Math 661
Algebraic Number Theory
Some Comments on Lattices

The purpose of this note is to add some material to Baker's treatment of Lattices.

First, recall his convention, and then recall his definition: His field k is allowed to be one of either $\mathbb{Q}$ or $\mathbb{R}$, and he defines a (complete) lattice in a finite dimensional vector space V over k to be an additive subgroup Λ of V which is discrete and spans V. (Here, "span" refers to the k-vector space structure, i.e, the span of a set is the set of k-linear combinations of elements of that set.)

0.1. **Discreteness.** How does he define "discrete?" He says a subset $\Lambda \subset V$ is discrete if every bounded subset of V contains only finitely many points of V. Recall first that $k = \mathbb{Q}$ or $k = \mathbb{R}$. Thus, the "bound" he refers to is with respect to the Euclidean metric on V. The first thing we want to understand is the relation of this definition to another property: that each point of V have a neighborhood in which there are no other points of Λ. We have the following:

Lemma 1. *If V and k are as above, and if $S \subset V$ is discrete according to the definition above, then every point Q of V has an open ball $B_r(Q) = \{x \in V \mid |x - Q| < r\}$ (for some $r > 0$) such that $B_r(Q) \cap \Lambda = \{Q\}$.*

Proof. Take the ball of radius 1 around Q, i.e, $B_1(Q)$. Because S is discrete, $B_1(Q)$ contains only finitely many points of S: say $P_0 = Q, P_1, \ldots P_n$. In particular, all points of S other than $P_1, \ldots, P_n$ are at a distance at least 1 from Q. Take $0 < r < \min\{|P_i - P_0|\}$, $i = 1, \ldots, n$. Then it is clear that $B_r(Q) \cap S = \{Q\}$. □

Now let us add the hypothesis that S is not just an arbitrary subset of V but actually a subgroup of V. We then have the following:

Lemma 2. *Let k and V be as above, and let S be a subgroup of V. If S has the property that every point $Q \in S$ has a neighborhood in which there are no other points of S, then S is discrete (where "discrete" is as defined above).*

Proof. Let $X \subset V$ be any bounded set. Assume to the contrary that X contains infinitely many points of S. Then these infinite points in $S \cap X$, being bounded, must have a limit point Q in V. In particular, there is a sequence of points $\{P_i\} \subset S \cap X$ that converges to Q. This is a Cauchy sequence, so we can find n and m such that $|P_n - P_m|$ is arbitrarily close to zero. We now invoke the fact that S is a subgroup of V: the element $P_n - P_m$ of V is actually in S. Thus, S contains vectors of arbitrarily small length, so the point 0 of V cannot have a neighborhood around it in which it is the only point of S. This is a contradiction. □

We thus find that when Λ is a subgroup of V, we may equivalently define Λ to be discrete if every point of Λ is "isolated" in the sense we have been considering: there is a neighborhood of that point which contains no other point of Λ. Note that we may then equivalently define a subgroup Λ of V to be discrete if 0 is isolated. For, by translation, for any point $Q \in \Lambda$, Q is isolated if and only if 0 is isolated.

0.2. **Discrete Free Abelian Groups in $\mathbb{R}^n$.**

(1) A comment about the proof of Prop. 1.17 (ii/iii) implies (i). So we saw in class that the region $S = \{\Sigma \lambda_i x_i \mid \lambda \in \mathbb{R}, |\lambda_i| < 1\}$ is such that $S \cap \Lambda = \{0\}$. We want to show that $\{0\}$ is isolated, i.e., there is some open ball $B_r(0)$

such that $B_r(0) \cap \Lambda = \{0\}$. For this is, it suffices to show that S itself is open, since open balls $B_r(Q)$ about various points Q form a basis for the topology.

To do so, perform a Gram-Schmidt Orthonormalization to the basis x_1, ..., x_n. Take $e_1 = x_1/|x_1|$, $e_2' = x_2 - x_1\dfrac{(x_1 \cdot x_2)}{(x_1 \cdot x_1)}$ and then $e_2 = e_2'/|e_2|$, etc. Consider the linear transformation L that sends x_1 to e_1, x_2 to e_2, ..., x_n to e_n. Thus, the point $\Sigma\lambda_i x_i$ goes to $\Sigma\lambda_i e_i$, and the region S goes to $L(S) = \{\Sigma\lambda_i e_i \mid |\lambda_i| < 1\}$. L is invertible, and both L and L^{-1} are continuous maps of $\mathbb{R}^n$ to $\mathbb{R}^n$. Hence, L is a homeomorphism from $\mathbb{R}^n$ to $\mathbb{R}^n$. It is clear that $L(S)$ is open: it is simply the interior of the n-cube of length 2, so it follows that S is also open.

(2) In the proof of Prop. 1.17 (i) implies (ii/iii), he shows that Λ (already assumed to be a discrete subgroup of V that spans V, i.e., already assumed to be a lattice) is finitely generated. Since Λ is free, this shows that $\Lambda \cong \mathbb{Z}^t$ for some t. The question is, why should this t equal n? This can be done by using the Smith Normal Form of matrices over $\mathbb{Z}$ (which is one of the ways to prove the Fundamental Theorem of finitely generate abelian groups) but we will sketch a different approach below that reveals something about the fractional parts of tuple of real numbers.

So, take $e_1, \ldots, e_t$ to be a $\mathbb{Z}$-basis for Λ. Since Λ spans V as a k-space, and the $\mathbb{Z}$ span of the e_i is Λ, we find that the k-span of the e_i is V. Thus, the set $\{e_i\}$ contains a k-basis of V, and in particular, $t \geq n$. Now suppose, relabeling if necessary, that $e_1, \ldots, e_n$ form a k-basis of V. Assume that $t > n$. Then $e_{n+1} = r_1 e_1 + \ldots r_n e_n$, for $r_i \in k$. We wish to arrive at a contradiction.

If $k = \mathbb{Q}$ then writing each $r_i = \dfrac{a_i}{b_i}$ for suitable integers a_i, b_i, and clearing denominators, we would find a nontrivial $\mathbb{Z}$-linear combination (note: $\mathbb{Z}$ linear!) of the e_i that equals zero, a clear contradiction to the fact that the e_i form a $\mathbb{Z}$ basis for Λ. But what about the case where $k = \mathbb{R}$?

Here we need to invoke a pretty argument that uses the pigeon hole principle (and the primary reason I wrote this note is to show you this argument!). The result we will establish is the following: if $\alpha_1, \ldots, \alpha_n$ are real numbers such that at least on α_i is *irrational*, then given any $\epsilon > 0$, there exists some integer m such that the absolute value of the fractional part (see below) of each $m\alpha_i$ is less than ϵ!

OK, so our $k = \mathbb{R}^n$, the vectors $e_1, \ldots, e_n$ are a basis, and we had written $e_{n+1} = r_1 e_1 + \ldots r_n e_n$, for $r_i \in \mathbb{R}$. Write each in the unique form $r_i = m_i + \alpha_i$, where $m_i \in \mathbb{Z}$ and $-1/2 < \alpha_i \leq 1/2$. The quantity α_i is called the *fractional part* of r_i (and m_i is called the *integer part*). We may assume that at least one r_i is not rational, since we have already proved the theorem for the case where all $r_i \in \mathbb{Q}$. Now consider the "line" in $\mathbb{R}^n$ given by $x_i = m\alpha_i$, where m varies in $\mathbb{Z}$. (Here, the coordinates x_i etc., are with respect to the basis $e_1, \ldots, e_n$. Note that if m were allowed to be in $\mathbb{R}$, we would have an actual line.) We claim that no two points of this "line" are such that the difference vector lies in the subgroup $\Sigma\mathbb{Z}e_i$. For, if $a(\alpha_1, \ldots, \alpha_n) - b(\alpha_1, \ldots, \alpha_n) = (c_1, \ldots, c_n)$ for some integers a, b, and

c_i, and if say α_1 is known to be irrational, we would find $\alpha_1 = \dfrac{c_1}{a-b}$, a rational number, which is a contradiction.

Now, for each integer m, consider the n-tuple consisting of the fractional parts of $m\alpha_1, \ldots, m\alpha_n$. This will be a point inside the n-dimensional cube $-1/2 < x_i \leq 1/2$, $i = 1, \ldots, n$. By what we have seen above, for each m we get a distinct point. Now, given our $\epsilon > 0$, we assume (without loss of generality) that $\epsilon < 1/2$, and we choose N so that $1 < N\epsilon$, or equivalently $1/N < \epsilon$. Then by dividing each interval $-1/2 < x_i \leq 1/2$ into N equal segments, we divide the corresponding cube into N^n equal cubelets of side $1/N$. Taking $m = 1, \ldots, N^n + 1$, we find that the n-tuple of fractional parts of at least two points of our line $\{m(\alpha_1, \ldots, \alpha_n)\}$, say $a(\alpha_1, \ldots, \alpha_n)$ and $b(\alpha_1, \ldots, \alpha_n)$, must lie in the same cubelet. But then, if the fractional part of $a(\alpha_1, \ldots, \alpha_n)$ is $(\delta_1, \ldots, \delta_n)$ and the fractional part of $b(\alpha_1, \ldots, \alpha_n)$ is $(\theta_1, \ldots, \theta_n)$, each $|\delta_i - \theta_i|$ must be less than ϵ since each side of the cubelet is at most $1/N$. Moreover, since we have assumed $\epsilon < 1/2$, we see that $\delta_i - \theta_i$ must be the fractional part of $(a-b)(\alpha_i)$. Taking $m = a - b$, we have thus proved the result we alluded to two paragraphs above.

Now back to the proof that t must equal n. We start with $e_{n+1} = r_1 e_1 + \ldots r_n e_n = (m_1 + \alpha_1)e_1 + \ldots (m_n + \alpha_n)e_n$. Since $e_{n+1} - m_1 e_1 - \ldots m_n e_n \in \Lambda = \Sigma \mathbb{Z} e_i$, we find that $\alpha_1 e_1 + \ldots \alpha_n e_n \in \Lambda$. Hence, for all $m \in \mathbb{Z}$, $m(\alpha_1, \ldots, \alpha_n) \in \Lambda$. But then, as we have seen above, for any $\epsilon > 0$, there is an integer m such that the n-tuple of fractional parts of $m(\alpha_1, \ldots, \alpha_n)$ has each coordinate bounded above by ϵ. Since $m(\alpha_1, \ldots, \alpha_n)$ is in Λ, and the n-tuple of integer parts of $m(\alpha_1, \ldots, \alpha_n)$ is in Λ the n-tuple of fractional parts of $m(\alpha_1, \ldots, \alpha_n)$ must also be in Λ. But by choosing ϵ arbitrarily small, we find that Λ contains arbitrarily small vectors, which means that 0 is not an isolated point. This contradicts the fact that Λ is discrete. Hence $t = n$.