3.2. Over $\mathbb{Z}$

~~Identify monic pol. $f \in \mathbb{Z}[X]$ of degree n with vectors in~~

Identify $\{\text{monic deg. } n \text{ pol. } f \in \mathbb{Z}[X]\}$ with $\mathbb{Z}^n$

$$X^n + a_{n-1}X^{n-1} + \dots + a_0 \qquad (a_{n-1}, \dots, a_0)$$

and order them by any norm on $\mathbb{R}^n$.

Thm 3.2.1

$$\mathbb{P}_{\substack{f \in \mathbb{Z}[X] \\ \text{monic} \\ \text{degree } n}} (f \text{ has Galois group } S_n) = 1$$

i.e.: f is irred. and the Galois closure of $\mathbb{Q}[X]/f(X)$ over $\mathbb{Q}$ has group S_n

Lemma 3.2.2

$$\mathbb{P}(f \bmod p \text{ doesn't have splitting type } (k_1, \dots, k_r) \text{ for any } p) = 0$$

[as long as $k_1 + \dots + k_r = n$]

Pf $\text{LHS} \leq \prod_p (1 - \underbrace{\mathbb{P}(\text{has splitting type } (k_1, \dots, k_r) \bmod p)}_{\xrightarrow[p \to \infty]{} \mathbb{P}_{\pi \in S_n}(\text{cycle type } (k_1, \dots, k_r)) > 0}) = 0$

(by Thm 3.1.1)

$\square$

Pf of Thm

~~G must contain~~

Recall:
If $f \bmod p$ has splitting type $(k_1, \dots, k_r)$, then $\mathrm{Frob}(p) \in \mathrm{Gal}(f)$ has cycle type $(k_1, \dots, k_r)$.

$\Rightarrow$ With prob. 1, $\mathrm{Gal}(f) \subseteq S_n$ contains an element of every cycle type.

Any 2-cycle, $(n-1)$-cycle, and n-cycle together generate S_n.

$\square$

Rmk Using the large sieve (cf. Serre: Lectures on the Mordell–Weil Theorem, Chapter 12), one can show:

$$\#\{ f \in \mathbb{Z}[x] \text{ monic deg } n \mid f \text{ has Gal. grp. } \neq S_n \text{ and } \|f\| \leq T \}$$

$$\ll T^{n-\frac{1}{2}} \log T,$$

whereas

$$\#\{ f \in \mathbb{Z}[x] \text{ monic deg } n \mid \|f\| \leq T \} \asymp T^n .$$

Rmk Using the Lang-Weil bound / étale cohomology, one can

Chebotarev's sister

also deal with ~~special~~ families of special polynomials.

For example: (you can show this without Lang-Weil!!)
The pol. $f_T(X) = X^3 - TX + (T-3)X + 1$ has Gal. grp. $A_3 \subseteq S_3$ over $\mathbb{Q}(T)$.
For any $t \in \mathbb{F}_q$, the pol. $f_t(X) = X^3 - tX + (t-3)X + 1$ has Galois group 1 (=splits completely) or A_3 (irreducible), if f_t is sqfree.

$$\lim_{q\to\infty} \mathbb{P}_{t\in\mathbb{F}_q}(f_t \text{ splits completely}) = \mathbb{P}_{\pi\in A_3}(\pi = id) = \frac{1}{3}$$

$$\lim_{q\to\infty} \mathbb{P}(f_t \text{ irreducible}) = \mathbb{P}(\pi \neq id) = \frac{2}{3}.$$

$$\mathbb{P}_{t\in\mathbb{Z}}(f_t \text{ irred. with Gal. grp } A_3) = 1$$

4. Lattices

~~4.1. Successive minima~~

Def A rank r lattice in $\mathbb{R}^n$ is a subgr. Λ generated by r linearly indep. vectors $\underbrace{b_1, \dots, b_r}_{\text{basis of } \Lambda} \in \mathbb{R}^n$.

A full lattice in $\mathbb{R}^n$ is a rank n lattice.

The covolume of a full lattice is $\mathrm{covol}(\Lambda) = \left| \det \begin{pmatrix} -b_1- \\ \vdots \\ -b_n- \end{pmatrix} \right|$

$$= \mathrm{vol}\Big(\underbrace{\{ x_1 b_1 + \dots + x_n b_n \mid 0 \le x_i < 1 \ \forall i \}}_{\text{a fundamental cell of } \Lambda} \Big)$$

4.1. Successive minima

Let $D(R) := \{x \in \mathbb{R}^n : |x| \le R\}$.

<u>Def</u> Fix a norm $|\cdot|$ on $\mathbb{R}^n$. For $i = 1, \dots, r$, the <u>i-th successive minimum</u> of a rank r lattice Λ is $\lambda_i(\Lambda) := \min\{t \ge 0 \mid \exists\, v_1, \dots, v_i \in \Lambda$ linearly indep. of norm $\le t\}$.

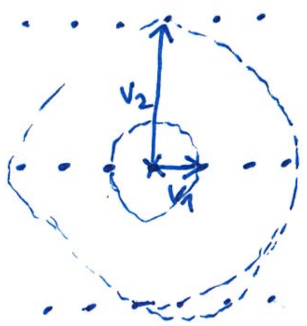
(w.r.t. $|\cdot|$)

<u>Rmk</u> a) $0 < \lambda_1 \le \dots \le \lambda_n$

b) There are lin. indep. vectors $v_1, \dots, v_n \in \Lambda$ with $|v_i| = \lambda_i \ \forall i$.
(Such a basis $(v_1, \dots, v_n)$ is a <u>directional basis</u> w.r.t. $\Lambda, |\cdot|$.)

c) If $\lambda'_1, \dots, \lambda'_n$ are the succ. min. w.r.t. $|\cdot|'$, then $\lambda_i \asymp_{|\cdot|, |\cdot|'} \lambda'_i \ \forall i$ by the equivalence of norms.

<u>Warning</u> For $n \ge 3$, there might be no directional basis that spans Λ! (HW)



Let $K = D(1)$.

<u>Rmk</u> a) K is compact convex centrally symmetric set.

b) For any cpt. conv. c.s. set $K \subset \mathbb{R}^n$, there is a norm:
$|v| := \min\{t \ge 0 \mid v \in tK\}$.

[Well-known:]

Thm 4.1.1 (Minkowski's first ~~theorem~~) Let Λ be a full lattice.

If $$\frac{\mathrm{vol}(K)}{2^n \cdot \mathrm{covol}(\Lambda)} \geq 1, \text{ then } \lambda_1(\Lambda) \leq 1.$$

(i.e. $\exists\, 0 \neq v \in \Lambda \cap K$)

This is a corollary of:

Thm 4.1.2 (Minkowski's second) Let Λ be a full lattice.

$$\frac{1}{n!} \leq \lambda_1 \cdots \lambda_n \cdot \frac{\mathrm{vol}(K)}{2^n \cdot \mathrm{covol}(\Lambda)} \leq 1.$$

In particular, $\lambda_1 \cdots \lambda_n \asymp_n \dfrac{\mathrm{covol}(\Lambda)}{\mathrm{vol}(K)}$. ["nearly orthogonal vectors"]

Pf $\frac{1}{n!} \leq \dots$

Let $v_1, \dots, v_n$ be a directional basis.

$\Lambda \supseteq \Lambda' :=$ lattice spanned by $v_1, \dots, v_n$.

$\mathrm{covol}(\Lambda) \leq \mathrm{covol}(\Lambda')$

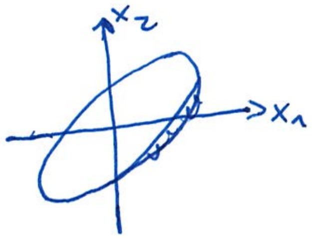
$K \supseteq K' :=$ convex hull of $\pm \frac{v_1}{\lambda_1}, \dots, \pm \frac{v_n}{\lambda_n}$.

$$\mathrm{vol}(K) \geq \mathrm{vol}(K') = \frac{2^n}{n!} \cdot \det \begin{pmatrix} - v_1/\lambda_1 - \\ \vdots \\ - v_n/\lambda_n - \end{pmatrix} = \frac{2^n \mathrm{covol}(\Lambda')}{n!\, \lambda_1 \cdots \lambda_n} \geq \frac{2^n \mathrm{covol}(\Lambda)}{n!\, \lambda_1 \cdots \lambda_n}$$

$\ldots \leq 1$

W.l.o.g. $v_1, \ldots, v_n$ are the standard basis of $\mathbb{R}^n$.

Let $U = B(1) = \{v \in \mathbb{R}^n : |v| < 1\}$.



We might try to scale U by a factor λ_i in the i-th coordinate direction, but that won't quite work! Instead, we apply an ingenious nonlinear transformation h.

Claim: There is a cont. fct. $h : U \to \mathbb{R}^n$ such that for $i = 1, \ldots, n$:

a) The i-th coord. of $h(x_1, \ldots, x_n)$ is $\lambda_i x_i + g_i(x_{i+1}, \ldots, x_n)$ for some fct. $g_i : \mathbb{R}^{n-i} \to \mathbb{R}$.

b) $h(x_1, \ldots, x_n) \in \lambda_i U + g_i'(x_{i+1}, \ldots, x_n)$ for some fct. $g_i' : \mathbb{R}^{n-i} \to \mathbb{R}^n$.

This suffices:

a) $\Rightarrow vol(h(U)) = \lambda_1 \cdots \lambda_n \cdot vol(U) = \lambda_1 \cdots \lambda_n vol(K)$.

Let $a \neq b \in U$, say $a_i \neq b_i$, $a_{i+1} = b_{i+1}, \ldots, a_n = b_n$.

By a), the i-th coord. of $p(a,b) := \frac{h(a) - h(b)}{2}$ is $\lambda_i(a_i - b_i) \neq 0$.

By b) and the triangle ineq., $|p(a,b)| < \lambda_i$

$\Rightarrow p(a,b) \notin \Lambda$ by def. of succ. min.

$\Rightarrow$ No two points in $U' := \frac{h(U)}{2}$ differ by an el. of Λ.

$\Rightarrow vol(U') \leq covol(\Lambda)$

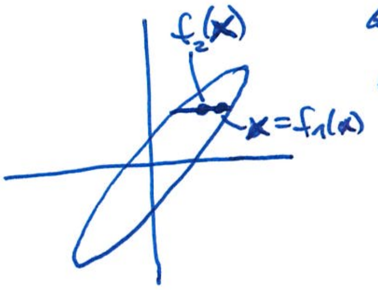
$$vol(U') = \frac{\lambda_1 \cdots \lambda_n}{2^n} \cdot vol(K)$$

To prove the claim:

Let $S_i := \mathbb{R}v_1 + \dots + \mathbb{R}v_i$.

Let $f_i : U \longrightarrow U$

$x \longmapsto$ centroid of the convex set $U \cap (x + S_{i-1})$



$f_i(a)$ only depends on $a_i, \dots, a_n$

and the last coord of $f_i(a)$ are $a_i, \dots, a_n$.

Let $h : U \longrightarrow \mathbb{R}^n$

$x \longmapsto \lambda_1 f_1(x) + (\lambda_2 - \lambda_1) f_2(x) + \dots + (\lambda_n - \lambda_{n-1}) f_n(x)$

The last $n-i$ summands only depend on $x_{i+1}, \dots, x_n$.

a): The i-th coord. of the first i summands sum to

$\lambda_1 x_i + (\lambda_2 - \lambda_1) x_i + \dots + (\lambda_i - \lambda_{i-1}) x_i = \lambda_i x_i$

b): The sum of the first i summands has norm

$< \lambda_1 + (\lambda_2 - \lambda_1) + \dots + (\lambda_i - \lambda_{i-1}) = \lambda_i$ by the triangle inequality because $|x| < 1$ (as $x \in U$). □