1. Minkowski's Theorem

Definition 1.1. *Let $n \geq 1$ be an integer. A free abelian group $L \subset \mathbb{R}^n$ such that*

$$L \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{R}^n$$

is called a lattice of rank n.

In other words, a lattice is a subgroup of $\mathbb{R}^n$ of the form

$$L = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_n,$$

where $v_1, \ldots, v_n$ are $\mathbb{R}$-linearly independent vectors. The collection $(v_1, \ldots, v_n)$ is called a *basis* of the lattice L. Given a lattice $L \subset \mathbb{R}^n$, and a choice of basis $(v_1, \ldots, v_n)$ of L, we define the *determinant* of L to be

$$d(L) = |\det(v_1, \ldots, v_n)|.$$

In some sense this should be thought of as a measure of how sparse the points of L are.

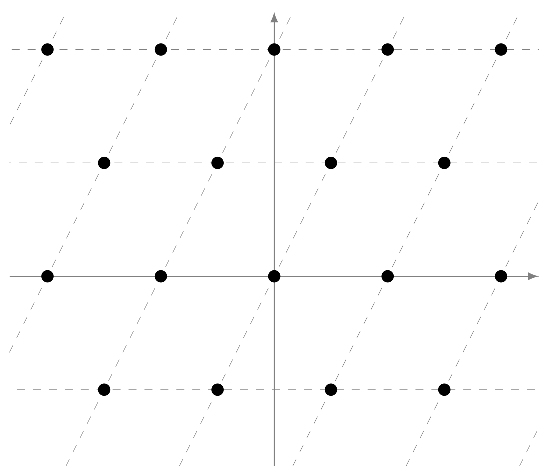

FIGURE 1. A lattice in $\mathbb{R}^2$.

Let $X \subset \mathbb{R}^n$. We say that X is *symmetric* if for all $x \in X$, we have $-x \in X$. We say X is *convex* if for all $x, y \in X$ the line segment spanned by x and y lies in X. Notice that in particular $0 \in X$, if X is convex and symmetrix. The point of Minkowski's Theorem, is that given a lattice $L \subset \mathbb{R}^n$, any large enough symmetric convex symmetric subset of $\mathbb{R}^n$ will contain a non-zero lattice point of L. As Hans Finkelnberg would say: "if we keep blowing up a balloon, it will eventually reach critical size, and be punctured by the lattice!". The question is now, "what is this critical size exactly?" Minkowski's Theorem tells us.

Theorem 1.2 (Minkowski)**.** *Let $L \subset \mathbb{R}^n$ be a lattice, and let $X \subset \mathbb{R}^n$ be a symmetric convex subset. If*

$$\mu(X) > 2^n d(L),$$

then X contains a non-zero lattice point of L. Here $\mu(X)$ denotes the Lebesgue-measure of X[1]

Proof. See [NS13, Chapter I, Theorem 4.4]. ■

There are two cute corollaries of this theorem listed below.

Corollary 1.3 (Fermat)**.** *Let $p > 2$ be a prime number. Then p is a sum of two squares if and only if $p \equiv 1 \mod 4$.*

Proof. See [ST16, Section 7.2] ■

Corollary 1.4 (Lagrange)**.** *Any positive integer is a sum of four squares.*

Proof. See [ST16, Section 7.3] ■

Besides these two corollaries, Minkowski's Theorem actually plays a very serious role in classical algebraic number theory. It is the key in the proof of finiteness of the class number of a number field and the Dirichlet Unit Theorem[2]. See [NS13, Chapter I].

2. Goals for a report

Prove Theorem 1.2. This usually comes down to a Lemma of Blichfeldt. Discuss applications of this Theorem. The two corollaries listed are a maybe a little too elementary on their own, but could serve as good side quests. It would be really cool if you could discuss some more advanced applications, such as finiteness of the class number and the Dirichlet unit Theorem.

2.1. **Prerequisites.** Besides basic linear algebra, none come to mind.

[1] If you have never heard of this, this is just the volume of X.

[2] Minkowski's Theorem can technically be avoided in these proofs by adopting the adèlic point of view. Regardless, the original proof of finiteness of the class number is useful, because it gives *Minkowski's bound*, which in turn can be used to actually compute the class number.

References

[NS13] Jurgen Neukirch and Norbert Schappacher. *Algebraic number theory*. 1999th ed. Vol. 322. Grundlehren der mathematischen Wissenschaften. Springer, 2013.

[ST16] Ian Stewart and David Tall. *Algebraic Number Theory and Fermat's last Theorem*. 4th ed. CRC Press, Taylor and Francis Group, 2016.