Midterm 2 Problem 1

Jacobi Symbol

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

$\gcd(a, n) = 1$

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{a_1} \cdots \left(\frac{a}{p_r}\right)^{a_r}$$

Legendre Symbol

$\left(\frac{a}{p}\right) = 1 \iff x^2 \equiv a \pmod{p}$ has a solution

Jacobi Symbol

$x^2 \equiv a \pmod{n}$ has a solution

$\implies \left(\frac{a}{n}\right) = 1$

$\not\Longleftarrow$ not true

Revisit Fermat's 2 square thm

Thm: $p \equiv 1 \pmod 4 \iff p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$

pf: Alternate proof using binary quadratic forms.

Let p be a prime, $p \equiv 1 \pmod 4$.

$\exists\, r, u$ s.t $pu + r^2 = -1$

Consider $Q(x,y) = px^2 + 2rxy - uy^2$

$\Delta = 4r^2 + 4pu = 4(-1) = -4$

$Q(1,0) = P$

So, Q is positive definite.

What are all positive definite quadratic forms (up to equivalence) such that $\Delta = -4$?

Minimum value $u \le \sqrt{4/3} \le 1$

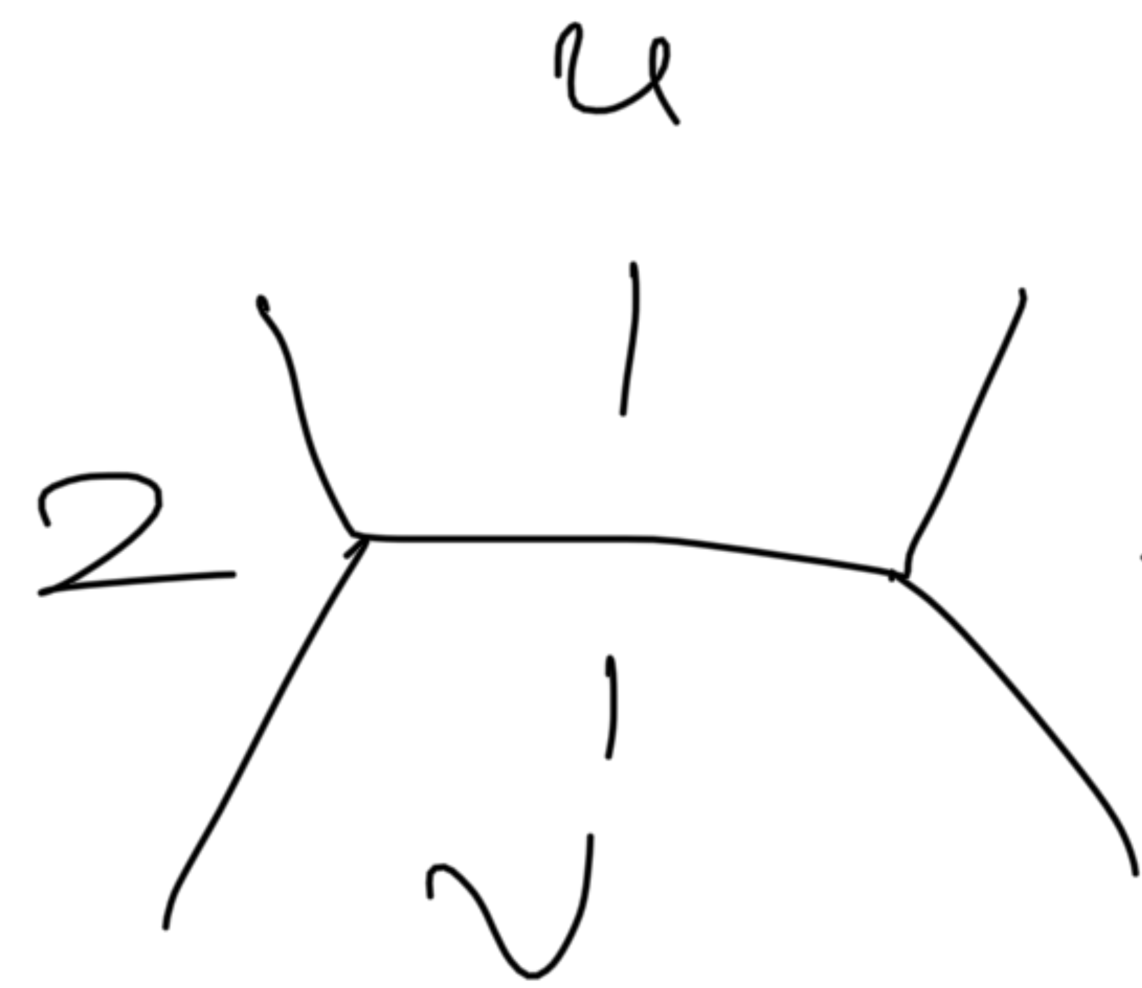
So, $u = 1$,

$0 \le h \le u$

$\Delta = -4 \Rightarrow h$ even, $h = 0$

$$h^2 - 4uv = -4$$

$$uv = 1 \Rightarrow v = 1$$



double well

$u+v-h$

$$\boxed{x^2+y^2}$$

So, Q is equivalent to x^2+y^2.

Q represents P

So, $\boxed{x^2+y^2 \text{ represents } P.}$

Thm: If $p \equiv 1 \pmod 3$, then

$x^2 + xy + y^2 = p$ has a solution.

Pf: $$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$$

$$= \left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)(-1)^{\left(\frac{3-1}{2}\right)\left(\frac{p-1}{2}\right)}$$

$$= \left(\frac{-1}{p}\right)\left(\frac{-1}{p}\right)\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = 1$$

$\exists\ r, u$ s.t. $\quad -3 \equiv r^2 \pmod p$

$$-3 = r^2 + pu$$

$$Q(x,y) = px^2 + 2rxy - uy^2$$

$$\Delta(Q) = 4r^2 + 4pu$$
$$= 4(r^2 + pu) = -12$$
(positive def)

$x^2 + xy + y^2$ has $\Delta = -3$

Need to find another quadratic form.

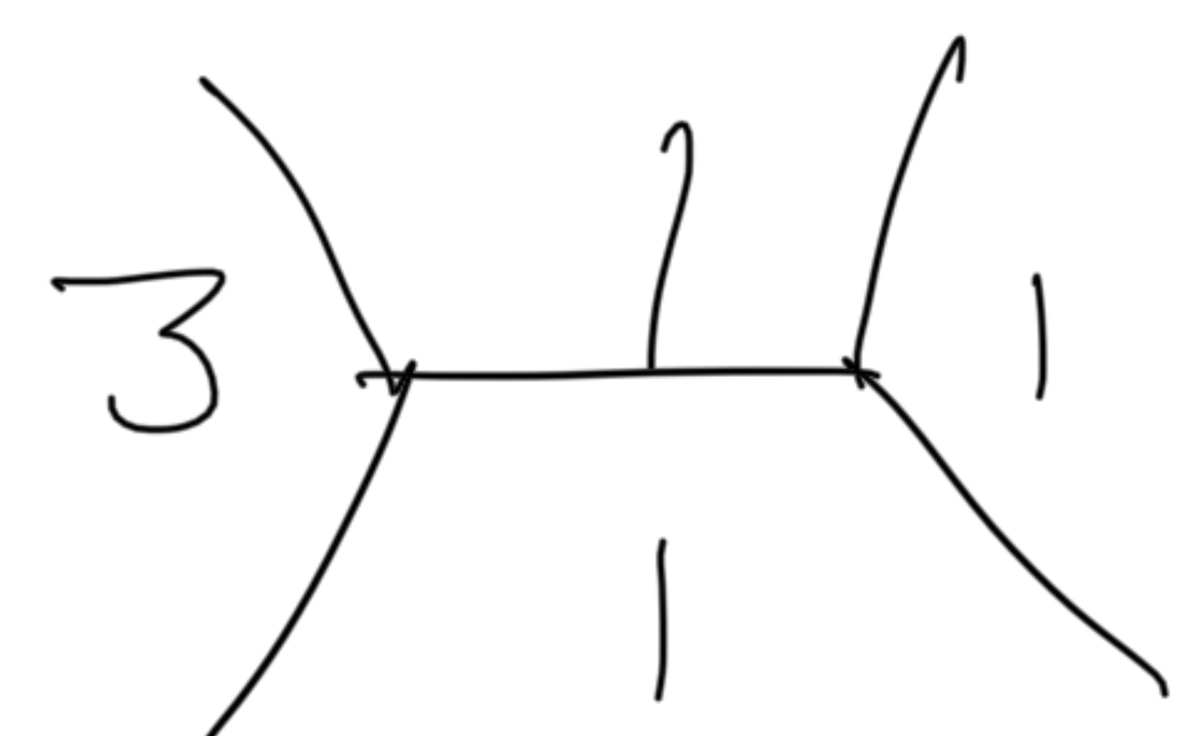
$$-3 = r^2 + pu$$

$$Q(x,y) = px^2 + rxy - (u/4)y^2$$

$$\Delta(q) = r^2 + 4(p)\left(u^2/4\right)$$
$$= r^2 + pu^2 = -3$$

$$u \leq \sqrt{\frac{|\Delta|}{3}} = \sqrt{1} = 1$$

$u=1$ $\quad h=1$ $\quad v=1$



$\sim x^2 + xy + y^2$

Practice Problems

1. Show that every positive definite binary quadratic form of $\Delta = -12$ is equivalent to

$$x^2 + 3y^2 \quad \text{or to} \quad 2x^2 + 2xy + 2y^2$$

Soln: We start with classifying wells

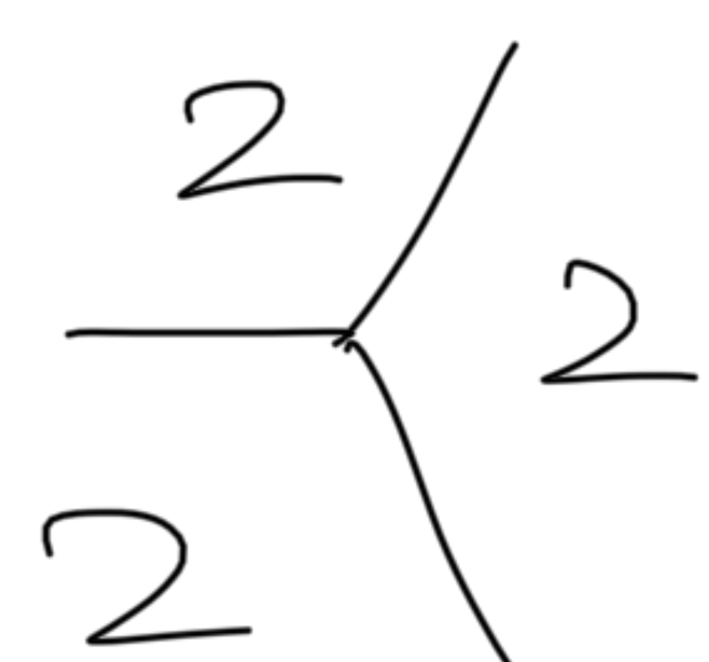
1) $0 < u \leq \sqrt{\frac{|\Delta|}{3}} = \sqrt{\frac{12}{3}} = 2$

2) $0 \leq h \leq u$

3) $\Delta = h^2 - 4uv$

u	h	v
1	0	3
2	0	3/2 ← not an integer
2	2	2

x^2+3y^2



$2x^2+2xy+2y^2$

2. $Q_1(x,y) = 41x^2 + 70xy + 30y^2$

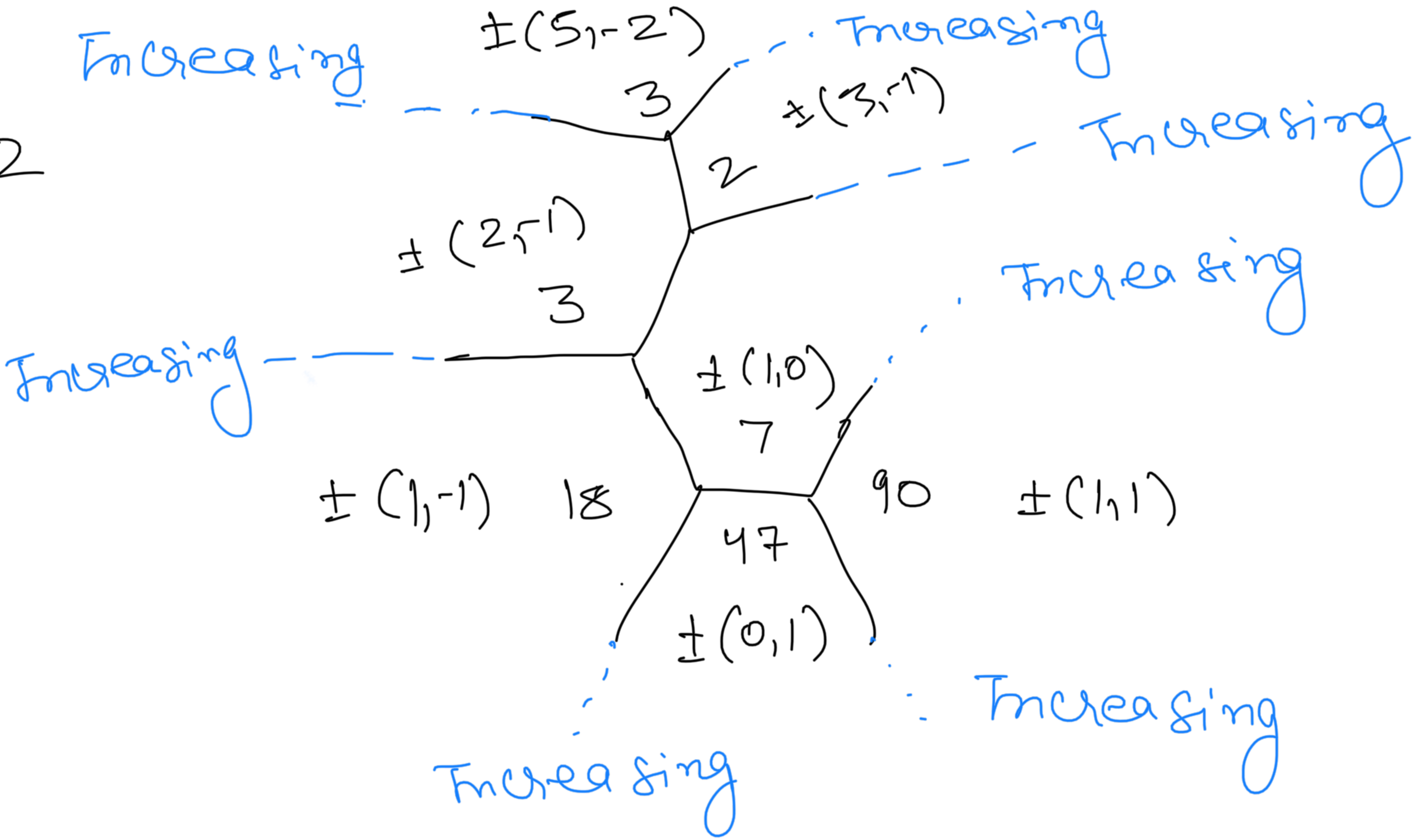
$Q_2(x,y) = 7x^2 + 36xy + 47y^2$

$Q_3(x,y) = 23x^2 + 76xy + 63y^2$

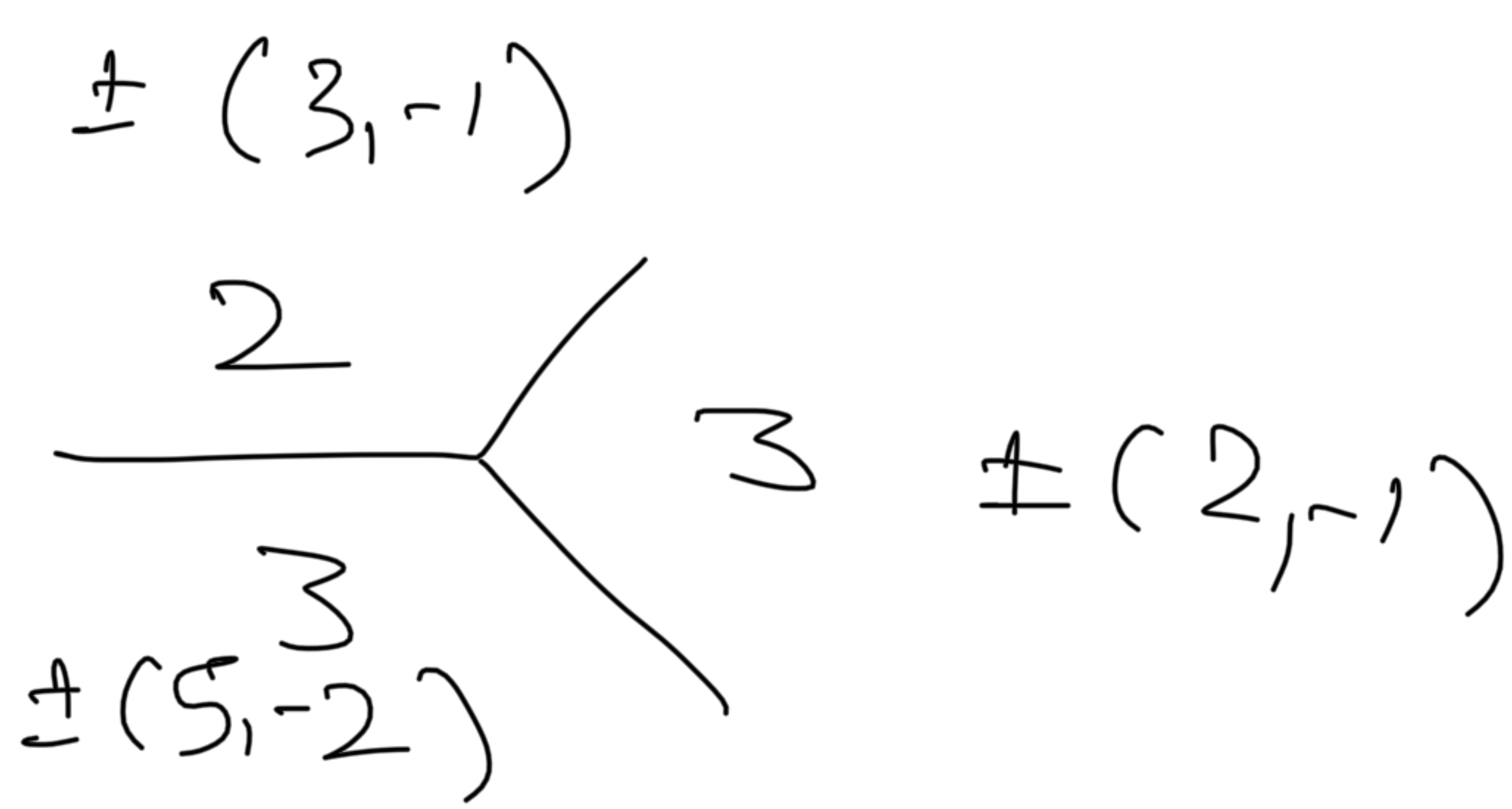
All of them have same discriminant -20. Which of them are properly equivalent?

Let us start by finding wells in their range topographs

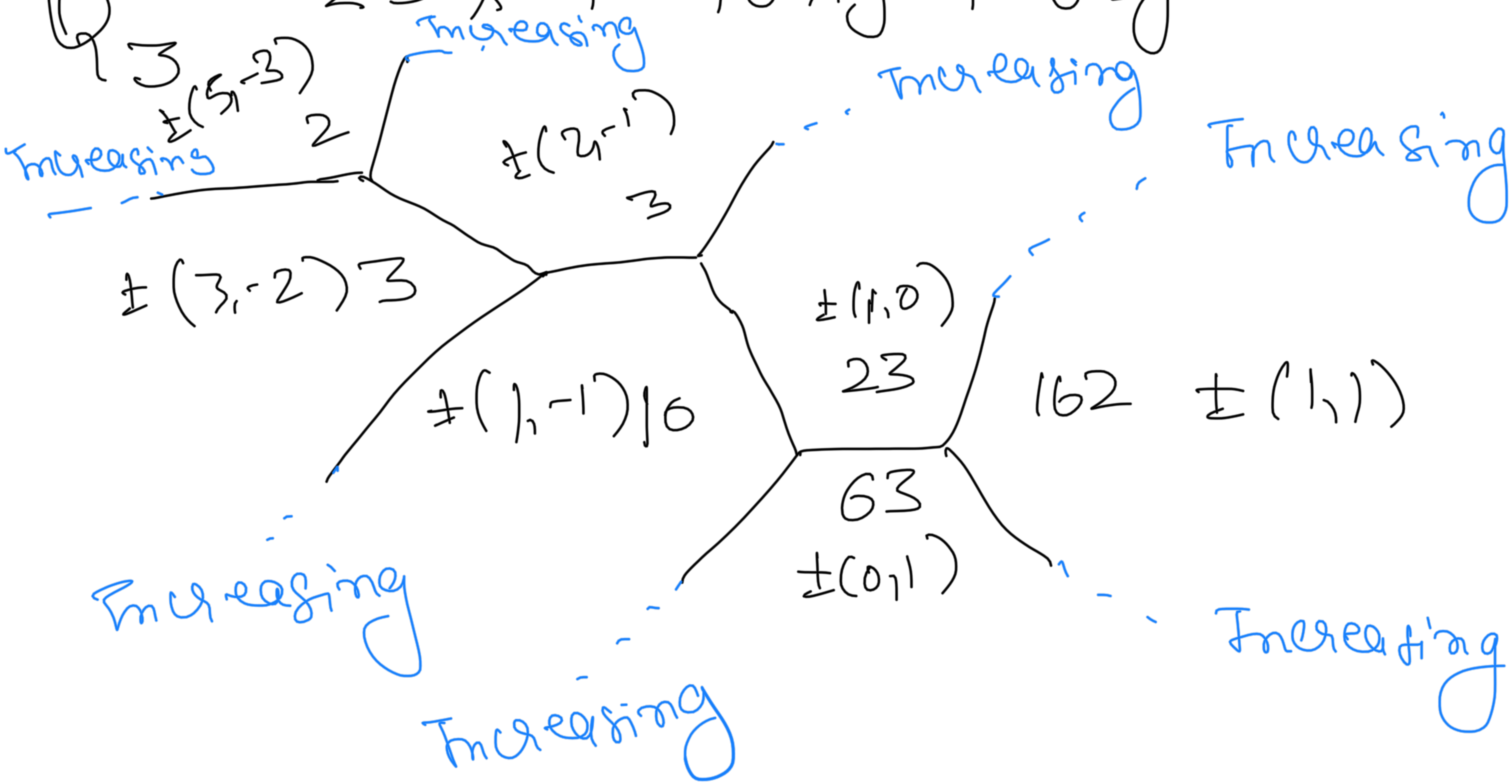
Q22


±(5,-2)
3
Increasing
Increasing
±(3,-1)
2
Increasing
±(2,-1)
3
Increasing
Increasing
±(1,0)
7
±(1,-1)
18
90
±(1,1)
47
±(0,1)
Increasing
Increasing

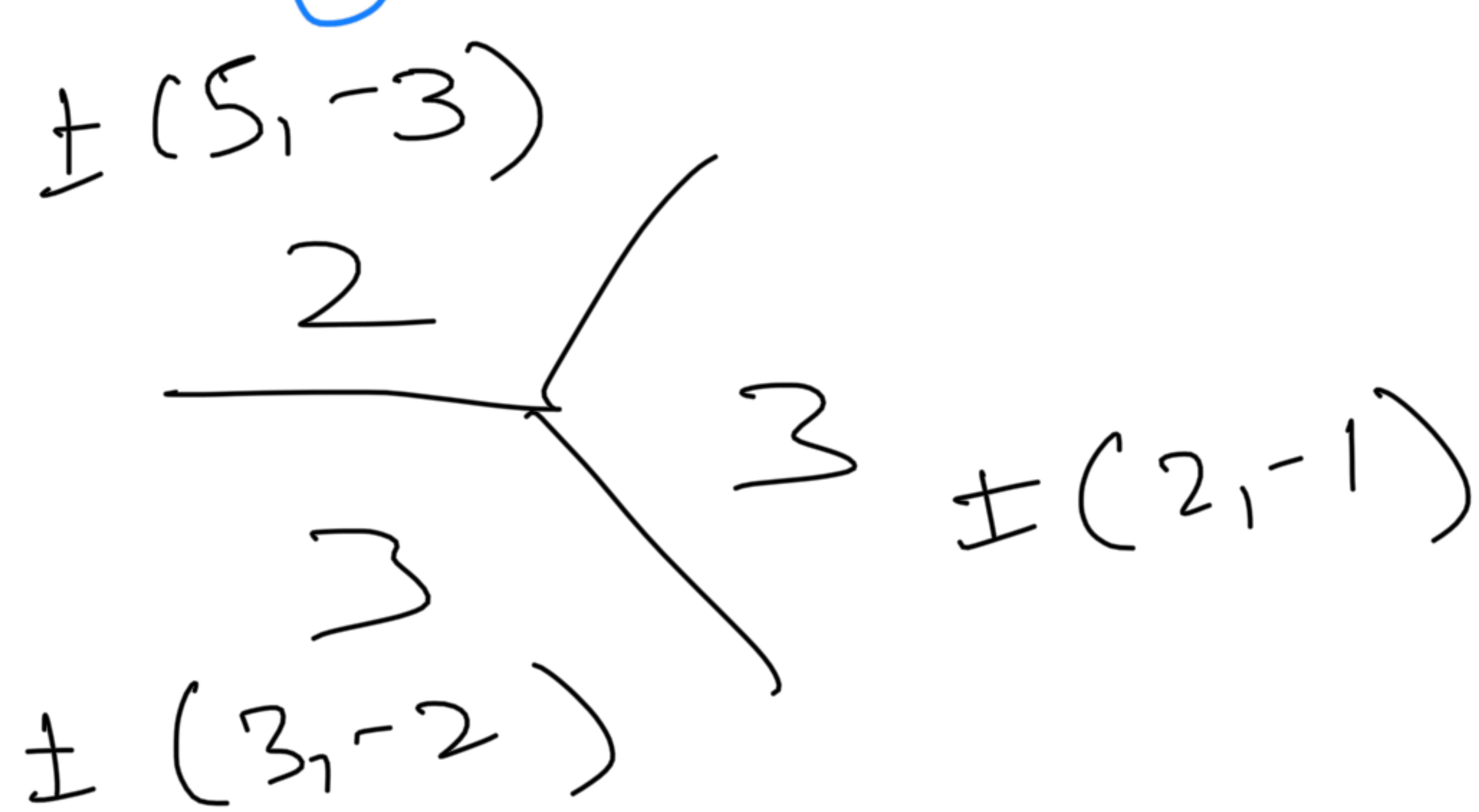
Well


±(3,-1)
2
3
±(2,-1)
3
±(5,-2)

Q 3 $\quad 23x^2 + 76xy + 63y^2$



Well

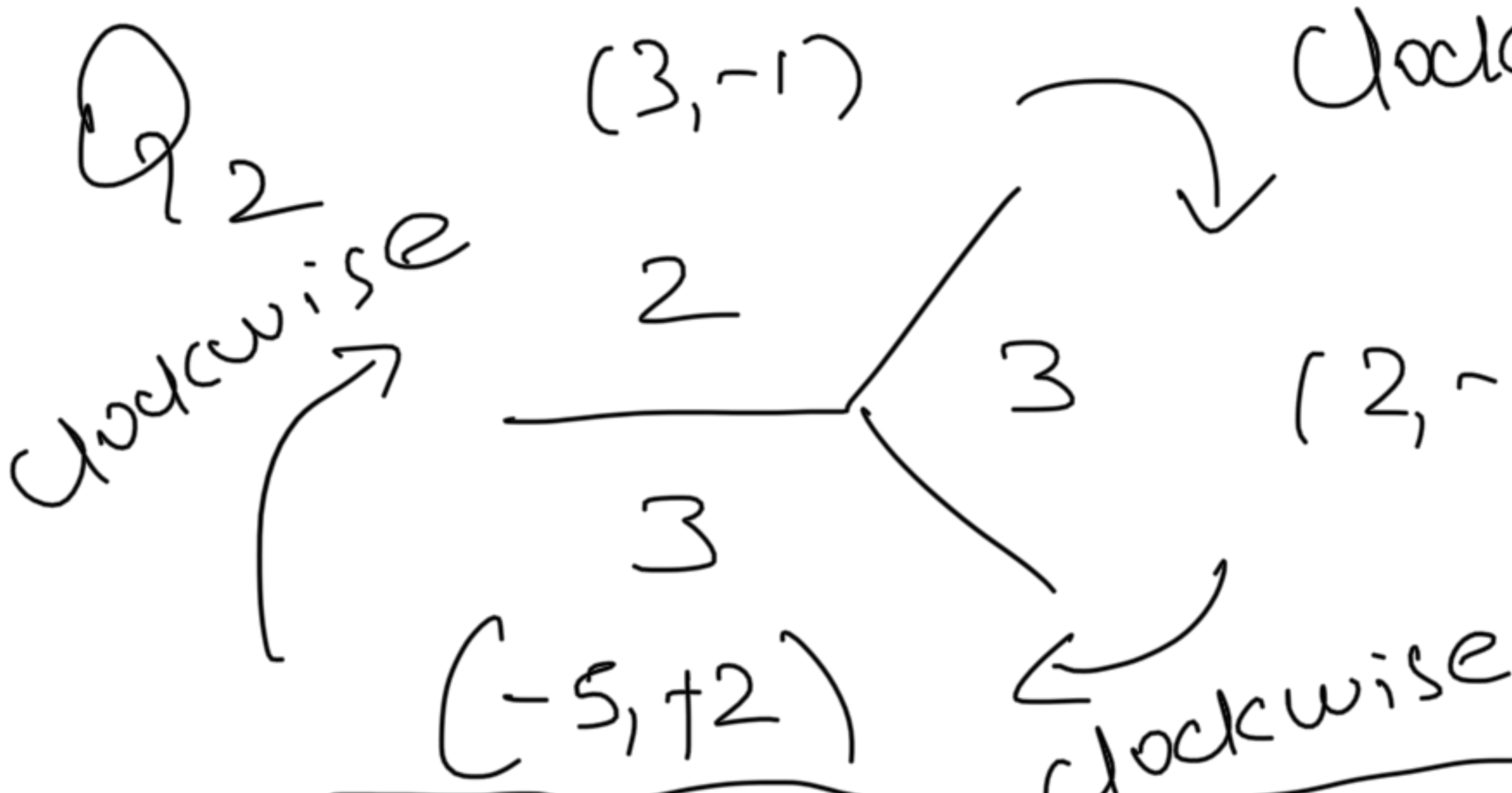


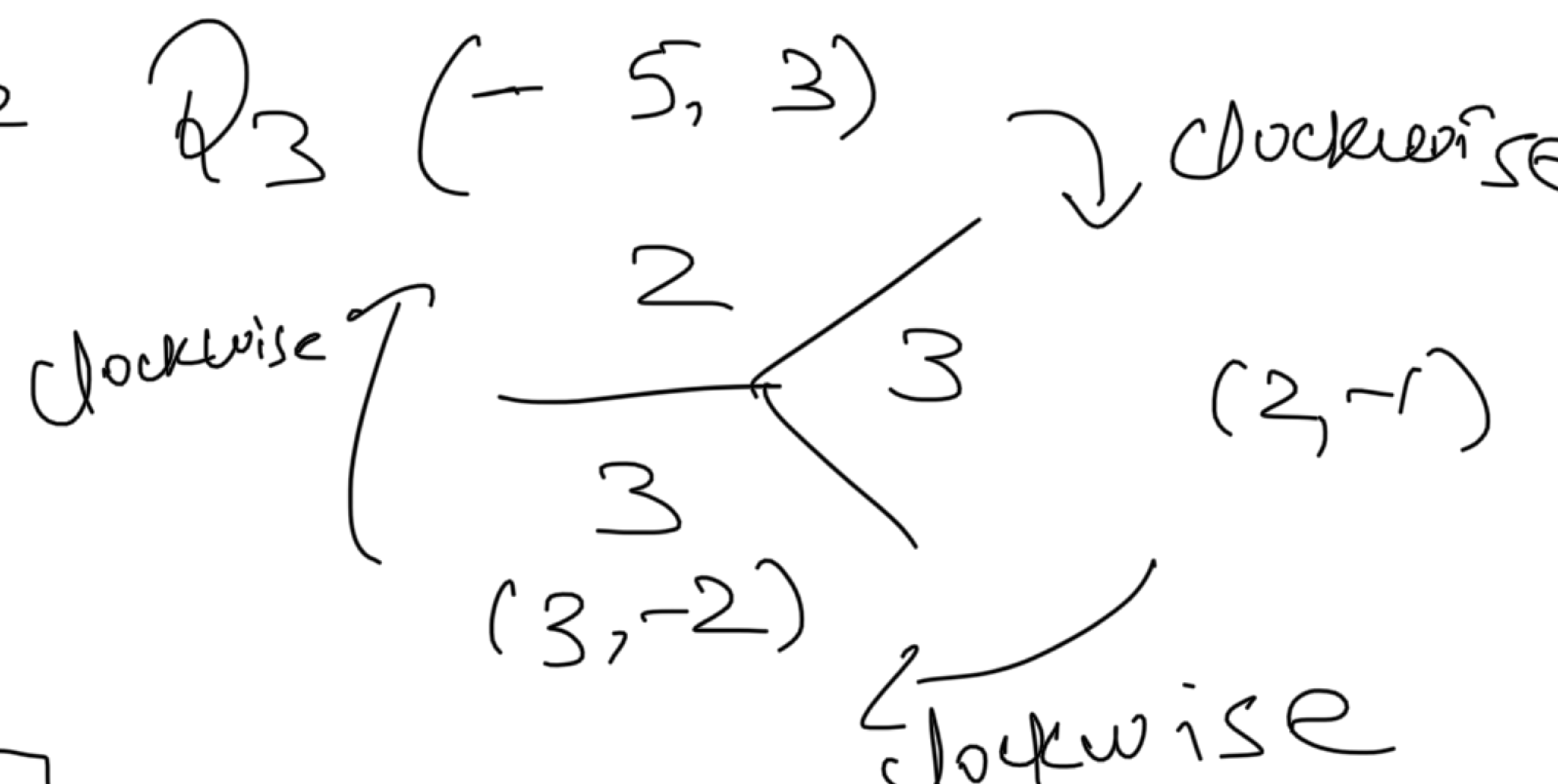
So, Q_2 & Q_3 are equivalent.

By observation $Q_1(1,-1) = 41(1)^2 + 70(-1) + 30(-1)^2$
$= 41 - 70 + 30 = 1$

So, Q_1 is not equivalent to Q_2 or Q_3.

Let's look at orientation of Q_2 & Q_3's wells.





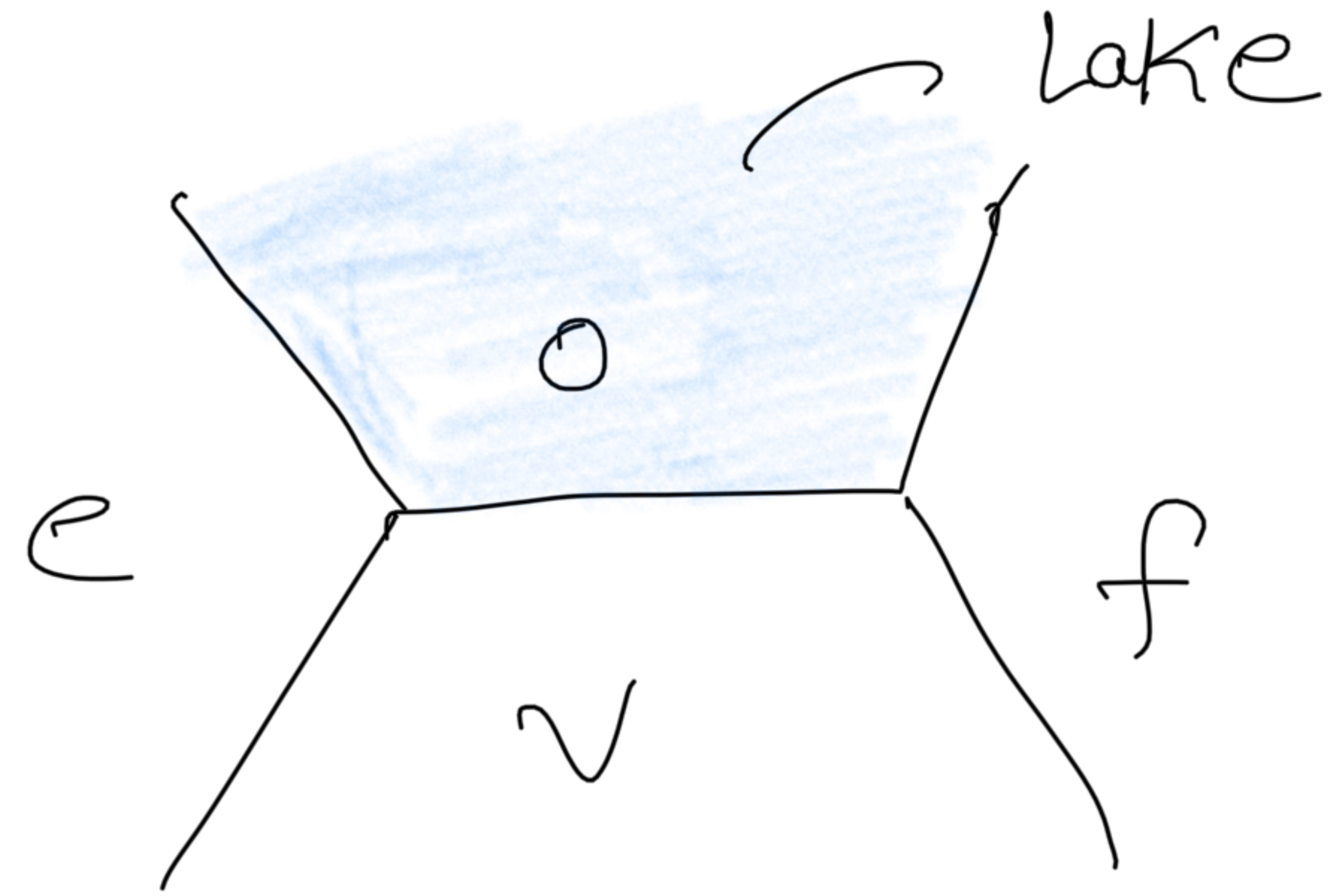
$\boxed{\text{Properly equivalent}}$

We saw that if $Q(x,y)$ is positive definite then its range topograph contains exactly one well.

What happens if $Q(x,y)$ is positive semi-definite

$$Q(x,y) \geq 0$$

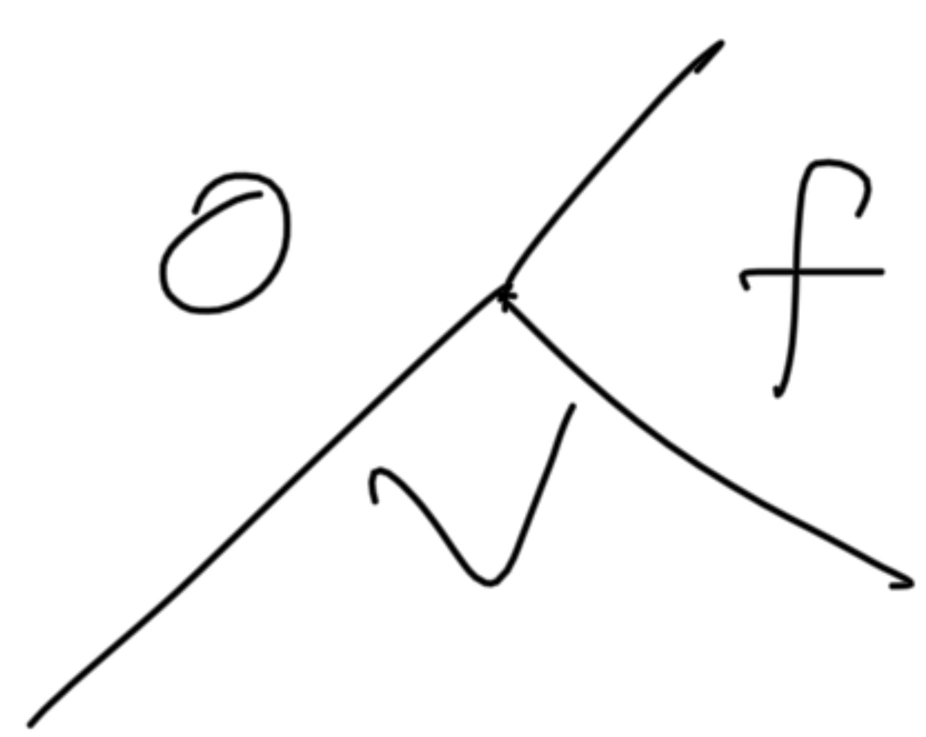
Suppose Q is positive semi definite.



$e \quad v \quad f$ are in arithmetic progression

$f = v + h$

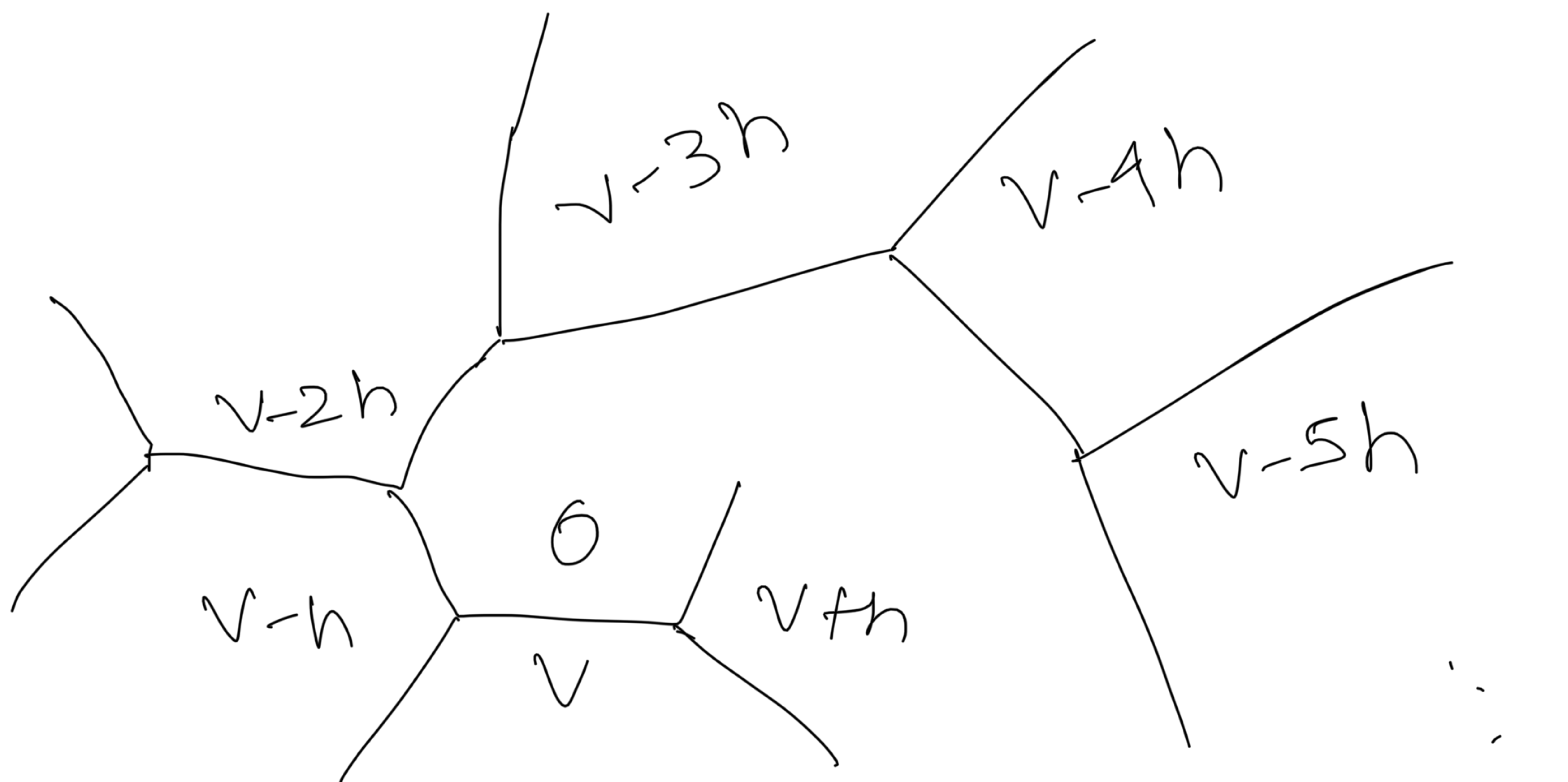
$\Delta(Q)$



$$= f^2 + v^2 - 2vf$$

$$\Delta(Q) = (f-v)^2 = h^2$$

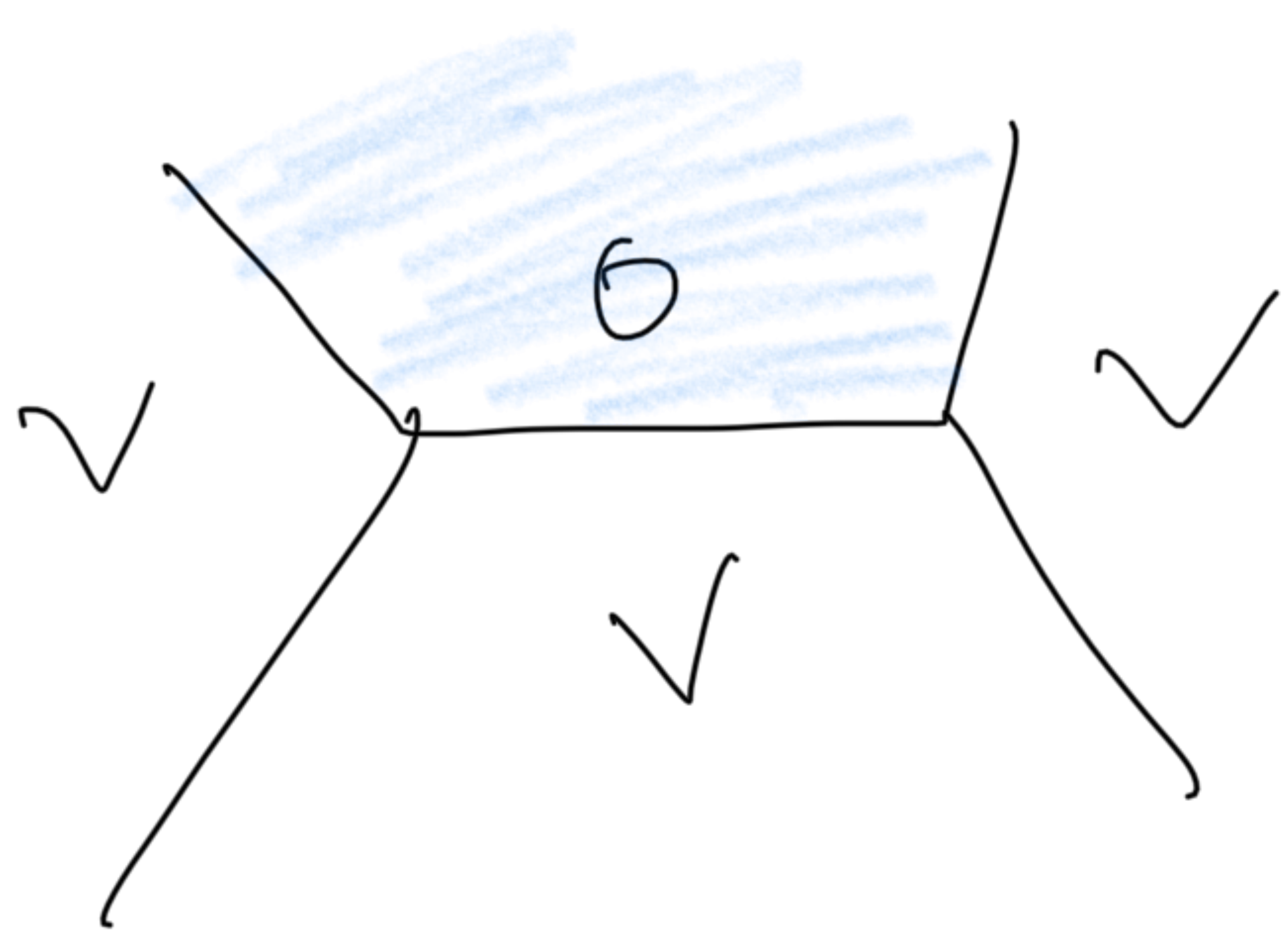
Let's explore this h.



$\Rightarrow \quad h = 0$

So, if Q is positive semidefinite

$$\Delta(Q) = 0.$$

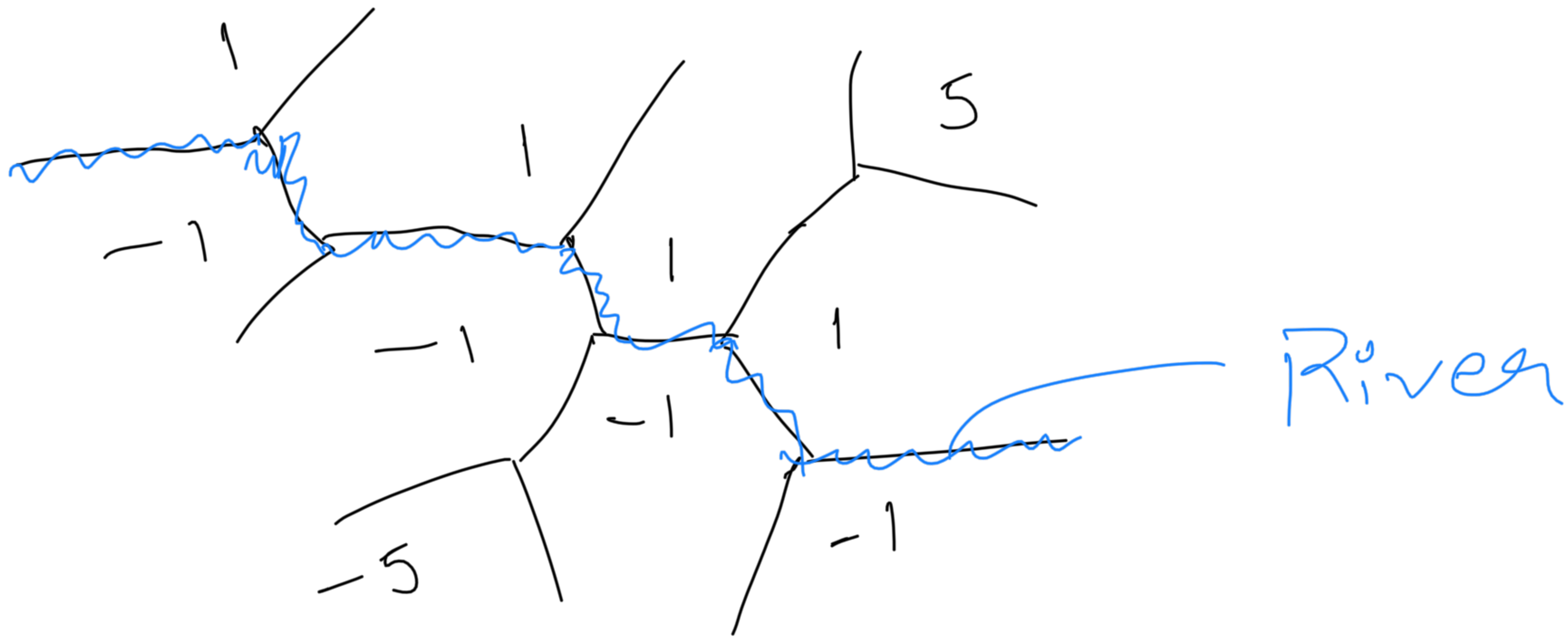


$$Q(x,y) = vx^2$$

Q positive semidefinite $\Rightarrow$ Q is equivalent to vx^2, $v \in \mathbb{Z}$.

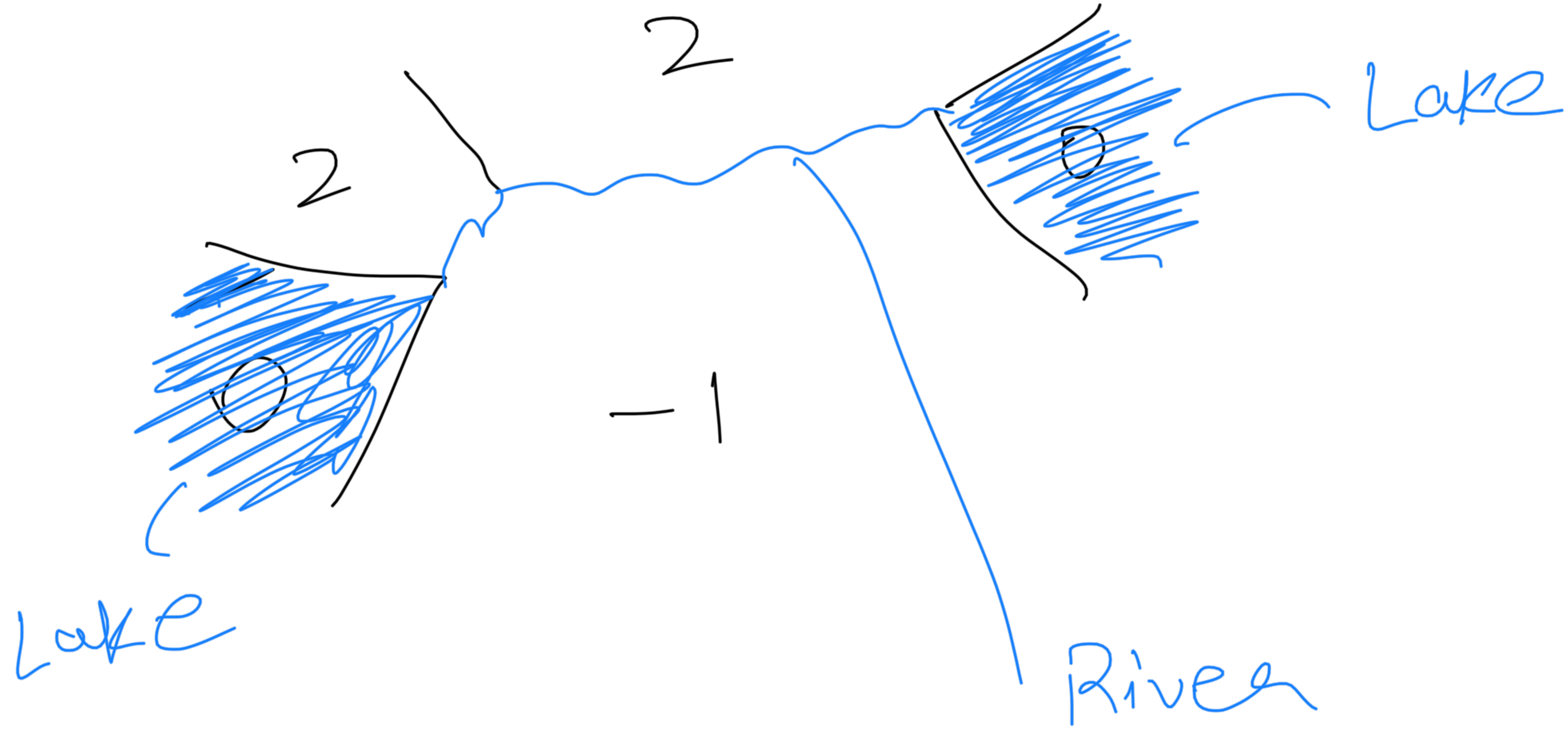
Indefinite forms

$x^2 + xy - y^2$



Another example

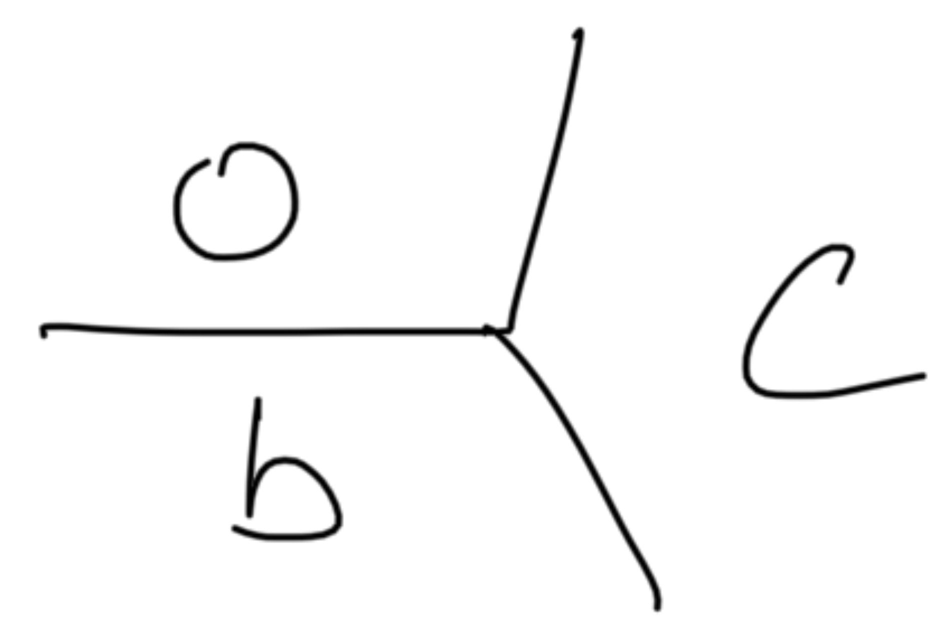
$\Delta = 1 - 4(1)(-1)$
$= 5$



$$\Delta = 4 + 1 - 2(2)(-1)$$
$$= 5 + 4 = 9 = 3^2$$

Thm: There is atleast one lake in range topograph of Q $\iff$ $\Delta(Q)$ is a square.

Pf: $\Rightarrow$



$$\Delta = b^2 + c^2 - 2bc = (b-c)^2$$

$\Leftarrow$ Suppose $\Delta(Q)$ is a square

$$Q(x,y) = ax^2 + bxy + cy^2$$

We want to show that 0 is in range of Q.

$a=0$, then $Q(1,0)=0$

$a\neq 0$, then $x=\sqrt{\Delta}-b$

$y=2a$

$$Q(x,y)=a(\sqrt{\Delta}-b)^2+2ba(\sqrt{\Delta}-b)+c(4a^2)$$

$$=a\Delta+ab^2-\cancel{2ab\sqrt{\Delta}}+\cancel{2ab\sqrt{\Delta}}$$

$$-2b^2a+4ca^2$$

$$=a\Delta-ab^2+4ca^2$$

$$=a(\Delta-b^2+4ca)=a(0)=0$$

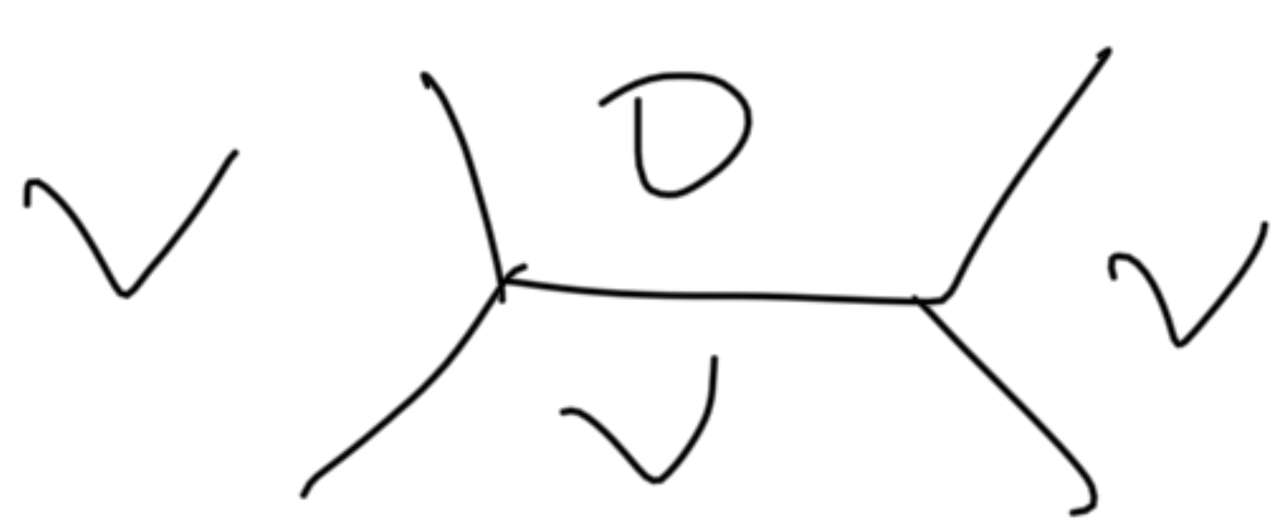
If (x,y) are coprime, then great

O.w replace (x,y) with $(x/d, y/d)$

$d = \gcd(x,y)$

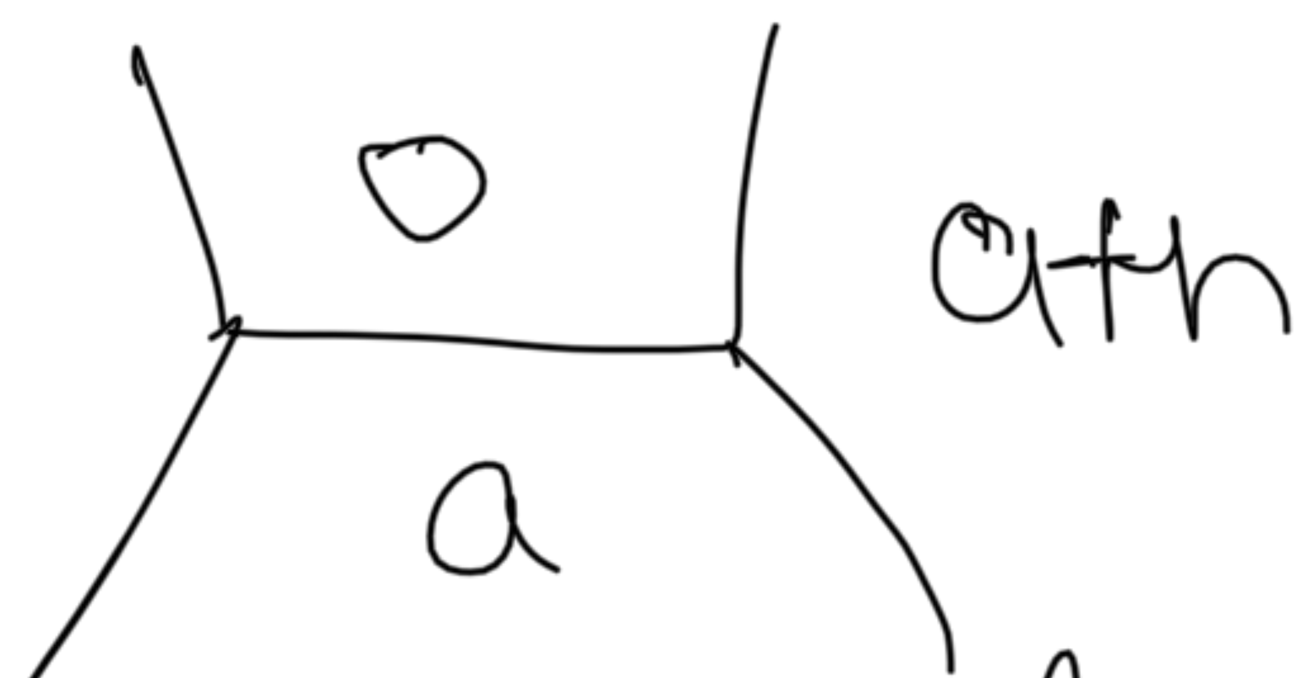
$$Q\left(x/d, y/d\right) = \frac{1}{d^2} Q(x,y) = 0$$

In the case of semidefinite forms we saw that Q is equivalent to vx^2



In general if there is a lake in range topograph of Q assume $\sqrt{\Delta} \neq 0$, then Q is equivalent to $ax^2 + \sqrt{\Delta}\, xy$ for some $0 \le a < \sqrt{\Delta}$.

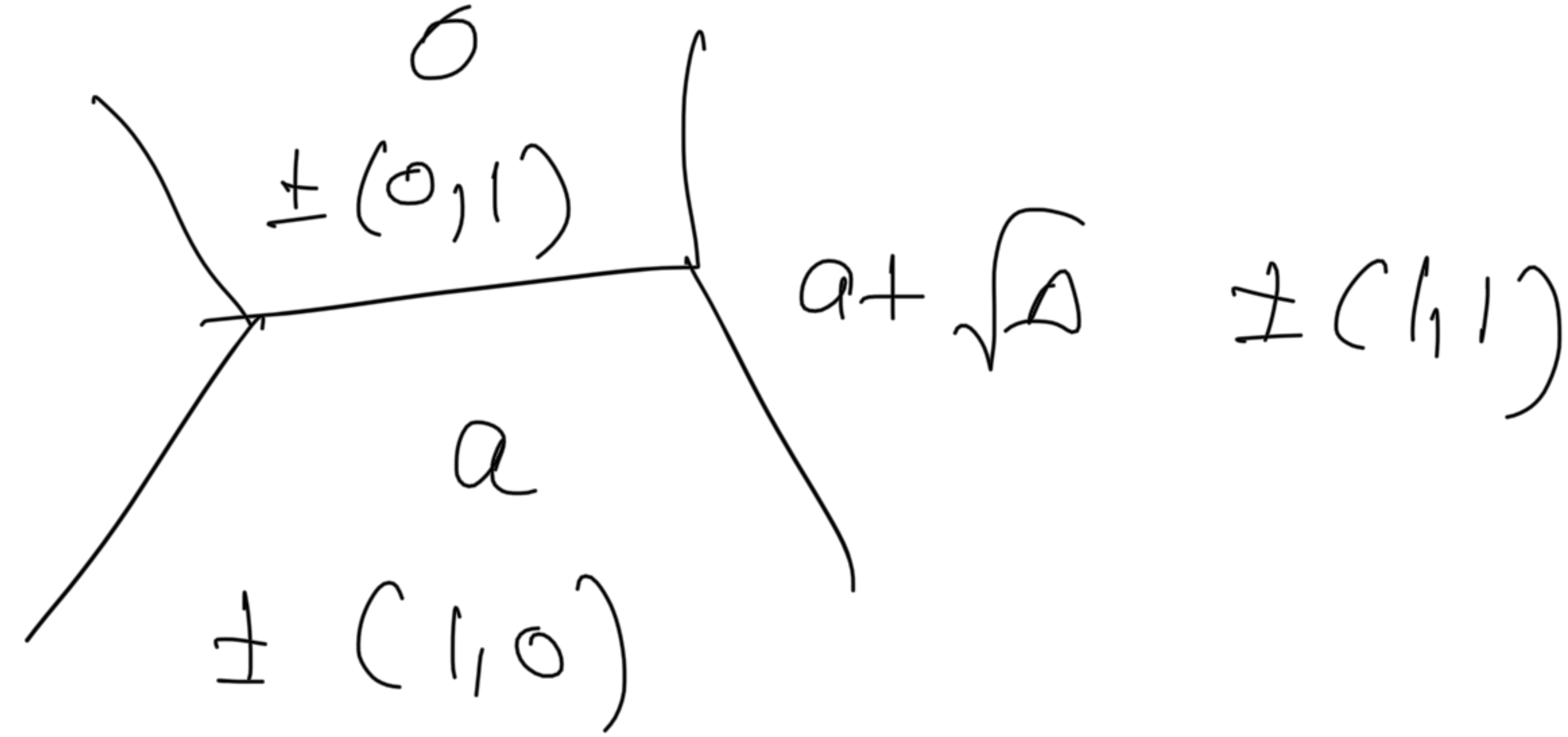
Proof:



a is chosen to be smallest among neighbours of 0.

This triad also appears in range topograph of $ax^2 + \sqrt{\Delta}\, xy$

$ax^2 + \sqrt{\Delta}xy$



Q is positive definite $\rightarrow$ no lakes

Q is indefinite or semidefinite (+ or −) $\longrightarrow$ there are lakes

How many?

Depends on the discriminant

if Q is positive semidefinite
then Q is equivalent to ax^2.

$$ax^2 = 0 \iff x = 0$$

So, there is only one lake.

Q is indefinite $ax^2 + \sqrt{\Delta}\,xy$, $\sqrt{\Delta} \neq 0$

$$ax^2 + \sqrt{\Delta}xy = 0$$

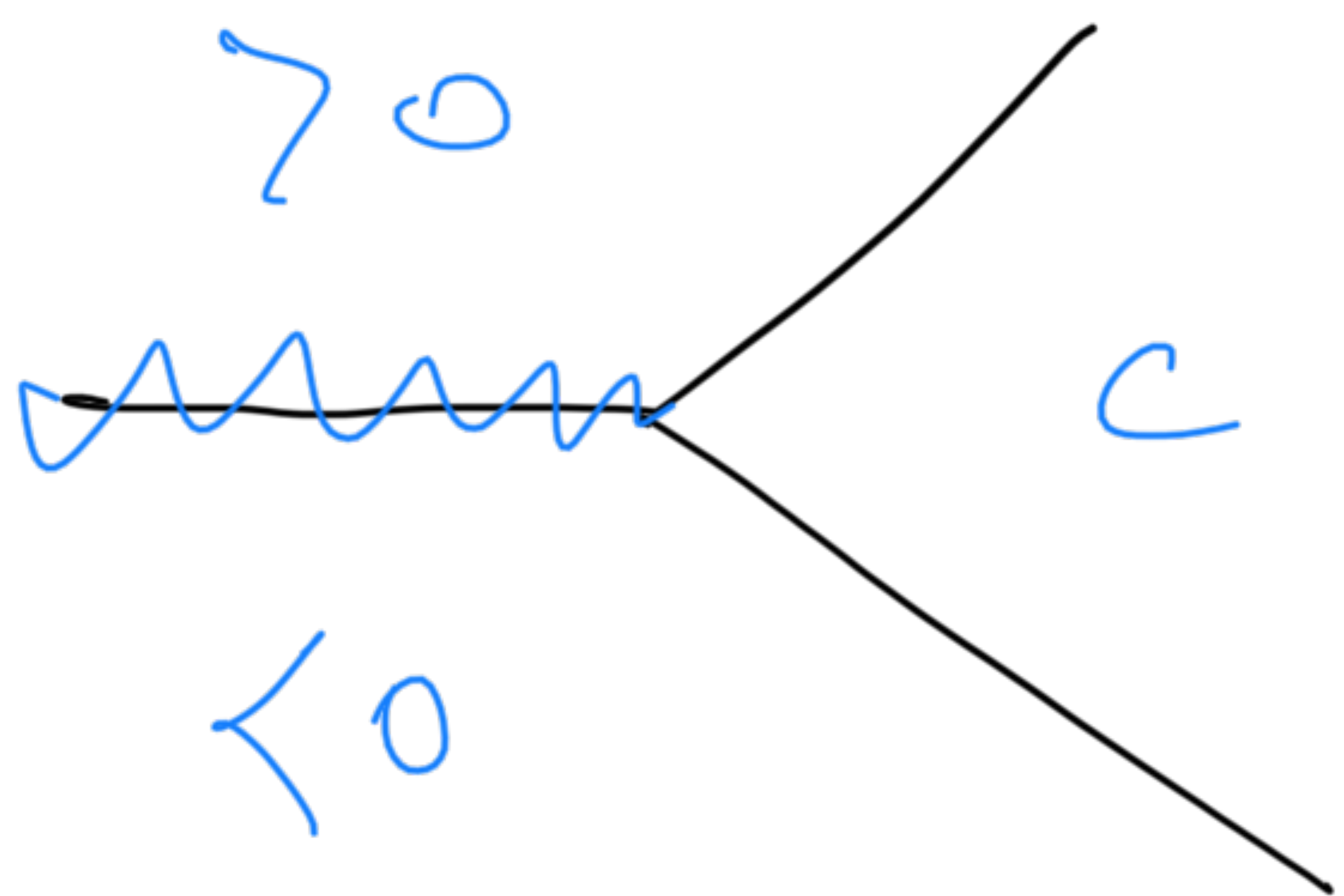
$$\Longleftrightarrow \quad ax^2 = -\sqrt{\Delta}xy$$

$x = 0$ or $ax = -\sqrt{\Delta}y$

$\pm(0,1)$ $\qquad$ $\pm(-\sqrt{\Delta}, a)$

Δ is not a square	no lakes
$\Delta = 0$	1 lake
Δ is square $\neq 0$	2 lakes

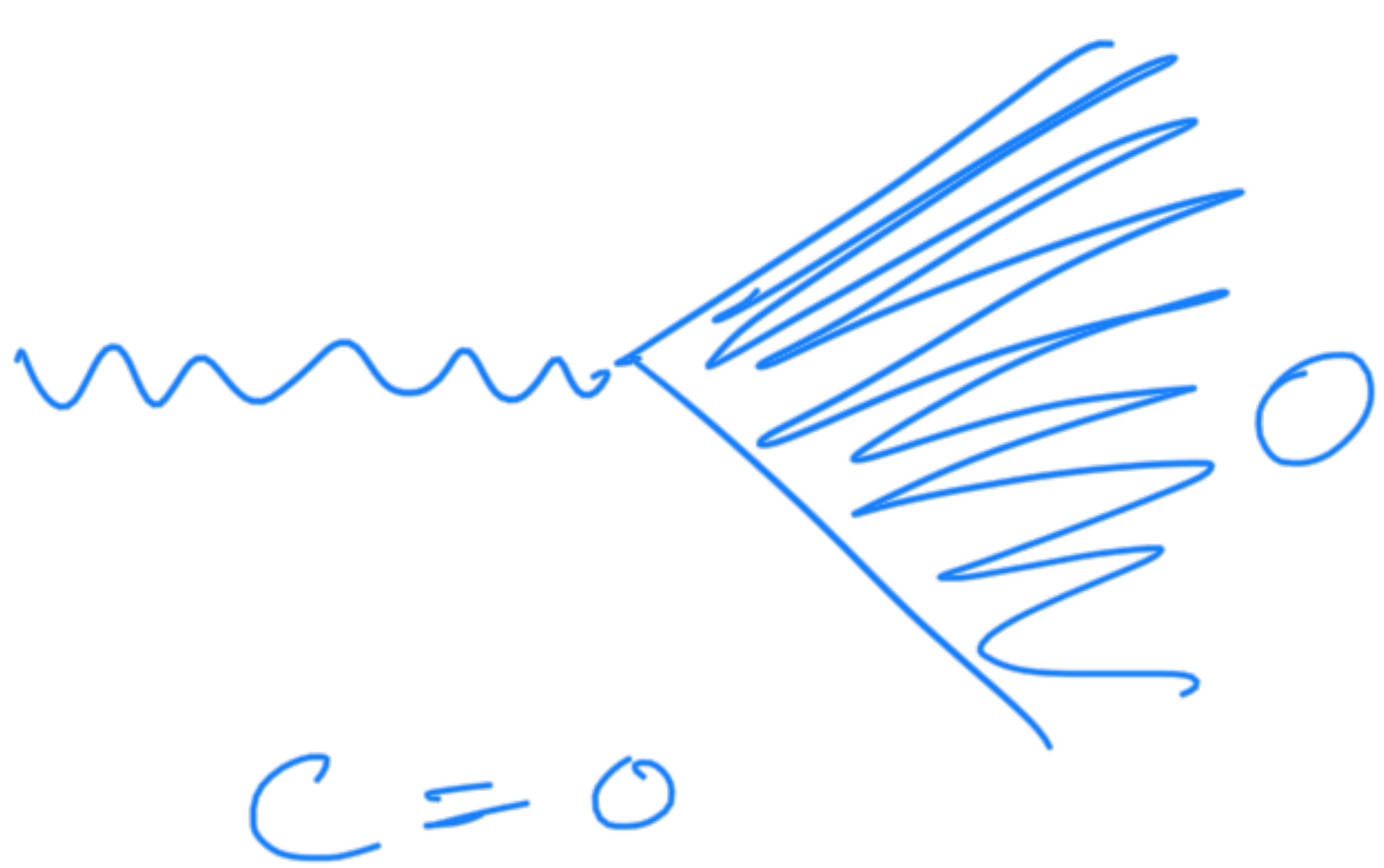
Observations: Suppose we have a triad containing a river

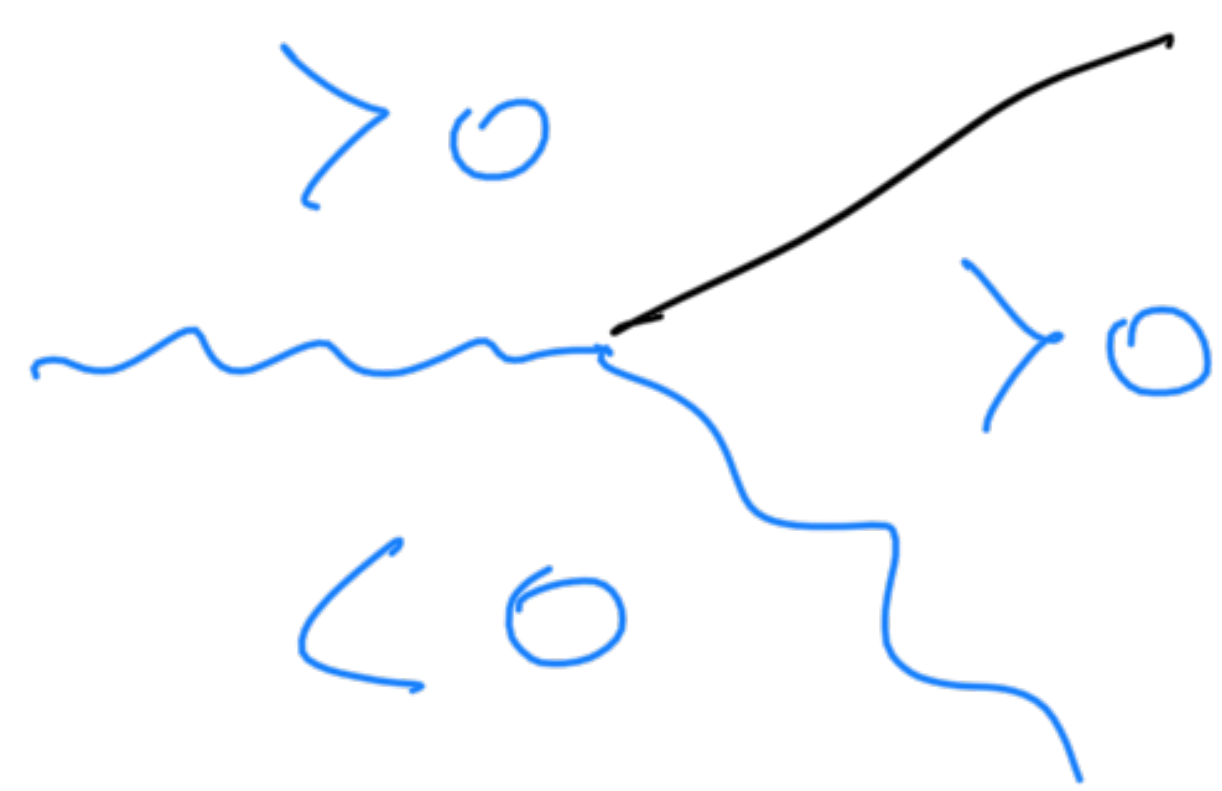


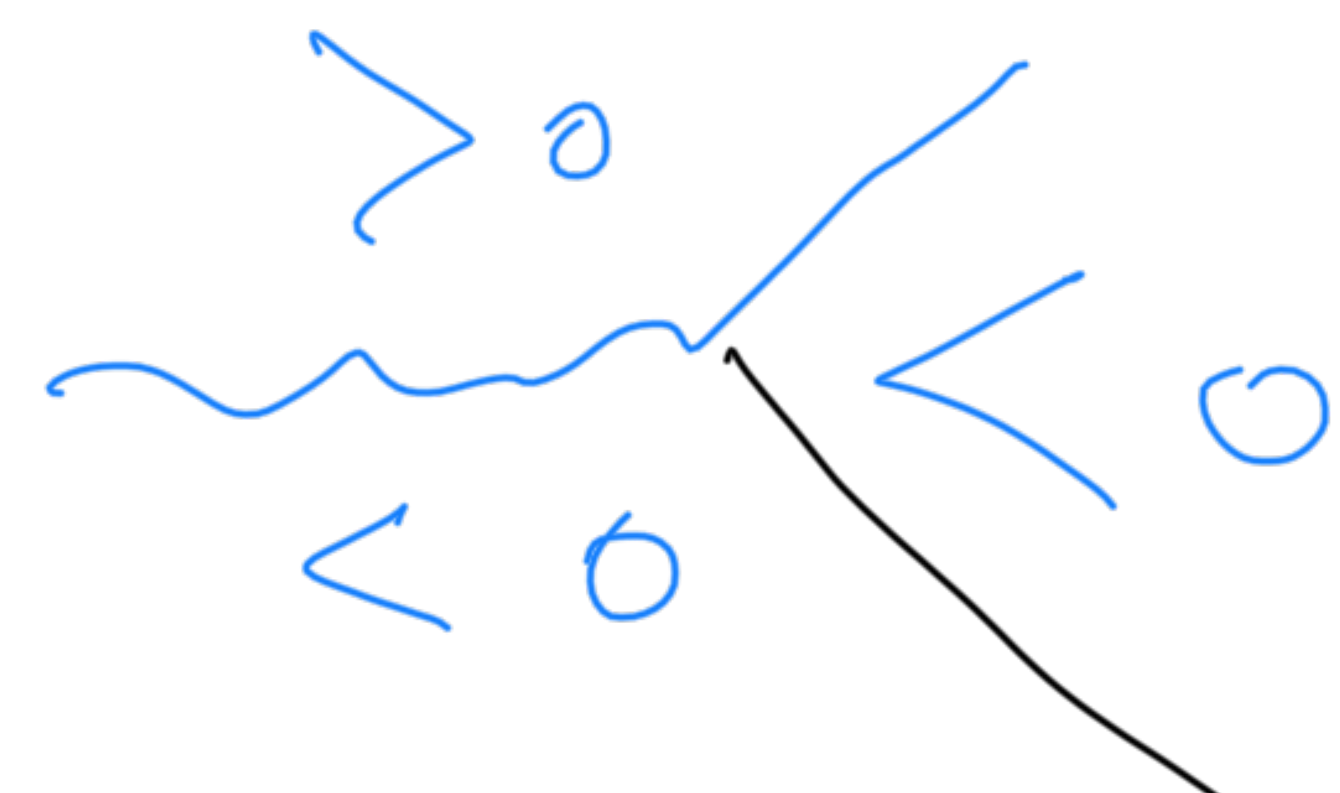
$c = 0$

$c > 0$

$c < 0$







Corollary 1) Rivers flow till they terminate in a lake.

2) If $\Delta(Q) > 0$ and Δ is not a square, then range topograph of Q contains an endless river.

Thm: A topograph contains at most one river.

pf: If $Q(x,y) \geq 0 \;\forall\, x,y$ then there is no river in range topograph of Q.

Suppose Q is indefinite. Suppose there are 2 rivers as shown

on next page.

either these values are positive

or negative

By climbing principle

will

along path values

keep on increasing.