4.3. ~~[illegible]~~ Rings of integers

If K is a number field (of degree n) with r_1 real emb. and r_2 pairs of complex emb., combine them to $K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$

as $\mathbb{R}$-vector spaces using $\mathbb{C} \cong \mathbb{R}^2$, $a+bi \leftrightarrow (a,b)$

$\mathcal{O}_K$ is a full lattice in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with

$$\mathrm{covol}(\mathcal{O}_K) = 2^{-r_2} \cdot |\mathrm{disc}(K)|^{1/2}.$$

Any fractional ideal $\mathfrak{a}$ is a full lattice with

$$\mathrm{covol}(\mathfrak{a}) = \mathrm{Nm}(\mathfrak{a}) \cdot \mathrm{covol}(\mathcal{O}_K).$$

We use the norm

$$\|(a_1, \ldots, a_{r_1}, b_1, \ldots, b_{r_2})\| = \max(|a_1|, \ldots, |a_{r_1}|, |b_1|, \ldots, |b_{r_2}|)$$

on $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

Rmk 4.3.1 $\|xy\| \le \|x\| \cdot |y|$

Lemma 4.3.2 $\lambda_1(\mathcal{O}_K) = 1$

Pf "$\le$": $|1| = 1$, $1 \in \mathcal{O}_K$. "$\ge$": For any $0 \ne x \in \mathcal{O}_K$, $1 \le |\mathrm{Nm}(x)| = \prod_{\sigma: K \hookrightarrow \mathbb{C}} |\sigma(x)|$.

$\Rightarrow |\sigma(x)| \ge 1$ for some σ $\Rightarrow |x| \ge 1$. $\square$

Ex Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ for primes $p<q$.

Then,

$$\lambda_2(\mathcal{O}_K) \asymp \sqrt{p},$$
$$\lambda_2(\mathcal{O}_K) \asymp \sqrt{q},$$
$$\lambda_3(\mathcal{O}_K) \asymp \sqrt{pq}.$$

Pf "$\ll$" $1, \sqrt{p}, \sqrt{q}, \sqrt{pq} \in \mathcal{O}_K$ lin. indep.

"$\gg$" follows because $\lambda_1\lambda_2\lambda_3\lambda_4 \asymp \text{covol} \asymp |\text{disc}(K)|^{1/2} \overset{\uparrow \text{HW}}{\asymp} pq$. $\square$

~~Ex picked a random monic pol. $f \in \mathbb{Z}[X]$ of deg. n~~

Rmk If you order degree n number fields K (with Galois group S_n) by $|\text{disc}(K)|$, it is expected that $\mathbb{P}_K(\lambda_n(\mathcal{O}_K)/\lambda_2(\mathcal{O}_K) \le c) \xrightarrow[c\to\infty]{} 1$.
(known for $n \le 5$ by Bhargava, Harron: The equidist. of lattice shapes of rings of int. in cubic, quartic, quintic)

Def A number field K is primitive if there is no field $\mathbb{Q} \subsetneq F \subsetneq K$.

Ex a) A number field of prime degree.

b) A number field of degree n with Galois group (of the Galois closure) S_n.

Thm 4.3.3 If K is primitive, then

$$\lambda_{i+j-1}(\mathcal{O}_K) \le \lambda_i(\mathcal{O}_K)\lambda_j(\mathcal{O}_K) \quad \forall\, 1 \le i,j \le n \text{ with } i+j-1 \le n.$$

This follows from:

Lemma 4.3.4 (Multiplicative Kneser's Theorem: Hou, Leung, Xiang: A generalisation of an addition theorem of Kneser)

Let K be primitive, consider $\mathbb{Q}$-vector spaces $0 \ne A, B \subseteq K$.

$$\Rightarrow \dim(\underbrace{A \cdot B}_{\substack{\mathbb{Q}\text{-vector space} \\ \text{spanned by } a\cdot b \text{ for } a\in A,\, b\in B}}) \ge \min(\dim(A) + \dim(B) - 1, \dim(K)).$$

Pf of Thm Let $v_1, v_2, \dots, v_n$ be a directional basis,

$A_i = \langle v_1, \dots, v_i \rangle$.

By the lemma, $\dim(A_i \cdot A_j) \geq i+j-1$.

$A_i \cdot A_j$ is spanned by elements $v_r v_s \in \mathcal{O}_K$ with $r \leq i$, $s \leq j$.

$$|v_r v_s| \underset{\text{Remark 4.3.1}}{\leq} |v_r| \cdot |v_s| = \lambda_r \lambda_s \leq \lambda_i \lambda_j.$$

$$\Rightarrow \lambda_{i+j-1} \leq \lambda_i \lambda_j \qquad \square$$

Pf of Lemma by induction over $\dim(A)$.

$\dim(A) = 1$ is clear, so assume $\dim(A) \geq 2$. Fix $a, a' \in A$ lin. indep.

For $0 \neq b \in B$, let $V_{ab} = Ab \cap aB$,
$W_{ab} = Ab + aB$.

Case 1: $V_{a,b} = Ab$. $\forall 0 \neq b \in B$

$\Rightarrow Ab \subseteq aB \quad \forall 0 \neq b \in B$

$\Rightarrow A \cdot B \subseteq aB$. $\Rightarrow \frac{a'}{a} \cdot B \subseteq B \Rightarrow \underbrace{\mathbb{Q}\left(\frac{a}{a'}\right)}_{= K \text{ because } \frac{a}{a'} \notin \mathbb{Q},\ K \text{ primitive}} \cdot B \subseteq B \quad \Rightarrow B = K \Downarrow A \cdot B = K$

~~Let $a' \in A$ lin. indep. from~~

Case 2: $V_{a,b} \subsetneq Ab$ for some $0 \neq b \in B$

Apply the ind. hypothesis to $\underset{\neq 0}{V_{a,b}}$ and $\underset{\neq 0}{W_{a,b}}$: ($V_{a,b} \subsetneq Ab$, $W_{a,b} \supsetneq ab$)

$$\dim(A \cdot B) \geq \dim(\underbrace{V_{ab} \cdot W_{ab}}_{\subseteq abA \cdot B}) \geq \min(\underbrace{\dim(V_{ab}) + \dim(W_{ab})}_{= \dim(Ab) + \dim(aB) = \dim(A) + \dim(B)} - 1, \dim(K)) \qquad \square$$

Reference: Vemulapalli: Bounds on succ. min. of orders in n. f.
and scrollar invariants of curves

5. Fundamental domains

We will want to count orbits of an action $G \circlearrowright X$.

For example: $\mathcal{O}_K^\times \circlearrowright \mathcal{O}_K$ by left mult.

$GL_2(\mathbb{Z}) \circlearrowright \{$binary forms $f(x,y)$ of degree n with integer coefficients$\}$

Idea: count lattice points in a fundamental domain.
We'll use <u>weighted</u> fund. dom.
Let G act on fct. $f: X \to \mathbb{R}_{\geq 0}$ by $(gf)(x) = f(g^{-1}x)$.

(so $g\mathbb{1}_A = \mathbb{1}_{gA}$.)

<u>Def</u>: A <u>fund. dom.</u> for $G \circlearrowright X$ is a fct. $f: X \to \mathbb{R}_{\geq 0}$ s.t.

$$\sum_{g \in G} gf = 1.$$

[only allow nonneg. values to avoid issues with conditional convergence]

<u>Ex</u> If G is finite, $f(x) = \frac{1}{\#G}$ is the trivial <u>fund. dom.</u>

<u>Ex</u> $f = \mathbb{1}_{[0,1)}$ fund. dom. for $\mathbb{Z} \circlearrowright \mathbb{R}$ (addition)

~~$f = \mathbb{1}_{\text{fund. cell for}}$~~

<u>Ex</u> Λ full lattice in $\mathbb{R}^n$ with fund. cell C
$\mathbb{1}_C$ fund. dom. for $\Lambda \circlearrowright \mathbb{R}^n$ (addition)

<u>Ex</u> $f(x) = \begin{cases} 1 & , x > 0 \\ 1/2 & , x = 0 \\ 0 & , x < 0 \end{cases}$ for $\{\pm 1\} \underset{\text{mult.}}{\circlearrowright} \mathbb{R}$.

<u>Ex</u> $\mathbb{1}_{\text{squarefree int.}}$ fund. dom. for $\mathbb{Q}^{\times 2} \underset{\text{mult.}}{\circlearrowright} \mathbb{Q}^\times$

Rmk a) If $\# Stab(x) < \infty$ $\forall x$, and $S \subseteq X$ is a set containing exactly one (3) el. of each orbit, ~~then f is a fund. dom. if and only if~~

then $f(x) := \begin{cases} 1/\# Stab(x), & x \in S \\ 0, & x \notin S \end{cases}$

is a fund. dom.

b) Otherwise, there is no fund. dom.

Lemma 5.1 All fund. dom. f_1, f_2 for $G \curvearrowright X$ have the same size: $\sum_{x \in X} f_1(x) = \sum_{x \in X} f_2(x)$.

Cor $\sum_{x \in X} f(x) = \sum_{\text{orbit } Gx} \frac{1}{\# Stab(x)} \underbrace{= \frac{\# X}{\# G}}_{\text{if } G \text{ is finite}}$

Rmk a) If f is a fund. dom. for $G \curvearrowright X$, then $f \cdot 1_A$ is a fund. dom. for $G \curvearrowright A \subseteq X$.

b) If f is a fund. dom. for $G \curvearrowright X$, then gf — " — — " — for all $g \in G$.

Generalising Lemma 5.1 :

<u>Lemma 5.2</u> Let G be a countable group with a measure-preserving action on a measure space X. ($\mathrm{vol}(gA) = \mathrm{vol}(A)$)

Then, any two measurable fund. dom. f_1, f_2 have the same volume:

$$\int_X f_1(x)\,dx = \int_X f_2(x)\,dx$$

<u>Pf</u> HW $\square$

We call this integral (if there is a measurable fund. dom.) the <u>volume</u> of $G\backslash X$:

$$\mathrm{vol}(G\backslash X) = \int_X f(x)\,dx$$

[Lemma is the case of the counting measure]

<u>Ex</u>: Any two fund. cells for Λ have the same volume.

[Often, it's not so easy to pick a single repr. of each orbit. Easier to construct:]

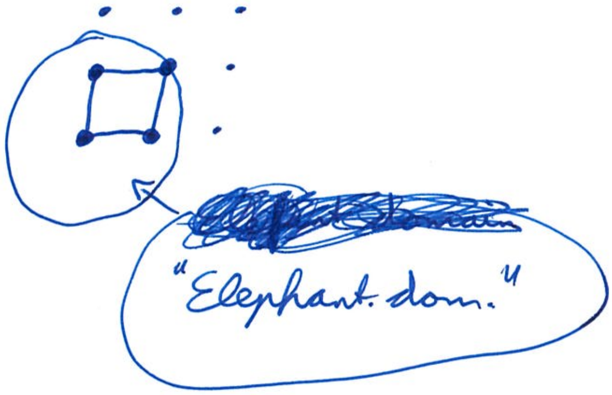
<u>Def</u> An <u>almost fund. dom.</u> (alephfund. dom.) for $G \curvearrowright X$ is a set $S \subseteq X$ such that $1 \leq \#\{g \in G \mid gx \in S\} < \infty$ for all $x \in X$.

<u>Rmk</u> This is equiv. to $\#\mathrm{Stab}(x) < \infty$ and $1 \leq \#(S \cap Gx) < \infty$.

<u>Def</u> The <u>associated fund. dom.</u> is

$$f(x) = \begin{cases} 1/\#\{g \in G \mid gx \in S\}, & x \in S \\ 0, & x \notin S. \end{cases}$$

<u>Ese</u> For any full lattice Λ, a suff. large ball $D(R)$ is an almost fund. dom. for $\Lambda \curvearrowright \mathbb{R}^n$.



<u>Ese</u> $\mathbb{Z} \curvearrowright \mathbb{R}$

$$S=[0, 1.5]$$

<u>Lemma 5.3</u> Let G be countable, with a measure-preserving action on X. If S is a measurable ~~almost fund. dom.~~ almost fund. dom., then f is measurable.

(the assoc. f.d.)

<u>Pf</u> For any finite $I \subseteq G$, $A_I := \bigcap_{g \in I} gS$ is measurable.

$\Rightarrow$ For any $k \geq 0$, $B_k := \bigcup_{\substack{id \in I \subseteq G \\ \# I = k}} A_I$ is measurable.

$\Rightarrow$ $\{x \in X \mid f(x) = \frac{1}{k}\} = B_k \setminus B_{k+1}$ is measurable.

$\Rightarrow$ f is measurable. $\square$