ZAHLENTHEORIE NOTE 13

We want to prove Minkowski's bound.

- <u>LATTICES</u>

Let V be a real vector space of finite dimension.

<u>def</u>: LATTICE

A lattice in V is a subgroup $\Lambda \subseteq V$ generated by $\mathbb{R}$-linearly independent vectors:

$$\Lambda = \{ n_1 e_1 + \dots + n_r e_r \mid n_i \in \mathbb{Z} \}$$

$e_1, \dots, e_r$ linearly independent in V.

<u>Rmk</u>: (1) If Λ is as before, then $\Lambda \cong \mathbb{Z}^{\oplus r}$ as an abstract group.

The RANK of the lattice is the rank of Λ as an abelian group: in the above notation $\operatorname{rank}(\Lambda) = r$.

A lattice $\Lambda \subseteq V$ of rank $r = \dim V$ is called FULL.

(2) A set of $\mathbb{R}$-linearly independent elements which generate Λ is said to be an

INTEGRAL BASIS of Λ. If $\Lambda \subseteq V$ is a full lattice and $(e_1, \dots, e_n)$ and $(f_1, \dots, f_n)$ are two integral bases, then the change of base matrix is in $GL(\mathbb{Z})$.

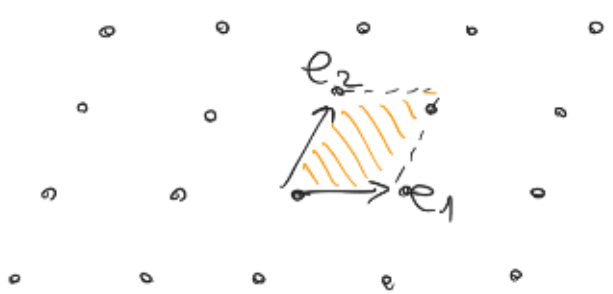
Another characterization of lattices is the following

<u>Prop</u>: Let $\Lambda \subseteq V$ be a subgroup.
Λ is a lattice $\iff$ Λ is discrete

<u>proof</u>: [MILNE, Prop 4.15]

<u>def</u>: FUNDAMENTAL PARALLELOPIPED
Let $\Lambda \subseteq V$ be a full lattice with an integral basis $e_1, \dots, e_n$. Then the fundamental parallelopiped of Λ w.r.t. $(e_1, \dots, e_n)$ is

$$D = \{ a_1 e_1 + \dots + a_n e_n \mid 0 \leq a_i < 1 \}$$



Observe that if D is a fundamental parallelepiped then

$$V = \bigsqcup_{\lambda \in \Lambda} (D + \lambda) \quad \left(\begin{array}{c}\text{two translates} \\ \text{are disjoint}\end{array}\right)$$

Now consider the case of $V = \mathbb{R}^n$, and $\Lambda \subseteq \mathbb{R}^n$ a full sublattice. Let also $e_1, \dots, e_n$ be an integral basis of Λ. Then the fundamental parallelepiped

$$D = \{ \sum a_i e_i \mid 0 \leq a_i < 1 \}$$

is a Lebesgue-measurable subset of $\mathbb{R}^n$ and its volume is given by

$$\mu(D) = |\det(e_1, e_2, \dots, e_n)|$$

(standard calculus fact).

<u>Rmk</u>: (1) If $e'_1, \dots, e'_n$ is another integral basis and D' is the corresponding fundamental parallelogram, then

$$\mu(D) = \mu(D')$$

indeed the change of base matrix is in $GL(\mathbb{Z})$ so it has determinant ± 1.

(2) If $\Lambda' \subseteq \Lambda \subseteq \mathbb{R}^n$ are two full sublattices

Then one can find a basis $e_1, \dots, e_n$ for Λ such that $d_1 e_1, \dots, d_n e_n$ with $d_i > 0$ positive integers is a basis of Λ'. (Smith normal form).
Hence, if D, D' are the respective fundamental parallelepiped, we have

$$\left| \Lambda / \Lambda' \right| = \frac{\mu(D')}{\mu(D)}$$

<u>Thm</u>: Let $\Lambda \subseteq \mathbb{R}^n$ be a full lattice, with fundamental parallelepiped D. Let also $S \subseteq \mathbb{R}^n$ be a measurable subset. If

$$\mu(S) > \mu(D)$$

then there are $\alpha, \beta \in S$, $\alpha \neq \beta$ s.t.

$$\alpha - \beta \in \Lambda.$$

<u>proof</u>: since $\mathbb{R}^n = \bigsqcup_{\lambda \in \Lambda} D + \lambda$, we have also

$$S = \bigsqcup_{\lambda \in \Lambda} S \cap (D + \lambda) \text{ so that}$$

$$\mu(S) = \sum_{\lambda \in \Lambda} \mu(S \cap (D + \lambda))$$

$$= \sum_{\lambda \in \Lambda} \mu((S - \lambda) \cap D)$$

Suppose the sets $(S - \lambda) \cap D$ are pairwise

disjoint in D. Then

$$\mu(S) = \sum_{\lambda \in \Lambda} \mu((S-\lambda)\cap D) = \mu\left(\bigcup (S-\lambda)\cap D\right) \leq \mu(D)$$

which is absurd. Hence there must be

$$v \in (S-\lambda)\cap(S-\lambda')\cap D \qquad \lambda \neq \lambda'$$

so $\quad v = \alpha - \lambda = \beta - \lambda' \quad$ for $\alpha, \beta \in S$

and

$$\alpha - \beta = \lambda - \lambda' \in \Lambda.$$

$$\lambda - \lambda' \neq 0.$$

<u>Thm</u>: [MINKOWSKI'S CONVEX BODY THEOREM]

Let $\Lambda \subseteq \mathbb{R}^n$ be a full lattice with fundamental parallelepiped D. Let also $T \subseteq \mathbb{R}^n$ be a convex, compact subset which is symmetric in the origin ($\alpha \in T \Rightarrow -\alpha \in T$). If

$$\mu(T) \geq 2^n \mu(D)$$

Then T contains a point in Λ different from 0.

<u>proof</u>: $\boxed{\mu(T) > 2^n \mu(D)}$: Let $S = \frac{1}{2}T = \{\frac{1}{2}\alpha \mid \alpha \in T\}$.

Then $\mu(S) = \frac{1}{2^n}\mu(T) > \mu(D)$ by hypothesis, so that the previous theorem tells

so that there are $\alpha, \beta \in S$ s.t.

$$\alpha - \beta \in \Lambda, \ \alpha - \beta \neq 0.$$

Since $\alpha, \beta \in S$ we have $\alpha = \frac{1}{2}\alpha'$, $\beta = \frac{1}{2}\beta'$ for $\alpha', \beta' \in T$, and then

$$\alpha - \beta = \frac{1}{2}(\alpha' - \beta')$$

Now we see that $\frac{1}{2}(\alpha' - \beta') \in T$: indeed $-\beta' \in T$ by symmetry, and then $\frac{1}{2}(\alpha' - \beta') \in T$ by convexity. (NO NEED T COMPACT)

$\boxed{\mu(T) = 2^n \mu(D)}$: since T is closed we have

$$T = \bigcap_{\rho > 1} \rho \cdot T$$

Each of the $\rho \cdot T$ is convex, symmetric, compact and $\mu(\rho T) > \mu(T) = 2^n \mu(D)$. Hence

$$\rho T \cap (\Lambda \setminus \{0\}) \text{ is nonempty}$$

by the previous case, and it is finite because it is compact and discrete.

So, the $\rho T \cap (\Lambda \setminus \{0\})$ are all nonempty finite subsets with $\rho_1 T \subseteq \rho_2 T$ if $\rho_1 \leq \rho_2$. Hence

$$T = \bigcap_{\rho > 1} \rho \cdot T \cap (\Lambda \setminus \{0\}) \neq \emptyset$$

as well. $\square$

- PROOF of MINKOWSKI'S BOUND

K = number field, $[K:\mathbb{Q}] = n$. Let

$\rho_1, \dots, \rho_r$ = real embeddings $K \hookrightarrow \mathbb{C}$

$\tau_1, \dots, \tau_s$ = complex embeddings $K \hookrightarrow \mathbb{C}$

$\bar{\tau}_1, \dots, \bar{\tau}_s$

This gives us a group embedding

$$\sigma : K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s$$
$$\alpha \longmapsto (\rho_1(\alpha), \dots, \rho_r(\alpha), \tau_1(\alpha), \dots, \tau_s(\alpha))$$

We have the usual isomorphism $\mathbb{C} \cong \mathbb{R}^2$ of $\mathbb{R}$-vector spaces given by the basis $(1, i)$ of $\mathbb{C}$, then we can look at

$$\mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^r \times \mathbb{R}^{2s} = \mathbb{R}^n$$

<u>Prop 1</u>: Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal. Then
$$\sigma(I) \subseteq \mathbb{R}^r \times \mathbb{C}^s$$
is a full lattice.

<u>proof</u>: we know that $I \subseteq \mathcal{O}_K$ is a subgroup. Since $\mathcal{O}_K$ is a free $\mathbb{Z}$-mod also I is a free $\mathbb{Z}$-module. Moreover $\mathcal{O}_K$ has rank n and $\mathcal{O}_K/I$ is finite hence I has rank n as well.

Let $\alpha_1, \dots, \alpha_n$ be a basis of I as a $\mathbb{Z}$-module.
we need to show that the vectors

$$\sigma(\alpha_1), \dots, \sigma(\alpha_n) \text{ are } \mathbb{R}\text{-linearly independent.}$$

Those vectors form the matrix

$$\begin{pmatrix} \rho_1(\alpha_1) & \rho_1(\alpha_2) & \dots & \rho_1(\alpha_n) \\ \rho_2(\alpha_1) & \rho_2(\alpha_2) & \dots & \rho_2(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \rho_r(\alpha_1) & \rho_r(\alpha_2) & \dots & \rho_r(\alpha_n) \\ \mathrm{Re}\,\tau_1(\alpha_1) & \mathrm{Re}\,\tau_1(\alpha_2) & \dots & \mathrm{Re}\,\tau_1(\alpha_n) \\ \mathrm{Im}\,\tau_1(\alpha_1) & \mathrm{Im}\,\tau_1(\alpha_2) & \dots & \mathrm{Im}\,\tau_1(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \mathrm{Re}\,\tau_s(\alpha_1) & \mathrm{Re}\,\tau_s(\alpha_2) & \dots & \mathrm{Re}\,\tau_s(\alpha_n) \\ \mathrm{Im}\,\tau_s(\alpha_1) & \mathrm{Im}\,\tau_s(\alpha_2) & \dots & \mathrm{Im}\,\tau_s(\alpha_n) \end{pmatrix} = A$$

and we need to show that this has determinant zero. However let's consider the matrix

$$\begin{pmatrix} \rho_1(\alpha_1) & \rho_1(\alpha_2) & \dots \\ \rho_2(\alpha_2) & \rho_2(\alpha_2) & \dots \\ \vdots & \vdots & \\ \rho_r(\alpha_1) & \rho_r(\alpha_2) & \dots \\ \tau_1(\alpha_1) & \tau_1(\alpha_2) & \dots \\ \overline{\tau}_1(\alpha_1) & \overline{\tau}_1(\alpha_2) & \dots \\ \vdots & \vdots & \\ \tau_s(\alpha_1) & \tau_s(\alpha_2) & \dots \\ \overline{\tau}_s(\alpha_1) & \overline{\tau}_s(\alpha_2) & \dots \end{pmatrix} = B$$

We know that

$$(\det B) = \operatorname{disc}(\alpha_1, \dots, \alpha_n) \neq 0$$

hence $\det B \neq 0$.

You can prove by row and column operations that

$$\det A = (-2i)^{-s} \cdot \det B$$

hence $\det A \neq 0$ as well. $\square$

<u>Prop 2</u>: Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal, and D a fundamental parallelepiped for the lattice $\sigma(I) \subseteq \mathbb{R}^r \times \mathbb{C}^s = \mathbb{R}^n$. Then

$$\mu(D) = \frac{1}{2^s} \cdot \|I\| \cdot \sqrt{|\Delta_K|}$$

<u>proof</u>: we keep the same notation of the previous proof. Since $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ is an integral basis of I, the volume of a fundamental parallelepiped is given by

$$\mu(D) = |\det A| = |(-2i)^{-s} \cdot \det B|$$

$$= \frac{1}{2^s} |\det B| = \frac{1}{2^s} |\operatorname{disc}(\alpha_1, \dots, \alpha_n)|$$

We need to show that

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \|I\| \cdot \sqrt{|\Delta_K|}$$

and this is in the Exercise sheet 9. $\square$

Prop 3: Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal. Then

I contains $\alpha \in I, \alpha \neq 0$ s.t.

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \|I\| \cdot \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \cdot \sqrt{|\Delta_K|}$$

<u>proof</u>: define a norm $\|\cdot\|_*$ on $\mathbb{R}^r \times \mathbb{C}^s$ by

$$\|(x_1, \dots, x_r, z_1, \dots, z_s)\|_* := \sum_{i=1}^{r} |x_i| + 2 \sum_{j=1}^{s} |z_j|$$

and consider the set

$$X_t = \{ v \in \mathbb{R}^r \times \mathbb{C}^s \mid \|v\|_* \leq t \}, \ t > 0$$

One can compute with some calculus [MILNE, Lemma 4.22] that

$$\mu(X_t) = 2^r \left(\frac{\pi}{2}\right)^s \left(\frac{t^n}{n!}\right)$$

so, if we choose $t > 0$ such that

$$t^n = \|I\| \cdot n! \frac{2^{n-r}}{\pi^s} \cdot \sqrt{|\Delta_K|}$$

<u>Prop 2</u> shows that $\mu(X_t) = 2^n \mu(D)$

Moreover X_t is convex, compact and symmetric around the origin, so Minkowski's convex body theorem shows that $\mu(X_t)$ contains a point $\sigma(\alpha)$ of the lattice $\sigma(I)$, $\sigma(\alpha) \neq 0$.

In other words, there is $\alpha \in I, \alpha \neq 0$ s.t.

$$\|\sigma(\alpha)\|_k \leq t$$

i.e.

$$\sum_{i=1}^{r} |\rho_i(\alpha)| + 2\sum_{j=1}^{s} |\tau_j(\alpha)| \leq t$$

Now, we see that

$$|N_{K/\mathbb{Q}}(\alpha)| = \prod_{i=1}^{r} |\rho_i(\alpha)| \cdot \prod_{j=1}^{s} |\tau_j(\alpha)| \cdot |\overline{\tau_j}(\alpha)|$$

$$= \prod_{i=1}^{r} |\rho_i(\alpha)| \cdot \prod_{j=1}^{s} |\tau_j(\alpha)|^2$$

and by the AM-GM inequality we get that

$$|N_{K/\mathbb{Q}}(\alpha)| \underset{\text{AM-GM}}{\leq} \left(\frac{\sum_{i=1}^{r} |\rho_i(\alpha)| + 2\sum_{j=1}^{s} |\tau_j(\alpha)|}{n} \right)^n \underset{\sigma(\alpha) \in X_t}{\leq} \frac{t^n}{n^n}$$

By our choice of t, we get what we want. $\square$

We conclude with the proof of Minkowski's bound

<u>Proof of Minkowski's bound</u>: Let J be a fractional ideal of $\mathcal{O}_K$. We need to show that the class of J in $Cl(K)$ is represented by an ideal $I \subset \mathcal{O}_K$ s.t.

in $Cl(K)$ is represented by an ideal $I \subseteq \mathcal{O}_K$ s.t.

$$\|I\| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\Delta_K|} =: B_K$$

There is $d \in \mathcal{O}_K$, $d \neq 0$ s.t. $M = dJ^{-1} \subseteq \mathcal{O}_K$ is an ideal. then there is an $\alpha \in dJ^{-1}$, $\alpha \neq 0$ s.t.

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \|M\| \cdot B_K$$

Since $\alpha \mathcal{O}_K \subseteq M$, we have $I = \alpha \cdot M^{-1} = \alpha \cdot d^{-1} J \subseteq \mathcal{O}_K$ is an ideal. Clearly $I = \alpha d^{-1} \cdot J$ has the same class of J in $Cl(K)$, moreover

$$\|I\| \cdot \|M\| = \|I \cdot M\| = \|\alpha \mathcal{O}_K\|$$

$$= |N_{K/\mathbb{Q}}(\alpha)| \leq \|M\| \cdot B_K$$

hence $\|I\| \leq B_K$. $\square$

Ultima modifica: 13:24