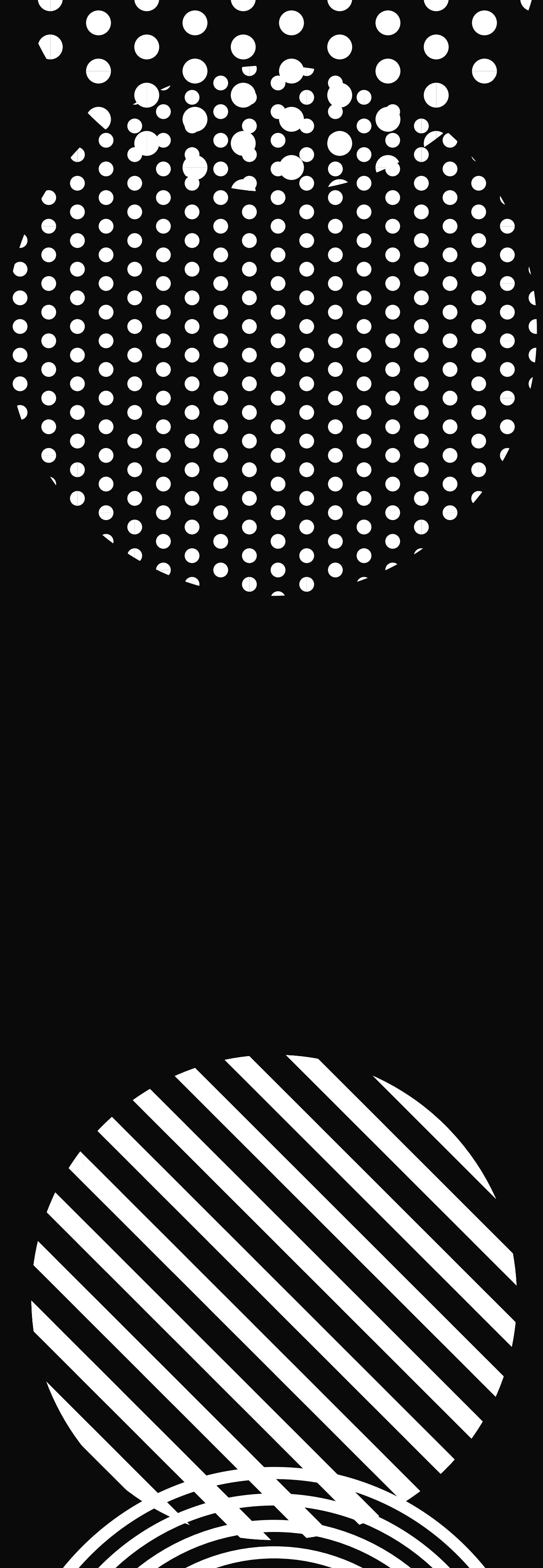


Q 1.1 Find a counterexample to "If $(X, \leq)$ where $\# X \leq 2^n$, then $(X, \leq)$ admits an order embedding into $(\mathcal{P}(\{1, \dots, n\}), \subseteq)$".

$\# \mathcal{P}(\{1, \dots, n\}) = 2^n$

Remark: In class we proved that always true that $(X, \leq)$ order embeds into $(\mathcal{P}(X), \subseteq)$ but $\# \mathcal{P}(X) = 2^{\# X} >$

2^n if $\#X = 2^n$.

<u>Solution:</u>

(<u>Idea:</u> Recall $(X, \leq)$ order embed into $(\mathcal{P}(\{1, \ldots, n\}), \subseteq)$ means that $(X, \leq) \simeq$ some subposet of $(\mathcal{P}(\{1, \ldots, n\}), \subseteq)$.

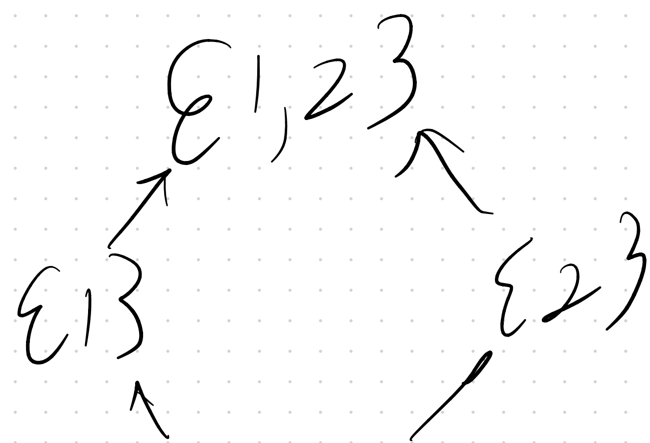
Want: find a property involving posets that $(X, \leq)$ but no subposet of $\left(\left(\mathcal{P}(\{1, \ldots, n\}), \subseteq\right)\right)$

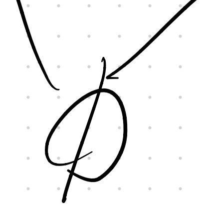
Take $X = \{a < b < c < d\}$

Observe that $\# X = 4 = 2^2$

but we claim that $(X, \leq)$ does not order embed into $(\mathcal{P}(\{1,2\}), \subseteq)$.

<u>Pf</u>:





Note that the poset $P(\{1,2\})$ has a maximal length chain of 3

$$\emptyset \subseteq \{1\} \subseteq \{1,2\}$$

$$\emptyset \subseteq \{2\} \subseteq \{1,2\}$$

Assume that $f: X \to P(\{1,2\})$ is an order embedding. Then since $a < b < c < d$ then

$$f(a) \subseteq f(b) \subseteq f(c) \subseteq f(d).$$

S

I If f was just monotone

$f(a) = f(b)$

But, since f is an order embedding we proved in class that f is injective.

So,

$$f(a) \subset f(b) \subset f(c) \subset f(d).$$

But, we saw that $P(\{1, 2\})$ does not have such a chain of length 4. Contradiction. $\boxtimes$

Remark: If $(X, \leq)$ poset $S \subseteq X$, then $(S, \leq)$ is a poset subposet. An order embedding $(X, \leq) \to (Y, \preceq) \Leftarrow$ an isom. $(X, \leq) \to (S, \preceq)$ w/ $S \subseteq \preceq$.

Alternative solution:

Take $X = \{a, b\}$ w/ Hasse diagram

We have $\# X = 2 = 2!$. But $(X, \leq)$ does not order ented into $P(\{1\})$,

$P(\{1\})$:

$$\begin{tikzcd} \{1\} \\ \emptyset \arrow[u] \end{tikzcd}$$

Suppose $f : X \to P(\{1\})$ is an order embedding. WLOG

$f(a) = \emptyset \qquad f(b) = \{1\}$

b/c f is injective. But

$$f(a) = \emptyset \subseteq \{1\} = f(b)$$

$\xRightarrow[\text{preserving}]{\text{order}}$ $a \leq b$. Contradiction. $\blacksquare$

$\overset{\triangle S}{\perp}$; f is an order embedding

$\Leftrightarrow$ f is monotone and order preserving $\quad (\Downarrow \;\; \not\Uparrow)$

$\not\Leftrightarrow$ f is monotone and injective

Q1.2 Find a counterexample to

"$a, b \in \mathbb{Z}$ and p a prime $v_p(a+b) = \max(v_p(a), v_p(b))$"

Remark: Actually true is

$$v_p(a+b) \geq \min(v_p(a), v_p(b))$$

if $v_p(a) \neq v_p(b) \Rightarrow v_p(a+b) = \min(v_p(a), v_p(b))$.

Solution: Set $a=b=p=2$. Then

$$v_p(a) = v_p(b) = v_2(2) = 1$$

but

$$v_p(a+b) = v_2(2+2) = v_2(4) = 2$$

So,

$$v_p(a+b) = 2 \neq \max(v_p(a), v_p(b)) = 1.$$

Alternative Solution: Take $a = p-1$, $b = 1$

w/ p any prime

Remark: on exam choose actual numbers!

Only doing this for culture.

$$V_p(a) = V_p(p-1) = 0$$

$$v_p(b) = v_p(1) = 0$$

but

$$v_p(a+b) = v_p(p-1+1) = v_p(p) = 1$$

So

$$v_p(a+b) = 1 \neq 0 = \max(v_p(a), v_p(b)).$$

Q1.3 Find a countee xample to

" If $f: X \to Y$ an $A \subseteq Y$ then

$A = f(f^{-1}(A))$."

Remark: In fact, this claim is true

$\forall A \subseteq Y$ precisely when f is surjective.

Solution: Take $X = \{a\}$ and $Y = \{1,2\}$. Define $f(a) = 1$. Take $A = \{2\} \subseteq Y$. Then,

$$f^{-1}(A) = \{x \in X : f(x) \in A\}$$
$$= \emptyset$$

Then

$$f(f^{-1}(A)) = f(\emptyset)$$
$$= \emptyset$$
$$\neq A. \qquad \blacksquare$$

<u>Remark</u>: If $A = \{1\}$, then

$$f^{-1}(A) = \{x \in X : f(x) \in A\}$$

$$= \{a\}$$

$$= X$$

the

$$f(f^{-1}(A)) = f(X)$$

$= \{1\}$

$= A.$

Remark: $A = f(f^{-1}(A)) \Leftarrow$

$A \subseteq f(X).$

Remark: Study what $\boxed{\text{images}}$ (i.e., $f(-)$) and $\boxed{\text{preimages}}$ (i.e., $f^{-1}(-)$) are — understand the difference between $\boxed{\text{preimage}}$

and inverse function

Q2| Prove by induction that for all $n \geq 1$, 6 divides $n^3 - n$.

Pf: We proceed by induction.

Base Case ($n=1$): $1^3 - 1 = 0$ which is divisible by 6. ✓

Inductive step: Assume that $6 \mid n^3 - n$. Want to show that $6 \mid (n+1)^3 - (n+1)$.

Observe that

$$(n+1)^3 - (n+1) = n^3 + 3n^2 + 2n$$

$$= (n^3 - n) + 3n^2 + 3n$$

We know is that $6 \mid n^3 - n$ by IH. So, it suffices to show $6 \mid 3n^2 + 3n$. Note

$$3n^2 + 3n = 3(n^2 + n) = 3\,n(n+1).$$

Because n or $n+1$ is even $\Rightarrow 2 \mid n(n+1)$. So,

$3 \cdot 2 \mid 3 \cdot n(n+1)$, i.e., $6 \mid 3n(n+1)$. $\blacksquare$

<u>Remark</u>: You can also show $6 \mid 3n(n+1)$ by induction.

— there's also a proof that $6 \mid n^3 - n$

in a similar fashion (exercise: $(n-1)\cdot n(n+1)$).

Q3 | Let n, m be coprime elements of $\mathbb{N}$.

Show that if $x \in \mathbb{N}$ and $\sqrt[m]{x^n} \in \mathbb{Q} \Rightarrow \sqrt[m]{x} \in \mathbb{Q}$.

Solution: From class: $\sqrt[m]{x} \in \mathbb{Q} \iff$

- $\text{sgn}(x) = 1$ or $(\text{sgn}(x) = -1$ and m is odd$)$,
- $\forall$ prime p, $m \mid v_p(x)$.

Note that $x \in \mathbb{N}$, $\operatorname{sgn}(x) = 1$. So, the first bullet is satisfied.

But, for p a prime we want to show $m \mid v_p(x)$. But, $\sqrt[m]{x^n} \in \mathbb{Q}$ so $m \mid v_p(x^n)$. But, $v_p(x^n) = n \cdot v_p(x)$, so $m \mid n \cdot v_p(x)$. But, since m, n coprime

$m \mid n \cdot v_p(x) \implies m \mid v_p(x).$ ∎

Remark: Common mistake: $v_p(\sqrt[m]{x})$ does not make sense unless $\sqrt[m]{x} \in \mathbb{Q}$.

$v_p(\underbrace{\sqrt[m]{x^n}}_{\in \mathbb{Q}})$

$v_p(x^{\frac{n}{m}})$

wanted to say $v_p(\sqrt[m]{x}) = v_p(x^{\frac{1}{m}}) = \frac{v_p(x)}{m}$

Alternative Solution: As m and n are coprime

Bezout's lemma $\Longleftrightarrow$ $am + bn = 1$ for some $a, b \in \mathbb{Z}$,

$$\sqrt[m]{x} = x^{\frac{1}{m}}$$
$$= (x^{1})^{\frac{1}{m}}$$
$$= (x^{am+bn})^{\frac{1}{m}}$$
$$= x^{a} \cdot x^{\frac{bn}{m}}$$
$$= x^{a} \cdot (\sqrt[m]{x^{n}})^{b} \in \mathbb{Q} \text{ bc } \sqrt[m]{x^{n}} \in \mathbb{Q}$$

$\uparrow$

Q

by assumption

Q41 Let $(X, \leq)$ be a poset. Define a relation $\leq^{op}$ on X by

$$x \leq^{op} y \overset{\text{def}^n}{\iff} x \geq y$$

1. Show that $(X, \leq^{op})$ is still a poset,
2. Show if $(Y, \preceq)$ is another poset then

$$(X, \leq) \simeq (Y, \preceq) \iff (X, \leq^{op}) \simeq (Y, \preceq^{op}).$$

e.g. $(X, \le) =$

$$\begin{tikzcd} & d & \\ b \arrow[ur] & & c \arrow[ul] \\ & a \arrow[ul] \arrow[ur] & \end{tikzcd}$$

$\Rightarrow (X, \le^{op}) =$

$$\begin{tikzcd} & d \arrow[dl] \arrow[dr] & \\ b \arrow[dr] & & c \arrow[dl] \\ & a & \end{tikzcd}$$

e.g. 1 $\bullet \xrightarrow{\le} \bullet \xrightarrow{\le} \bullet \xrightarrow{\le} \cdots$ $\mathcal{L}$ infinite

$(X, \le)$ //

$\mathbb{Z}$

$$(X, \leq^{op}) = \bullet \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \leftarrow \cdots$$

<u>Solution:</u>

1. Want to show that $\leq^{op}$ is reflexive, transitive, and anti-symmetric.

<u>Reflexive:</u> $x \leq^{op} x \overset{\text{def'n}}{\Longleftarrow} \quad x \leq x$

and the latter is true by reflexivity of

$\leq$.

Transitivity: Assume that $x \leq^{op} y$ and $y \leq^{op} z$. By definition this is equivalent to $x \geq y$ and $y \geq z$. So by transitivity of $\leq$ we see that $x \geq z$. So, by defn $x \leq^{op} z$.

Anti-symmetry: Assume that $x \leq^{op} y$ and $y \leq^{op} x$. But, by defn this is equivalent to $x \geq y$ and $y \geq x$. But by anti-symmetry of $\leq \Rightarrow x = y$.

2. An isom. $(X, \leq) \to (Y, \preceq)$

or $(X, \leq^{op}) \to (Y, \preceq^{op})$ in particular a bijection $f: X \to Y$ s.t. f is monotone and order preserving. For the first case this is equivalent to

$$x_1 \leq x_2 \iff f(x_1) \preceq f(x_2) \quad \forall x_1, x_2 \in X \quad (\ast)$$

In the latter case this is equivalent to

$x_1 \leq^{op} x_2 \Longleftrightarrow f(x_1) \preceq^{op} f(x_2)\ \forall x_1, x_2 \in X$.

But, by definition this is equivalent to

(**) $x_1 \geq x_2 \Longleftrightarrow f(x_1) \succeq f(x_2)\ \forall x_1, x_2 \in X$

But, (*) and (**) are the same condition, so, the claim follows. □

Q51 Let $f: X \to Y$ be a function.

Show the following are equivalent:

1.) f is bijective,

2.) $\forall A \subseteq X$: $f(X-A) = Y - f(A)$.

Solution: $1. \Rightarrow 2.$ First take $y \in f(X-A)$.

By definition of image $\exists\, x \in X-A$ s.t.

$y = f(x)$. Note $y \notin f(A)$. Indeed, if it were true by def'n $\exists\ a \in A$ s.t. $y = f(a)$.

But as $y = f(x)$ and f is injective $\Rightarrow x = a$.

But, $x \in X - A$ and $a \in A$, this is a contradiction.

So, $y \in Y - f(A)$.

Conversely, $y \in Y - f(A)$. As f is surj.

$\exists\ x \in X$ s.t. $y = f(x)$. Note $x \notin A$ as then $y = f(x)$ would be in $f(A)$. Thus, $x \in X - A$. So, $y = f(x) \in f(X - A)$.

2. $\Rightarrow$ 1: To show f is surj.

we must show $Y = f(X)$. To show

this we take $A = \emptyset$ so

$$f(X) = f(X - \emptyset) = Y - f(\emptyset) = Y$$

as desired.

To show f is injective assume $x_1 \neq x_2$ want to show $f(x_1) \neq f(x_2)$. Take $A = \{x_1\}$.

Note $x_2 \in X - A$, so $f(x_2) \in f(X - A)$

$$= Y - f(A)$$

$$= Y - \{f(x_1)\}$$

So $f(x_2) \notin \{f(x_1)\} \Rightarrow f(x_2) \neq f(x_1)$ $\boxtimes$

Remark: Common mistakes:

1) Not using full power for $1. \Rightarrow 2.$ or $2. \Rightarrow 1$ (e.g., for $1. \Rightarrow 2.$ using that f is surjective but not using that f was injective).

2) They made claims which

looked reasonable but actually need a condition, e.g., $x \notin A \Rightarrow f(x) \notin f(A)$.

But is equivalent to f being injective. (exercise!).

Q61 Look at exam

1. Show $\mathcal{I} = \{(a,b) : a \le b \text{ rationals}\}$ countable

$(1,0)$

Solution: Let $S = \{(a,b) \in \mathbb{Q}^2 : a \le b\}$. Then,

$f : S \to \mathcal{I}$ given by $(a,b) \mapsto [a,b]$. This

is surj. so

from class

$$\# \mathcal{I} \le \# S \le \# \mathbb{Q}^2 \le \aleph_0 \quad \blacksquare$$

2: Show $\mathcal{U} = \left\{ [a_1, b_1] \cup \cdots \cup [a_n, b_n] : \begin{array}{l} n \geq 1 \text{ and} \\ a_i \leq b_i \in \mathbb{Q} \\ \forall i = 1, \ldots, n \end{array} \right\}$

is countable.

Solution: Note $\mathcal{U} = \bigcup_{n=1}^{\infty} \mathcal{U}_n$ where

$$\mathcal{U}_n = \left\{ [a_1, b_1] \cup \cdots \cup [a_n, b_n] : \begin{array}{l} a_i \leq b_i \in \mathbb{Q} \\ i = 1, \ldots, n \end{array} \right\}$$

Note for each n we have a surj.

$$S^n \to \mathcal{U}_n,\ ((a_1,b_1),\dots,(a_n,b_n)) \mapsto [a_1,b_1] \cup \dots \cup [a_n,b_n]$$

So

$$\# \mathcal{U}_n \le \# S^n \le \# (\mathbb{Q}^2)^n = \aleph_0$$

proved in class.

So, each U_n is countable, so

$U = \bigcup_{n=1}^{\infty} U_n$ is a countable union

of countable sets, so countable

from theorem in class.

3. Why does this not contradict

that $P(\mathbb{R})$ is uncountable?

<u>Solution:</u> There are many $S \subseteq \mathbb{R}$ not in $\mathcal{U}$, e.g., $\{\sqrt{2}\} \notin \mathcal{U}$.

Email Q and A:

Q1: Can we use (when proving equality of subsets) set algebra and/or set identities (e.g., de Morgan's laws, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, ...)

A: No.

"e.g." To show that $A = B$

your proof should look like "take

$x \in A$ ... basic logic ... then $x \in B$..."

not

"$A = \_\_ = \_\_ = \_\_$

$= \_\_ = B$"

Q2.1

Q2.1 Are there any properties of posets not preserved by taking opposites? (as in Q4 of practice tutorial).

A: Yes! If $(X, \leq)$ has a

largest element thm $(X, \leq^{op})$ need

not e.g. $(X, \leq) = \bullet \to \bullet \to \bullet \to \cdots$

Q2.2) In Q3 what goes wrong if n and m are not coprime?

Cases, for $\sqrt[m]{x^n} \in \mathbb{Q} \Rightarrow \sqrt[m]{x} \in \mathbb{Q}$)

A) Lots $\longrightarrow$ $m = n$ fu

$$\sqrt[m]{x^m} = x \in \mathbb{Q} \not\Rightarrow \sqrt[m]{x} \in \mathbb{Q}.$$

Functionally in the proof the step $m \mid n \cdot v_p(x) \Rightarrow m \mid v_p(x)$ fails if m and n are not coprime, Q2.3) How much algebra is expected in inductive steps,

A) Minimal – all basic algebraic manipulations (e.g. FOIL, groupings of terms, etc.) can be skipped. Show any "not obvious steps"

Q2.4) Is a finite union of countable sets countable? What about an infinite union?

A) A countable union of countable sets is countable. (e.g. $\bigcup_{n=0}^{\infty} S_n$ ← countable)

But an uncountable union of countable sets need not be countable.

Q: How is $\aleph_0$ useful in proofs

A: X being countable $\iff \#X \leq \aleph_0$

So b/c $f: X \to Y$ surj $\Rightarrow$

$\#Y \leq \#X$, or $f: X \to Y$ inj

$\Rightarrow \#X \leq \#Y$

characterization is helpful for manipulating

Q: Can we approach 3. by

$$v_p(\sqrt[m]{x^n}) = v_p(x^{\frac{n}{m}}) = \frac{n}{m} v_p(x) \; ?$$

$\mathbb{Q}$

A: No! BC $v_p(xy) = v_p(x) + v_p(y)$ ~~(x)~~

when $x, y \in \mathbb{Q}$.

When trying to prove $v_p(x^{\frac{n}{m}}) = \frac{n}{m} v_p(x)$

you're trying to apply (*) as

$$v_p(x^{\frac{n}{m}}) = v_p(\underbrace{x^{\frac{1}{m}} \cdot x^{\frac{1}{m}} \cdots x^{\frac{1}{m}}}_{n \text{ times}})$$

$$= n\, v_p(x^{\frac{1}{m}})$$

By $\quad m\, v_p(x^{\frac{1}{m}}) = v_p\left(\left(x^{\frac{1}{m}}\right)^m\right)$

$$= v_p(x)$$

$$\Rightarrow \quad v_p(x^{\frac{1}{m}}) = \frac{1}{m} v_p(x).$$

In particular this will

invalid $v_p(x^{\frac{1}{n}})$ which is bad

— $v_p(x^\alpha) = \alpha \cdot v_p(x)$ works

if $x \in \mathbb{Q}$ and $\alpha \in \mathbb{Z}$