W8D2
15/12/14

Geom. of Nums.

For a bounded K containing a ball around the origin, we've defined $\Delta(K) = \inf\{d(\Lambda) \mid K \cap \Lambda = \{0\}\}$.

We've been studying $\Delta(B_2(0,1)) = \Delta_n$.

We now consider $(-1,1)^n = B_\infty(0,1)$. By Minkowski I, $\Delta(K) \geq 1$ and we get equality from $\Lambda = \mathbb{Z}^n$.

Ques. What are the critical lattices?

Prop Suppose $\Lambda = \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \mathbb{Z}^n$. Then $d(\Lambda) = 1$ and $K \cap \Lambda = \{0\}$.

pf. By induction. For $n=1$ $\Lambda = \mathbb{Z}$ and there's nothing to prove. O/W, Let $P: \mathbb{R}^n \to \mathbb{R}^{n-1}$, $P(x_1, \dots, x_n) = P(x_2, \dots, x_n)$. $P(\Lambda) \cap K_{n-1} \overset{\text{ind.}}{=} \{0\}$ and $d(P(\Lambda)) = 1$. So, if $\lambda \in K \cap \Lambda \setminus \{0\}$, $P(\lambda) = 0$ and so $\lambda = te_1$. But $t \in \mathbb{Z}$ since e_1 is part of a generating set - but then $\|te_1\|_\infty \geq 1$ in contradiction.

(Minkowski's) Conj. Up to a perm. of coordinates these are all the examples.

If $K \subseteq \mathbb{R}^n$ is as before, X_0 some set, K tiles $\mathbb{R}^n$ using trans. from X_0 (K, X_0 is a tiling) if $\forall y \in \mathbb{R}_n \exists x \in X_0, k \in \bar{K}$ s.t. $y = x + k$ $[\bar{K} + X = \mathbb{R}^n]$ and $\forall x, x' \in X_0$, $x \neq x'$ then $(x+K) \cap (x'+K) = \emptyset$.

If $X_0 = \Lambda$ a lattice the tiling is a lattice tiling. Alt. formulation of the same conj.: for $K = (-\frac{1}{2}, \frac{1}{2})^n$ and (K, Λ) is a lattice tiling, it has an element of the standard basis, ("two tiles touch face to face"). Some related conj.:

Keller conj. Any tiling of $\mathbb{R}^n$ by cubes contains a pair of face to face cube. Was shown true for dim ≤ 6. Turns out it's false for dim ≥ 8 (open for dim $= 7$).

Fürtwängler conj. Any k-tiling by cubes contains face-to-face cubes (stronger then Keller, so it's false).

k-tiling - any $y \notin X + \partial K$ is covered exactly k times.

A counterexample was first shown for $n=4$, $k=9$. Except for $n=7$, $k=1$, the values for which this is true are all known.

Recall Ω is a fund. dom. for Λ if $\overset{(i)}{\forall} y\in\mathbb{R}^n$ belongs to $\lambda+\Omega$ for some $\lambda\in\Lambda$, and $\overset{(ii)}{\text{the}}$ translates are disjoint.

Ex. If Ω_0 satisfies (ii) $\exists$ fund. dom. $\Omega\supseteq\Omega_0$.

Therefore, tiling $(K,\Lambda)\to Vol(\bar{K})\geq Vol(\Omega)=d(\Lambda)\geq Vol(K)$. If $Vol(\bar{K})=Vol(K)$ those must also be $d(\Lambda)$.

Prop. Let K be convex, cent. symm. & bounded. (K,Λ) a tiling $\iff$ $2K\cap\Lambda=\{0\}$ & $d(\Lambda)=Vol(K)$.

Pf. We saw (K,Λ) tiling $\Rightarrow d(\Lambda)=Vol(K)$. If $\lambda\in 2K\cap\Lambda\setminus\{0\}$ then $\lambda/2\in K$, $-\lambda/2\in K$. But then $\frac{\lambda}{2}\in 0+K$ & $\frac{\lambda}{2}=\lambda+(-\frac{\lambda}{2})\in\lambda+K$, so the translates aren't disjoint. For the converse, recall the notation of K-norm - $\|x\|_K=\sup\{t>0\mid x\notin tK\}=\inf\{t>0\mid x\in tK\}$.

~~Let $\Omega=\{x\in\mathbb{R}^n\}$~~ For each $y\in\mathbb{R}^n$ choose $\lambda=\lambda_y\in\Lambda$ for which $\|y-\lambda\|_K$ is minimized.

If $\|y-\lambda\|_K<1$ then $y\in\lambda+K$. If $\|y-\lambda\|_K=1$ then $y\in\lambda+\bar{K}$. If $\|y-\lambda\|_K>1$ then there's a ball U around y s.t. $\forall u\in U$, $\|u-\lambda\|_K\geq 1$. Then $U\cup K$ has disjoint translates, if we choose U sufficiently small. But $Vol(U\cup K)>Vol(K)=d$ so this isn't possible (by ex.). So $\mathbb{R}^n$ is covered by $\Lambda+\bar{K}$.

If $(\lambda+K)\cap(\lambda'+K)\neq\emptyset$ for $\lambda\neq\lambda'\in\Lambda$ then $\lambda-\lambda'\in\Lambda$ and also to $2K$ in contradiction. So (K,Λ) is a tiling.

This prop. shows the equiv. of the 2 Minkowski conjectures.

Let G be an $\overset{\text{finite}}{}$ abelian group. $A\subseteq G$ (not nec. subgroup) is cylic if $\exists a\in A$ s.t. $A=\{1,a,a^2,\dots a^{r-1}\}$. A factorization of G is a choice of $A_1,\dots,A_k\subseteq G$ s.t. $A_1\times\dots\times A_k\to G$, $(a_1,\dots,a_k)\mapsto a_1\dots a_k$ is a bijection.

Thm. If $A_1,\dots,A_k$ is a factorization of G to cyclic subsets, then at least one of the A_i's is a subgroup.

Remark If $A_1,\dots,A_k$ is a (nontrivial, $\forall i$ $A_i\neq\{1\}$) factorization to cyclic subsets, $A_i=\{1,a_i,\dots,a_i^{r_i-1}\}$, then $r_i\leq ord(a_i)$. Thm. states equality holds for at least one i.

Example Denote $C_n = \mathbb{Z}/_{n\mathbb{Z}}$. $G = C_4 = \langle a \rangle_4 = \{1, a, a^2, a^3\}$. Then

$\{1, a\}, \{1, a^2\}$ is a cyclic factorization. And indeed, $\{1, a^2\}$ is a subgroup.

The Minkowski conj. can be reduced to this fact:

Thm. If $\exists \Lambda$ a counterexample to Minkowski's conj, $\exists \Lambda'$ a counterexample in $\mathbb{Q}^n$. (Same for Keller, Fürtwanger).

This is hard to prove and we skip the proof. Based on thm,

pf. of Minkowski's conj. 2nd formulation

Assume Λ' is a rational counterexample. Let $R \in \mathbb{N}$ so that $R\Lambda' \subseteq \mathbb{Z}^n$. Let $G = \mathbb{Z}^n/_{R\Lambda'}$. $((-1/2, 1/2)^n, \Lambda')$ is a tiling, so $\forall y \in \mathbb{R}^n$ can be written uniquely as $y = \lambda + x$, $\lambda \in \Lambda'$, $x \in [0,1)^n$. Now let $e_1, \dots, e_n$ be the standard basis vectors and $u_1, \dots, u_n$ their image in G. Every $y \in \mathbb{R}^n$ can be expressed as $R\lambda + x$ where $\lambda \in \Lambda'$, $x \in [0, R)^n$. In particual, $\forall z \in \mathbb{Z}^n$ can be written as $z = R\lambda + x = R\lambda + \sum_{i=1}^{n} b_i e_i$, $b_i \in \{0, 1, \dots, R-1\}$. So G has a factorization $A_i = \{1, u_i, \dots, u_i^{R-1}\}$. By the prev. thm, $\exists i$ s.t. $\{1, u_i, \dots, u_i^{R-1}\}$ is a group. So, $u_i^{R} = 1$. So, $Re_i \in R\Lambda'$ so $e_i \in \Lambda'$.

We now go on to prove the thm. about cyclic factorization.

Recall $G = \oplus C_{p_i^{e_i}}$ (p_i prime). G is called a p-group if its order is a power of p ($\Rightarrow \forall i, p_i = p$).

We'll only prove for G a p-group.

First consider the case $G = \oplus C_{p} \Leftrightarrow \mathrm{ord}(g) = p$ for any $g \in G \setminus \{0\}$.

If $A_1 \dots A_k$ is a fact. then $|G| = |A_1| \cdot \ldots \cdot |A_k|$ so each $|A_i|$ is a power of p. Since A_i is cyclic so $|A_i| = p$, so each A_i is a subgroup.

Similarly for any group G, ~~each $|A_i|$ is a prime power~~;

Lemma we may assume $|A_i|$ prime.

pf. If $|A| = r \cdot s$ cyclic $(r, s > 1) \Rightarrow \exists B_1, B_2$ cyclic, $|B_1| = r, |B_2| = s$, $A = B_1 B_2$. If one of the B_i is a subgroup so will A be.

If $A = \{1, a, \dots, a^{rs-1}\}$ just take $B_1 = \{1, a, \dots, a^{r-1}\}$, $B_2 = \{1, a^r, \dots, a^{r(s-1)}\}$.

Lemma Suppose $\underbrace{p}_{G=AB}$ prime, $t \in \mathbb{N}$, $p \nmid t$. $G = AB$ where $A = \{1, a, \dots, a^{p-1}\}$.

Then $A' = \{1, a^t, \dots, a^{t(p-1)}\}_{\text{ }}$ (it may happen that $A' = A$).

pf. $G = AB = B \cup aB \cup a^2 B \dots a^{p-1} B$. Mult. by a to get

$G = aB \cup a^2 B \cup \dots \cup a^p B$. So, $B = a^p B$. So, $i \equiv j\ (p) \Rightarrow a^i B = a^j B$.

Now, for G a p-group, $A \subseteq G$. $|\langle A \rangle|$ is a power of p, p^r where $r = r(A)$.

Main Lemma G fin. ab. gr. $A \subseteq G$, $r(B) \geq |B|$ for any $B \subseteq A$, $r(A) = |A|$.

(pf. will be uploaded to the course site) Then $\forall a \in A\ \exists s = s_a$ a power of p s.t.

$\langle A \rangle = \bigoplus_{a \in A} \{1, a^{s_a}, a^{2s_a}, \dots, a^{(p-1)s_a}\}$. One of these sets is a subgroup.

Using this we can prove the thm:

Can assume $\forall i\ |A_i| = p$, $A_i = \{1, a_i, \dots, a_i^{p-1}\}$. For any s elements, one from each A_i, they generate a group of at least p^s.

But $|G| = p^k$ is generated by $a_1, \dots, a_n$. So we can apply the lemma for $A = \{a_1, \dots, a_k\}$. So, $\exists S_i$ a power of p, such that that $A_i' = \{1, a_i^{s_i}, \dots, a_i^{s_i(p-1)}\}$ is a factorization of G in which at least one is cyclic. If $s_1 = \dots = s_k = 1$ then $\forall i\ A_i = A_i'$ and we're done. o/w, $s_1, \dots, s_m \neq 1$, $s_{m+1} = \dots = s_k = 1$. So

$G = A_1' \dots A_m' A_{m+1} \dots A_k$ is a factorization with

$a_1 \dots a_m = a_1^{s_1 t_1} \dots a_m^{s_m t_m} a_{m+1}^{t_{m+1}} \dots a_k^{t_k}$. Equiv.

(*) $1 = a_1^{s_1 t_1 - 1} \dots a_m^{s_m t_m - 1} a_{m+1}^{t_{m+1}} \dots a_k^{t_k}$. But $s_i t_i - 1$ is relatively prime to p, so by prev. lemma $A_i^* = \{1, a_i^{s_i t_i - 1}, \dots, a_i^{(p-1)(s_i t_i - 1)}\}$, so

$A_1^* A_2^* \dots A_m^* A_{m+1} \dots A_k$ is a factorization - which contradicts (*).