$ are vectors of norm 1. Since $\{v \in V : \|v\| = 1\}$ is compact, the sequence $\{v_i'\}$ has a convergent subsequence; let v be its limit. We claim that G contains cv for all $c \in \mathbf{R}$. If $\|v_i' - v\| < \epsilon$ then $\|cv_i' - cv\| < |c|\epsilon$. But cv_i' is within $\|v_i\|$ of an integer multiple of v_i, and all such multiples are in G. Since ϵ can be taken arbitrarily small and $\|v_i\| \to 0$, it follows that G contains elements arbitrarily close to cv, and since G is closed it follows that $G \ni cv$. Thus G contains the one-dimensional subspace $\mathbf{R}v$ of V. □

Now if G contains two vector subspaces U_1, U_2 of V, then it also contains $U_1 + U_2$. So there exists a largest subspace $U \subseteq V$ such that $G \subseteq U$. Then G is determined by U and the image G_1 of G in the quotient space V/U; in fact G is the preimage of G_1 in V. Moreover, G_1 is a discrete subgroup of V/U, else by Proposition 3 there would be a nonzero subspace of V/U contained in G_1, and its preimage in V would be a subspace properly containing U and contained in G. Using Proposition 2, we thus obtain a complete description of closed subgroups of V:

Theorem. *Let V be a real vector space of dimension n, and let G be a closed subgroup. Let U be the largest subspace of V that contains G. Then there exist linearly independent $v_1, \ldots, v_m \in V$ whose span has zero intersection with U, such that G is the direct sum of U with the integer combinations of $v_1, \ldots, v_m$.*

Conversely, it follows from our first Lemma that for any such U and v_i the subgroup of V generated by U and the v_i is in fact closed.

Corollary. *Let V be a finite-dimensional real vector space. A subgroup G of $(V, +)$ is dense in V if and only if there is no nonzero functional $v^* \in V^*$ such that $v^*(G) \subseteq \mathbf{Z}$. If moreover G is finitely generated then G is dense in V if and only if there is no nonzero functional $v^* \in V^*$ such that $v^*(G) \subseteq \mathbf{Q}$.*

Proof: If there exists such v^* then any $v \in V$ for which $v^*(v) \neq \mathbf{Z}$ has a neighborhood disjoint from G, so G is clearly not dense.

Conversely, if G is not dense then we may apply our Theorem to the closure $\overline{G}$, which is also a subgroup of $(V, +)$. Since $\overline{G} \neq V$, we have $m \neq 0$, so we may find $v^* \in U^\perp$ such that $v^*(v_1) = 1$ and $v^*(v_i) = 0$ for $i > 1$.

If G is finitely generated then we need only check $v^*(v) \in \mathbf{Q}$ on finitely many generators, and then multiplying by a common denominator D yields nonzero $Dv^* \in V^*$ such that $(Dv^*)(G) \in \mathbf{Z}$, reducing to a result already proved. □