Lattices

PS2 is posted (due Oct 22).

From BallotTrax Notifications <updates@caballottrax.com>
Subject **2020 General Election: Ballot Status Update**
Reply to Vote-By-Mail Team <votebymail@sdcounty.ca.gov>
To kskedl@gmail.com

Hello KIRAN KEDLAYA,

This is a message from San Diego Registrar of Voters. Your ballot for the 2020 General Election was received and will be counted. Thank you for voting!

Share that you voted!

Facebook | Twitter

Lattices in rational vector spaces

V = finite dim. $\mathbb{Q}$-vector space

$L \subset V$ is a lattice if

L is a finitely generated free $\mathbb{Z}$-submod. "bdd"

which spans V over $\mathbb{Q}$.

e.g. for K a number field,

$\mathcal{O}_K$ is a lattice in K

Lattices in Euclidean spaces

V is a finite-dim'l $\mathbb{R}$-vecspace with a positive-definite inner product

$L \subset V$ is a complete lattice if L is a fin.gen. discrete $\mathbb{Z}$-submodule of V whose $\mathbb{R}$-span is V. (so not $\mathbb{Z}+\mathbb{Z}\sqrt{2} \subset \mathbb{R}$)

$\operatorname{rank} L = \dim_{\mathbb{R}} V$

$\Longleftrightarrow$

V/L is compact.

Lattices in the wider world

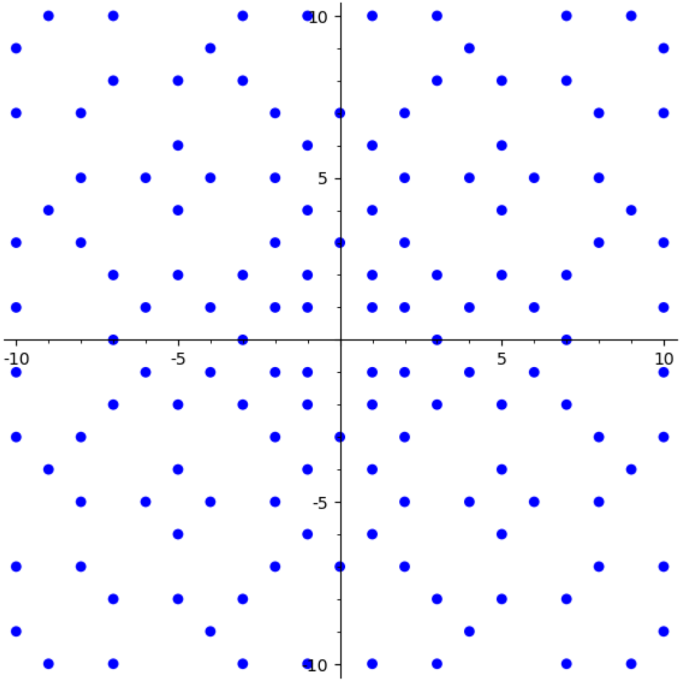
- Chemistry and materials
- Telecommunications/coding theory
- Cryptography (especially post-quantum)

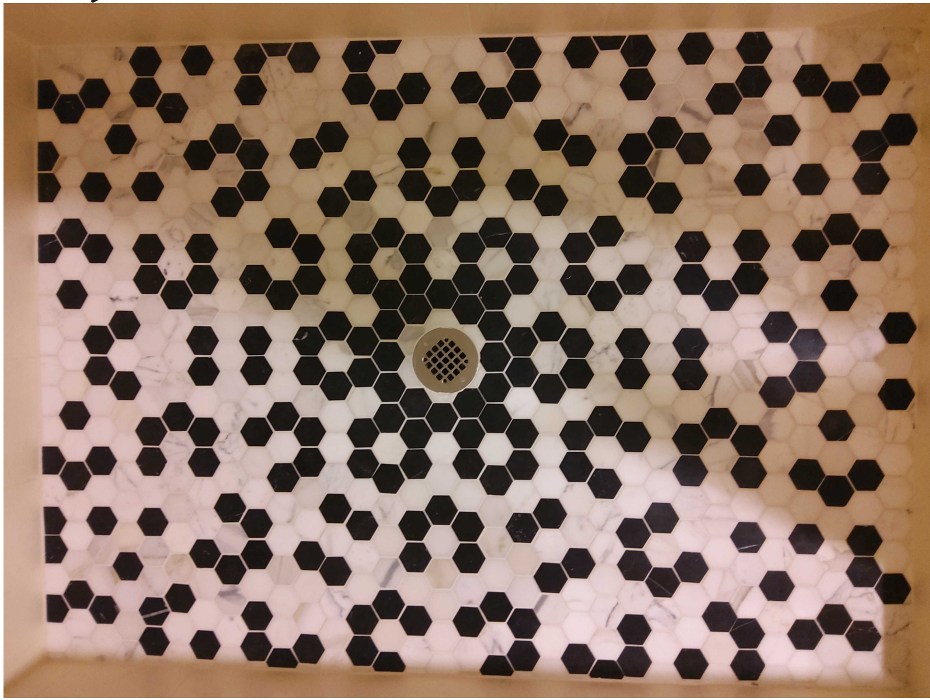
Conway & Sloane

Sphere packings, lattices & groups (SPLAG)

The lattice of a number field: imaginary quadratic case

$\langle z_1, z_2 \rangle = \underline{c}\, \mathrm{Re}(\bar{z}_1 \cdot z_2)$

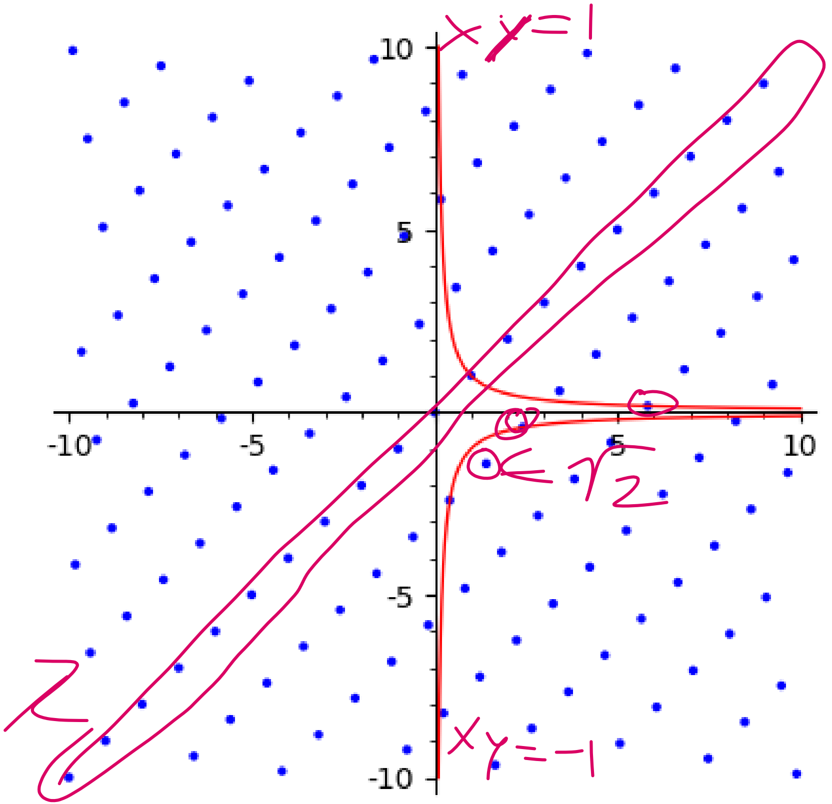




The lattice of a number field: real quadratic case

$$\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}\times\mathbb{R}$$

$$(a+b\sqrt{2}) \mapsto (a+b\sqrt{2}^{+},\ a-b\sqrt{2}^{+})$$




```
l = [(a+b*sqrt(2.0), a-b*sqrt(2.0)) for a in range(-10,10) for b in
range(-10,10)]
l = [(x,y) for x,y in l if abs(x) <= 10 and abs(y) <= 10]
list_plot(l, aspect_ratio=1) + plot(1/x,(x,0.1,10), color="red") +
plot(-1/x,(x,0.1,10), color="red")
```

The signature of a number field

$\mathbb{Q}(2^{1/3}) \sim (1,1)$

For K a number field with $[K:\mathbb{Q}]=n$, the **signature** of K is the pair (r_1, r_2)

$r_1 = \#$ of real embeddings: $K \hookrightarrow \mathbb{R}$

$r_2 = \#$ of pairs of complex embeddings: $K \hookrightarrow \mathbb{C}$

$\| \quad K \hookrightarrow \mathbb{C}$ 2:cc

Note: $\boxed{r_1 + 2r_2 = n}$

e.g. $n=2$

real quadratic $=(2,0)$, imag quadratic $=(0,1)$

The additive lattice of a number field

K (Minkowski)

$$j : K \longrightarrow K_{\mathbb{C}} = \prod_{\tau} \mathbb{C}$$

$\tau : K \to \mathbb{C}$ runs over n complex embeddings

$$a \longmapsto j(a) = (\tau(a))_{\tau}$$

$K_{\mathbb{C}}$ carries standard Hermitian innerproduct

$$\langle x, y \rangle = \sum \overline{x_{\tau}} y_{\tau}$$

$F : K_{\mathbb{C}} \to K_{\mathbb{C}}$ complex conjugation

$$(F(z))_{\tau} = \overline{z_{\overline{\tau}}} \qquad \overline{\tau} = c \circ \tau$$

$K_{\mathbb{R}} = F$-invariants of $K_{\mathbb{C}}$. $\underset{\sim}{\mathcal{O}_K} \subseteq K \hookrightarrow \underline{K_{\mathbb{R}}}$, restrict inner product.

The trace pairing revisited

The covolume of a Euclidean lattice

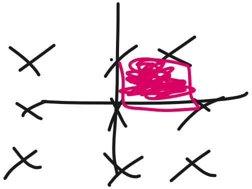
Image is discrete: For $a \in O_K$, $a \neq 0$, $\prod |j(a)| = \left|\mathrm{Norm}_{K/\mathbb{Q}}(a)\right| \geq 1$.

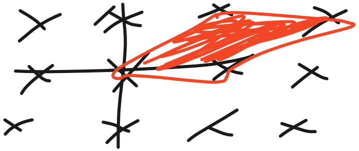
$L \subset V \leftarrow$ Euclidean space

lattice

inner product $\rightsquigarrow$ normalization of volume measure on V

covolume of L = volume of a fundamental domain of L





= volume of V/L for induced measure.

The absolute discriminant as a covolume

$L \subset V$ lattice in Euclidean space

$\alpha_1, \ldots, \alpha_n \in L$ basis

then covolume $= \left|\det(\langle \alpha_i, \alpha_j \rangle_{i,j})\right|^{1/2}$

In case of $\mathcal{O}_K \subset K_{\mathbb{R}}$,

$(\text{Covolume})^2 = |\text{discriminant}|$!

similarly if $I =$ ideal

$(\text{covolume of } I)^2 = |\text{discriminant of } I|$

$= |\text{disc } \mathcal{O}_K| \cdot [\mathcal{O}_K : I]^2$

e.g. for Gaussian lattice,

$|\text{covolume}|^2 = 4$, not 1.

$(\operatorname{disc} = -4)$