Day 2 scribbles

July 20, 2020 1:14 PM

Geometry of Lattices Day 2

(open-ended) What do you like to see in a basis?

What makes a basis easy to work with?

Exp 7 (Day 1)

$\{u, v\}$, $\{p, q\}$ bases for same lattice.

e.g. $\{p, q\} = \{\pm u, \pm v\}$.

$$\left.\begin{aligned} p &= au + bv \\ q &= cu + dv \end{aligned}\right\} \quad \begin{pmatrix} p_1 & q_1 \\ p_2 & q_2 \end{pmatrix} = \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

"p and q are in the lattice gen by u, v.

$$\left.\begin{aligned} u &= ep + fq \\ v &= gp + hq \end{aligned}\right\} \quad \boxed{\begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} = \begin{pmatrix} p_1 & q_1 \\ p_2 & q_2 \end{pmatrix}\begin{pmatrix} e & g \\ f & h \end{pmatrix}}$$

$$\Longrightarrow \cancel{\begin{pmatrix} p_1 & q_1 \\ p_2 & q_2 \end{pmatrix}} = \cancel{\begin{pmatrix} p_1 & q_1 \\ p_2 & q_2 \end{pmatrix}}\begin{pmatrix} e & g \\ f & h \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \underset{p,q \to u,v}{\begin{pmatrix} e & g \\ f & h \end{pmatrix}}\underset{u,v \to p,q}{\begin{pmatrix} a & c \\ b & d \end{pmatrix}}$$

← all entries are integers!

Take determinant: (multiplicative)

$$1 = (eh - gf)(ad - bc)$$

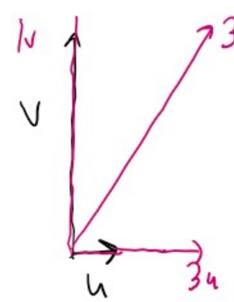
Changing a lattice basis:

In $\{u, v\}$ is basis

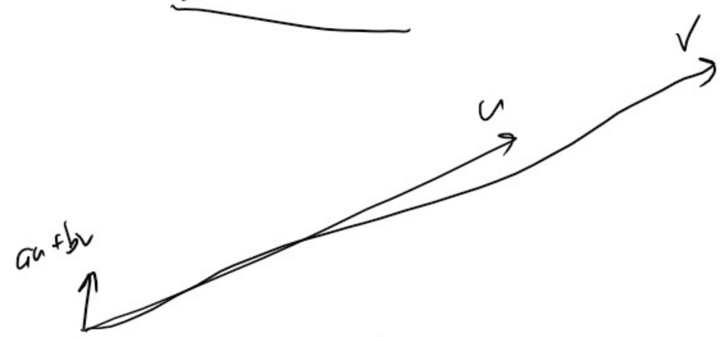
Changing a [illegible]

If $\{u, v\}$ is a basis,
<u>and</u> a, b, c, d are integers w/ $|ad - bc| = 1$,
Then $\{au + bv, cu + dv\}$ is also a basis of same lattice.

Nice bases	Bad bases



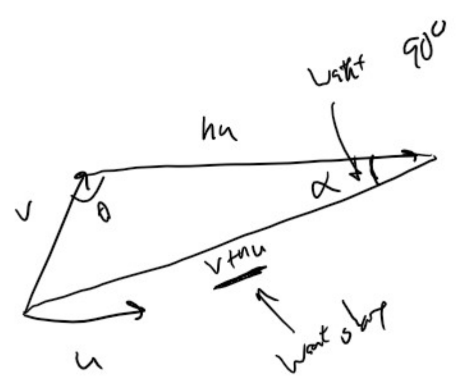
$$\|au + bv\|^2 = a^2\|u\|^2 + b^2\|v\|^2$$



"Surprise" short vectors

starting here...
how do we get as close as possible to here?

Exp 2 Law of Sines



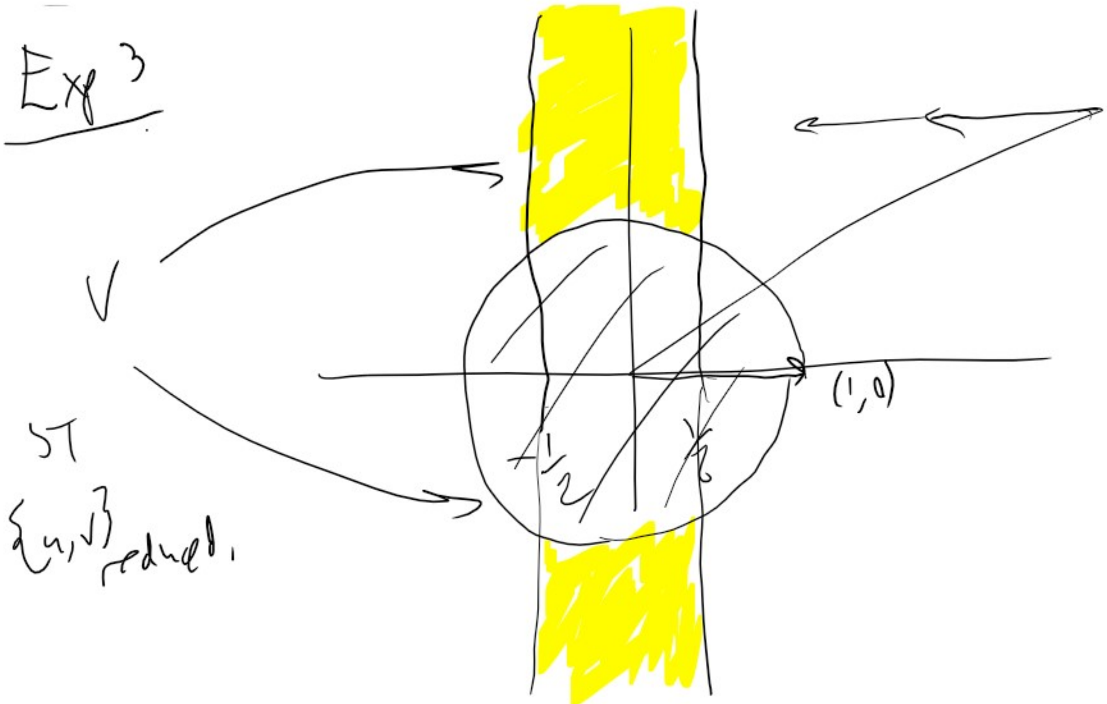
$$\frac{\|v + nu\|}{\sin\theta} = \frac{\|v\|}{\sin\alpha}$$

$$\Rightarrow \|v + nu\| \sin\alpha = \text{constant}$$

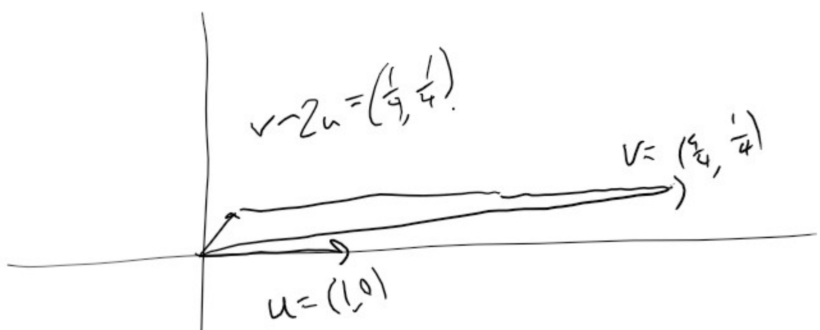
$\downarrow \quad \uparrow$

Exp 3

Exp 3



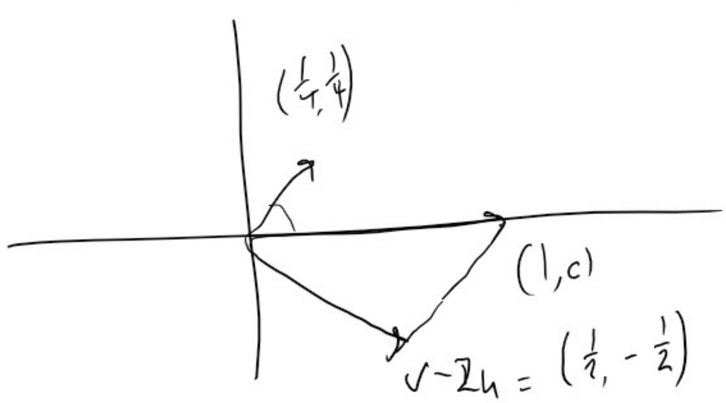
Exp 5

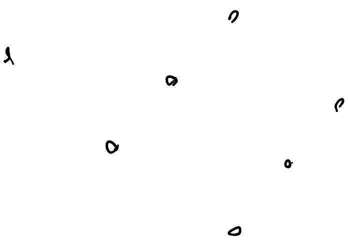


Swap and repeat.

Set $u = \left(\frac{1}{4}, \frac{1}{4}\right)$

$v = (1, 0)$





$v - 2u = \left(\frac{1}{2}, -\frac{1}{2}\right)$

replace v w/ $v-2u$.

$\left.\begin{array}{l}\underline{\text{Exp } 6}\\ \underline{\text{Exp } 7}\\ \underline{\text{Exp } 8}\end{array}\right\}$ recommend