Valuations and S-units

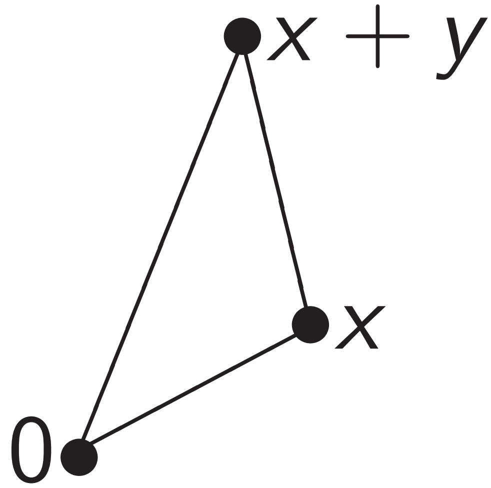
D. J. Bernstein

University of Illinois at Chicago;
Ruhr University Bochum

$\mathbf{R}$ = field of real numbers.
$\mathbf{C}$ = field of complex numbers.

The function $x \mapsto |x|$
from $\mathbf{C}$ to $\mathbf{R}$ is a **valuation on C**:

- $|0| = 0$.
- $x \neq 0 \Rightarrow |x| > 0$.
- $|xy| = |x||y|$.
- $|x + y| \leq |x| + |y|$.



There are other valuations on **C**.

e.g. $x \mapsto \sqrt{|x|}$ is a valuation.
Exercise: $\sqrt{|x+y|} \leq \sqrt{|x|} + \sqrt{|y|}$.

There are other valuations on **C**.

e.g. $x \mapsto \sqrt{|x|}$ is a valuation.
Exercise: $\sqrt{|x+y|} \le \sqrt{|x|} + \sqrt{|y|}$.

e.g. $x \mapsto |x|^{0.31415}$ is a valuation.

There are other valuations on **C**.

e.g. $x \mapsto \sqrt{|x|}$ is a valuation.
Exercise: $\sqrt{|x+y|} \le \sqrt{|x|} + \sqrt{|y|}$.

e.g. $x \mapsto |x|^{0.31415}$ is a valuation.

e.g. $x \mapsto |x|^{\delta}$ is a valuation
for any $\delta \in \mathbf{R}$ with $0 < \delta \le 1$.

There are other valuations on $\mathbf{C}$.

e.g. $x \mapsto \sqrt{|x|}$ is a valuation.
Exercise: $\sqrt{|x+y|} \le \sqrt{|x|} + \sqrt{|y|}$.

e.g. $x \mapsto |x|^{0.31415}$ is a valuation.

e.g. $x \mapsto |x|^{\delta}$ is a valuation
for any $\delta \in \mathbf{R}$ with $0 < \delta \le 1$.

These valuations are **equivalent**:
positive powers of each other.
They have the same unit disks:
they map the same inputs to $\mathbf{R}_{\le 1}$.

There are other valuations on $\mathbf{C}$.

e.g. $x \mapsto \sqrt{|x|}$ is a valuation.
Exercise: $\sqrt{|x+y|} \le \sqrt{|x|} + \sqrt{|y|}$.

e.g. $x \mapsto |x|^{0.31415}$ is a valuation.

e.g. $x \mapsto |x|^{\delta}$ is a valuation
for any $\delta \in \mathbf{R}$ with $0 < \delta \le 1$.

These valuations are **equivalent**:
positive powers of each other.
They have the same unit disks:
they map the same inputs to $\mathbf{R}_{\le 1}$.

Not equivalent: **trivial valuation**
defined by $0 \mapsto 0$; $x \mapsto 1$ if $x \ne 0$.
Unit disk is all inputs.

$\mathbf{Q}$ = field of rational numbers.

The function $x \mapsto |x|$ from $\mathbf{Q}$ to $\mathbf{R}$ is a valuation on $\mathbf{Q}$. Same as previous $x \mapsto |x|$, but restricts $\mathbf{C}$ inputs to be in $\mathbf{Q}$.

$\mathbf{Q}$ = field of rational numbers.

The function $x \mapsto |x|$ from $\mathbf{Q}$ to $\mathbf{R}$ is a valuation on $\mathbf{Q}$. Same as previous $x \mapsto |x|$, but restricts $\mathbf{C}$ inputs to be in $\mathbf{Q}$.

A nonequivalent nontrivial valuation on $\mathbf{Q}$: define $|0|_3 = 0$, $|x|_3 = 3^{-e_3}$ if $x = \pm 2^{e_2} 3^{e_3} 5^{e_5} \cdots$. e.g. $|90|_3 = 1/9$; $|-7/3|_3 = 3$.

$\mathbf{Q}$ = field of rational numbers.

The function $x \mapsto |x|$
from $\mathbf{Q}$ to $\mathbf{R}$ is a valuation on $\mathbf{Q}$.
Same as previous $x \mapsto |x|$, but
restricts $\mathbf{C}$ inputs to be in $\mathbf{Q}$.

A nonequivalent nontrivial
valuation on $\mathbf{Q}$: define $|0|_3 = 0$,
$|x|_3 = 3^{-e_3}$ if $x = \pm 2^{e_2} 3^{e_3} 5^{e_5} \cdots$.
e.g. $|90|_3 = 1/9$; $|-7/3|_3 = 3$.

- $|0|_3 = 0$.
- $x \neq 0 \Rightarrow |x|_3 > 0$.
- $|xy|_3 = |x|_3 |y|_3$.
- $|x + y|_3 \leq |x|_3 + |y|_3$.

Even better: $\leq \max\{|x|_3, |y|_3\}$.

For $x \in \mathbf{Q}$, define $|x|_\infty = |x|$;
$|x|_p = p^{-e_p}$ if $x = \pm 2^{e_2} 3^{e_3} 5^{e_5} \ldots$.

x	$\lvert x\rvert_\infty$	$\lvert x\rvert_2$	$\lvert x\rvert_3$	$\lvert x\rvert_5$	$\ldots$	product
$\vdots$						
-2	2	1/2	1	1	$\ldots$	1
-1	1	1	1	1	$\ldots$	1
0	0	0	0	0	$\ldots$	0
1	1	1	1	1	$\ldots$	1
2	2	1/2	1	1	$\ldots$	1
3	3	1	1/3	1	$\ldots$	1
4	4	1/4	1	1	$\ldots$	1
5	5	1	1	1/5	$\ldots$	1
6	6	1/2	1/3	1	$\ldots$	1
$\vdots$						

[don't forget $x = 2/3$ etc.]

Infinite-dimensional lattice of $(\log|x|_\infty, \log|x|_2, \log|x|_3, \ldots)$:

$\log\|x\|_\infty$	$\log\|x\|_2$	$\log\|x\|_3$	$\log\|x\|_5$	$\ldots$
$\vdots$				
$\log 2$	$-\log 2$	0	0	$\ldots$
0	0	0	0	$\ldots$
[skip $x = 0$: log 0 not defined]				
0	0	0	0	$\ldots$
$\log 2$	$-\log 2$	0	0	$\ldots$
$\log 3$	0	$-\log 3$	0	$\ldots$
$\log 4$	$-\log 4$	0	0	$\ldots$
$\log 5$	0	0	$-\log 5$	$\ldots$
$\log 6$	$-\log 2$	$-\log 3$	0	$\ldots$
$\vdots$	[again don't forget 2/3 etc.]			

This lattice, the set of vectors $(\log|x|_\infty, \log|x|_2, \log|x|_3, \ldots)$, is
$(\log 2, -\log 2, 0, 0, 0, \ldots)\mathbf{Z} +$
$(\log 3, 0, -\log 3, 0, 0, \ldots)\mathbf{Z} +$
$(\log 5, 0, 0, -\log 5, 0, \ldots)\mathbf{Z} +$
$(\log 7, 0, 0, 0, -\log 7, \ldots)\mathbf{Z} +$
$\cdots$ where
$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

This lattice, the set of vectors
$(\log|x|_\infty, \log|x|_2, \log|x|_3, \ldots)$, is
$(\log 2, -\log 2, 0, 0, 0, \ldots)\mathbf{Z} +$
$(\log 3, 0, -\log 3, 0, 0, \ldots)\mathbf{Z} +$
$(\log 5, 0, 0, -\log 5, 0, \ldots)\mathbf{Z} +$
$(\log 7, 0, 0, 0, -\log 7, \ldots)\mathbf{Z} +$
$\cdots$ where
$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

$x = \pm 2^{e_2} 3^{e_3} 5^{e_5} \cdots$ maps to
$(\log|x|_\infty, \log|x|_2, \log|x|_3, \ldots) =$
$(\log 2, -\log 2, 0, 0, 0, \ldots)e_2 +$
$(\log 3, 0, -\log 3, 0, 0, \ldots)e_3 +$
$(\log 5, 0, 0, -\log 5, 0, \ldots)e_5 +$
$(\log 7, 0, 0, 0, -\log 7, \ldots)e_7 +$
$\cdots$

Can divide $\log|x|_p$ by $\log p$ to obtain an integer "$-\operatorname{ord}_p x$"; $\operatorname{ord}_p(\pm 2^{e_2} 3^{e_3} 5^{e_5} \cdots) = e_p$.

Number theorists include the $\log p$ weight for many reasons:

- leaving out the weight would produce infinitely many short log vectors (e.g., length <2);
- want "the product formula": $\prod_v |x|_v = 1$; $\sum_v \log|x|_v = 0$;
- this particular power $|x|_v$ has a probability interpretation (matches "Haar measure" on the "completion"); etc.

Say $S \subseteq \{\infty, 2, 3, 5, \ldots\}$, $\infty \in S$.

Typical case: $p \in S \Leftrightarrow p \leq 37$.

Say $S \subseteq \{\infty, 2, 3, 5, \ldots\}$, $\infty \in S$.
Typical case: $p \in S \Leftrightarrow p \le 37$.

$x \in \mathbf{Q}$ is called an S-**integer**
if $|x|_p \le 1$ for each $p \notin S$.

Say $S \subseteq \{\infty, 2, 3, 5, \ldots\}$, $\infty \in S$.
Typical case: $p \in S \Leftrightarrow p \leq 37$.

$x \in \mathbf{Q}$ is called an S-**integer**
if $|x|_p \leq 1$ for each $p \notin S$.

$\{S\text{-integers}\}$ is a subring of $\mathbf{Q}$:
closed under mult since $\mathbf{R}_{\leq 1}$ is;
closed under addition since
$|x + y|_p \leq \max\{|x|_p, |y|_p\}$.

Say $S \subseteq \{\infty, 2, 3, 5, \ldots\}$, $\infty \in S$.
Typical case: $p \in S \Leftrightarrow p \leq 37$.

$x \in \mathbf{Q}$ is called an S-**integer**
if $|x|_p \leq 1$ for each $p \notin S$.

$\{S\text{-integers}\}$ is a subring of $\mathbf{Q}$:
closed under mult since $\mathbf{R}_{\leq 1}$ is;
closed under addition since
$|x + y|_p \leq \max\{|x|_p, |y|_p\}$.

For any commutative ring R:
R^* means $\{u \in R : uR = R\}$.

Say $S \subseteq \{\infty, 2, 3, 5, \ldots\}$, $\infty \in S$.
Typical case: $p \in S \Leftrightarrow p \leq 37$.

$x \in \mathbf{Q}$ is called an S-**integer**
if $|x|_p \leq 1$ for each $p \notin S$.

$\{S\text{-integers}\}$ is a subring of $\mathbf{Q}$:
closed under mult since $\mathbf{R}_{\leq 1}$ is;
closed under addition since
$|x + y|_p \leq \max\{|x|_p, |y|_p\}$.

For any commutative ring R:
R^* means $\{u \in R : uR = R\}$.

$x \in \mathbf{Q}^*$ is called an S-**unit**
if $|x|_p = 1$ for each $p \notin S$.
$\{S\text{-units}\} = \{S\text{-integers}\}^*$.

e.g. x is an $\{\infty\}$-integer

$\Leftrightarrow |x|_2 \leq 1, |x|_3 \leq 1, \ldots$

$\Leftrightarrow x \in \mathbf{Z}$.

So $\{\{\infty\}\text{-integers}\} = \mathbf{Z}$,

the usual ring of integers.

e.g. x is an $\{\infty\}$-integer

$\Leftrightarrow |x|_2 \le 1,\ |x|_3 \le 1,\ \ldots$

$\Leftrightarrow x \in \mathbf{Z}$.

So $\{\{\infty\}$-integers$\} = \mathbf{Z}$,

the usual ring of integers.

e.g. x is an $\{\infty\}$-unit

$\Leftrightarrow |x|_2 = 1,\ |x|_3 = 1,\ \ldots$

$\Leftrightarrow \log|x|_2 = 0,\ \log|x|_3 = 0,\ \ldots$

$\Leftrightarrow x \in \{-1, 1\}$.

e.g. x is an $\{\infty\}$-integer
$\Leftrightarrow |x|_2 \le 1,\ |x|_3 \le 1,\ \ldots$
$\Leftrightarrow x \in \mathbf{Z}$.
So $\{\{\infty\}\text{-integers}\} = \mathbf{Z}$,
the usual ring of integers.

e.g. x is an $\{\infty\}$-unit
$\Leftrightarrow |x|_2 = 1,\ |x|_3 = 1,\ \ldots$
$\Leftrightarrow \log|x|_2 = 0,\ \log|x|_3 = 0,\ \ldots$
$\Leftrightarrow x \in \{-1, 1\}$.

This also forces $\log|x|_\infty = 0$:
$\{-1, 1\}$ have log vector $(0, 0, \ldots)$.

e.g. x is an $\{\infty\}$-integer
$\Leftrightarrow |x|_2 \le 1$, $|x|_3 \le 1$, ...
$\Leftrightarrow x \in \mathbf{Z}$.
So $\{\{\infty\}$-integers$\} = \mathbf{Z}$,
the usual ring of integers.

e.g. x is an $\{\infty\}$-unit
$\Leftrightarrow |x|_2 = 1$, $|x|_3 = 1$, ...
$\Leftrightarrow \log|x|_2 = 0$, $\log|x|_3 = 0$, ...
$\Leftrightarrow x \in \{-1, 1\}$.

This also forces $\log|x|_\infty = 0$:
$\{-1, 1\}$ have log vector $(0, 0, \ldots)$.

$\{-1, 1\} = \mathbf{Z}^*$.
Don't confuse with $\mathbf{Q}^* = \mathbf{Q} - \{0\}$.

e.g. x is an $\{\infty, 2, 3\}$-integer
$\Leftrightarrow |x|_5 \leq 1, |x|_7 \leq 1, \ldots$
$\Leftrightarrow x \in 2^{\mathbf{Z}} 3^{\mathbf{Z}} \mathbf{Z}$.

e.g. x is an $\{\infty, 2, 3\}$-integer
$\Leftrightarrow |x|_5 \le 1$, $|x|_7 \le 1$, ...
$\Leftrightarrow x \in 2^{\mathbf{Z}} 3^{\mathbf{Z}} \mathbf{Z}$.

e.g. x is an $\{\infty, 2, 3\}$-unit
$\Leftrightarrow |x|_5 = 1$, $|x|_7 = 1$, ...
$\Leftrightarrow x \in \pm 2^{\mathbf{Z}} 3^{\mathbf{Z}}$
$\Leftrightarrow x$ is “3-smooth”.

e.g. x is an $\{\infty, 2, 3\}$-integer
$\Leftrightarrow |x|_5 \le 1,\ |x|_7 \le 1,\ \ldots$
$\Leftrightarrow x \in 2^{\mathbf{Z}} 3^{\mathbf{Z}} \mathbf{Z}$.

e.g. x is an $\{\infty, 2, 3\}$-unit
$\Leftrightarrow |x|_5 = 1,\ |x|_7 = 1,\ \ldots$
$\Leftrightarrow x \in \pm 2^{\mathbf{Z}} 3^{\mathbf{Z}}$
$\Leftrightarrow$ x is "3-smooth".

For S-units can focus on S-logs:
$x \mapsto (\log |x|_\infty, \log |x|_2, \log |x|_3)$
maps group $\pm 2^{\mathbf{Z}} 3^{\mathbf{Z}}$ to lattice
$(\log 2, -\log 2, 0)\mathbf{Z} +$
$(\log 3, 0, -\log 3)\mathbf{Z}$.

Increase S for more S-units.

Prime element p of R:

- $R - pR$ closed under mult;
- $pR \neq R$ (i.e., $p \notin R^*$);
- $pR \neq \{0\}$ (i.e., $p \neq 0$).

Prime element p of R:

- $R - pR$ closed under mult;
- $pR \neq R$ (i.e., $p \notin R^*$);
- $pR \neq \{0\}$ (i.e., $p \neq 0$).

$\{\infty\}$-integers $\mathbf{Z}$ have prime elements $\{\pm 2, \pm 3, \pm 5, \pm 7, \ldots\}$, i.e., $\{2, 3, 5, 7, \ldots\}\mathbf{Z}^*$.

Prime element p of R:

- $R - pR$ closed under mult;
- $pR \neq R$ (i.e., $p \notin R^*$);
- $pR \neq \{0\}$ (i.e., $p \neq 0$).

$\{\infty\}$-integers $\mathbf{Z}$ have prime elements $\{\pm 2, \pm 3, \pm 5, \pm 7, \ldots\}$, i.e., $\{2, 3, 5, 7, \ldots\}\mathbf{Z}^*$.

Can write any $x \in \mathbf{Z} - \{0\}$ uniquely as $u 2^{e_2} 3^{e_3} 5^{e_5} \cdots$ where $u \in \mathbf{Z}^*$, $e_p \in \{0, 1, 2, \ldots\}$.

Prime element p of R:

- $R - pR$ closed under mult;
- $pR \neq R$ (i.e., $p \notin R^*$);
- $pR \neq \{0\}$ (i.e., $p \neq 0$).

$\{\infty\}$-integers $\mathbf{Z}$ have prime elements $\{\pm 2, \pm 3, \pm 5, \pm 7, \ldots\}$, i.e., $\{2, 3, 5, 7, \ldots\}\mathbf{Z}^*$.

Can write any $x \in \mathbf{Z} - \{0\}$ uniquely as $u 2^{e_2} 3^{e_3} 5^{e_5} \cdots$ where $u \in \mathbf{Z}^*$, $e_p \in \{0, 1, 2, \ldots\}$.

Log: nonnegative combination of $(\log 2, -\log 2, 0, 0, \ldots)$; $(\log 3, 0, -\log 3, 0, \ldots)$; etc. u disappears in log vector.

$\{\infty, 2, 3\}$-integers $2^{\mathbf{Z}}3^{\mathbf{Z}}\mathbf{Z}$ have prime elements $\{\pm 5, \pm 7, \ldots\}$.

$2, 3 \in (2^{\mathbf{Z}}3^{\mathbf{Z}}\mathbf{Z})^*$; no longer prime!

$\{\infty, 2, 3\}$-integers $2^{\mathbf{Z}}3^{\mathbf{Z}}\mathbf{Z}$ have prime elements $\{\pm 5, \pm 7, \ldots\}$. $2, 3 \in (2^{\mathbf{Z}}3^{\mathbf{Z}}\mathbf{Z})^*$; no longer prime!

Can write any $x \in 2^{\mathbf{Z}}3^{\mathbf{Z}}\mathbf{Z} - \{0\}$ uniquely as $u 5^{e_5} 7^{e_7} \cdots$ where $u \in (2^{\mathbf{Z}}3^{\mathbf{Z}}\mathbf{Z})^*$, $e_p \in \{0, 1, 2, \ldots\}$.

$\{\infty, 2, 3\}$-integers $2^{\mathbf{Z}}3^{\mathbf{Z}}\mathbf{Z}$ have prime elements $\{\pm 5, \pm 7, \ldots\}$.
$2, 3 \in (2^{\mathbf{Z}}3^{\mathbf{Z}}\mathbf{Z})^*$; no longer prime!

Can write any $x \in 2^{\mathbf{Z}}3^{\mathbf{Z}}\mathbf{Z} - \{0\}$ uniquely as $u 5^{e_5} 7^{e_7} \cdots$ where $u \in (2^{\mathbf{Z}}3^{\mathbf{Z}}\mathbf{Z})^*$, $e_p \in \{0, 1, 2, \ldots\}$.

i.e. $u \in \pm 2^{\mathbf{Z}}3^{\mathbf{Z}}$.
u logs: integer combination of
$(\log 2, -\log 2, 0, \ldots)$,
$(\log 3, 0, -\log 3, \ldots)$.

$\{\infty, 2, 3\}$-integers $2^{\mathbf{Z}}3^{\mathbf{Z}}\mathbf{Z}$ have prime elements $\{\pm 5, \pm 7, \ldots\}$.
$2, 3 \in (2^{\mathbf{Z}}3^{\mathbf{Z}}\mathbf{Z})^*$; no longer prime!

Can write any $x \in 2^{\mathbf{Z}}3^{\mathbf{Z}}\mathbf{Z} - \{0\}$ uniquely as $u 5^{e_5} 7^{e_7} \cdots$ where $u \in (2^{\mathbf{Z}}3^{\mathbf{Z}}\mathbf{Z})^*$, $e_p \in \{0, 1, 2, \ldots\}$.

i.e. $u \in \pm 2^{\mathbf{Z}}3^{\mathbf{Z}}$.
u logs: integer combination of
$(\log 2, -\log 2, 0, \ldots)$,
$(\log 3, 0, -\log 3, \ldots)$.

$5^{e_5} 7^{e_7} \cdots$ logs: combine
$(\log 5, 0, 0, -\log 5, \ldots)$;
$(\log 7, 0, 0, 0, -\log 7, \ldots)$;
etc.

The 4th cyclotomic field

i: the usual $\sqrt{-1}$ in $\mathbf{C}$.

$\mathbf{Q}(i) = \mathbf{Q} + \mathbf{Q}i$ is a field:

the "field of Gaussian rationals";

the "4th cyclotomic field".

e.g. $3/11 - 2i/5 \in \mathbf{Q}(i)$.

The 4th cyclotomic field

i: the usual $\sqrt{-1}$ in $\mathbf{C}$.
$\mathbf{Q}(i) = \mathbf{Q} + \mathbf{Q}i$ is a field:
the "field of Gaussian rationals";
the "4th cyclotomic field".
e.g. $3/11 - 2i/5 \in \mathbf{Q}(i)$.

(More generally, $\mathbf{Q}(\alpha)$ means the smallest field containing $\mathbf{Q}$, α.)

The 4th cyclotomic field

i: the usual $\sqrt{-1}$ in $\mathbf{C}$.
$\mathbf{Q}(i) = \mathbf{Q} + \mathbf{Q}i$ is a field:
the "field of Gaussian rationals";
the "4th cyclotomic field".
e.g. $3/11 - 2i/5 \in \mathbf{Q}(i)$.

(More generally, $\mathbf{Q}(\alpha)$ means the smallest field containing $\mathbf{Q}$, α.)

Fact: Each $x \in \mathbf{Q}(i)^*$
factors uniquely as $r \prod_{p \in P} p^{e_p}$
where $r \in \{1, i, -1, -i\}$;
$P = \{1 + i, 3, 2 + i, 2 - i, \ldots\}$;
each e_p is an integer.

$|a+bi|^2 = a^2 + b^2$ for $a, b \in \mathbf{R}$.

For each $p \in P$: have $p \in \mathbf{Z} + \mathbf{Z}i$, and $|p|^2$ is a prime not in $3 + 4\mathbf{Z}$ or the square of a prime in $3+4\mathbf{Z}$:

$p = 1 + i$: $|p|^2 = 2$.

$p = 3$: $|p|^2 = 9$.

$p = 2 + i$: $|p|^2 = 5$.

$p = 2 - i$: $|p|^2 = 5$.

$p = 7$: $|p|^2 = 49$.

$p = 11$: $|p|^2 = 121$.

$p = 3 + 2i$: $|p|^2 = 13$.

$p = 3 - 2i$: $|p|^2 = 13$.

etc. (To fully define P, also handle $1, i, -1, -i$ multiples.)

Standard *powers* of nonequivalent nontrivial valuations on $\mathbf{Q}(i)$:

$|x|_\infty = |x|^2$. (Warning: $x \mapsto |x|$ is a valuation; $x \mapsto |x|^2$ isn't!)

$|x|_{1+i} = 2^{-e_{1+i}}$.

$|x|_3 = 9^{-e_3}$. (So now $|3|_3 = 1/9$.)

$|x|_{2+i} = 5^{-e_{2+i}}$.

$|x|_{2-i} = 5^{-e_{2-i}}$.

$|x|_7 = 49^{-e_7}$.

$|x|_{11} = 121^{-e_{11}}$.

$|x|_{3+2i} = 13^{-e_{3+2i}}$.

$|x|_{3-2i} = 13^{-e_{3-2i}}$.

Etc. These have product 1.

For $x = 0$, all valuations 0.

$x \mapsto (\log|x|_\infty, \log|x|_{1+i}, \ldots)$
maps the group $\mathbf{Q}(i)^*$ onto
the infinite-dimensional lattice
$(\log 2, -\log 2, 0, 0, 0, \ldots)\mathbf{Z}$ +
$(\log 9, 0, -\log 9, 0, 0, \ldots)\mathbf{Z}$ +
$(\log 5, 0, 0, -\log 5, 0, \ldots)\mathbf{Z}$ +
$(\log 5, 0, 0, 0, -\log 5, \ldots)\mathbf{Z} + \cdots$.

$x \mapsto (\log|x|_\infty, \log|x|_{1+i}, \ldots)$
maps the group $\mathbf{Q}(i)^*$ onto
the infinite-dimensional lattice
$(\log 2, -\log 2, 0, 0, 0, \ldots)\mathbf{Z} +$
$(\log 9, 0, -\log 9, 0, 0, \ldots)\mathbf{Z} +$
$(\log 5, 0, 0, -\log 5, 0, \ldots)\mathbf{Z} +$
$(\log 5, 0, 0, 0, -\log 5, \ldots)\mathbf{Z} + \cdots.$

$S \subseteq \{\infty, 1+i, 3, \ldots\}$, $\infty \in S$:
$x \in \mathbf{Q}(i)^*$ is called an S-**unit**
if $\log|x|_p = 0$ for each $p \notin S$.

$x \mapsto (\log|x|_\infty, \log|x|_{1+i}, \ldots)$
maps the group $\mathbf{Q}(i)^*$ onto
the infinite-dimensional lattice
$(\log 2, -\log 2, 0, 0, 0, \ldots)\mathbf{Z} +$
$(\log 9, 0, -\log 9, 0, 0, \ldots)\mathbf{Z} +$
$(\log 5, 0, 0, -\log 5, 0, \ldots)\mathbf{Z} +$
$(\log 5, 0, 0, 0, -\log 5, \ldots)\mathbf{Z} + \cdots$.

$S \subseteq \{\infty, 1+i, 3, \ldots\}$, $\infty \in S$:
$x \in \mathbf{Q}(i)^*$ is called an S-**unit**
if $\log|x|_p = 0$ for each $p \notin S$.

e.g. $\{\infty\}$-units: $\{1, i, -1, -i\}$.

$x \mapsto (\log|x|_\infty, \log|x|_{1+i}, \ldots)$
maps the group $\mathbf{Q}(i)^*$ onto
the infinite-dimensional lattice
$(\log 2, -\log 2, 0, 0, 0, \ldots)\mathbf{Z} +$
$(\log 9, 0, -\log 9, 0, 0, \ldots)\mathbf{Z} +$
$(\log 5, 0, 0, -\log 5, 0, \ldots)\mathbf{Z} +$
$(\log 5, 0, 0, 0, -\log 5, \ldots)\mathbf{Z} + \cdots.$

$S \subseteq \{\infty, 1+i, 3, \ldots\}$, $\infty \in S$:
$x \in \mathbf{Q}(i)^*$ is called an S-**unit**
if $\log|x|_p = 0$ for each $p \notin S$.

e.g. $\{\infty\}$-units: $\{1, i, -1, -i\}$.

e.g. $\{\infty, 1+i, 2+i\}$-unit lattice:
$(\log 2, -\log 2, 0, 0, 0, \ldots)\mathbf{Z} +$
$(\log 5, 0, 0, -\log 5, 0, \ldots)\mathbf{Z}$.

Variant appearing in literature:
Split $|x|_\infty$ into two copies of $|x|$.
Gives slightly different lattice:

$$(0.5\log 2, 0.5\log 2, -\log 2, 0, 0, 0, \ldots)$$
$$(0.5\log 9, 0.5\log 9, 0, -\log 9, 0, 0, \ldots)$$
$$(0.5\log 5, 0.5\log 5, 0, 0, -\log 5, 0, \ldots)$$
$$(0.5\log 5, 0.5\log 5, 0, 0, 0, -\log 5, \ldots)$$
$$\vdots$$

Minor advantages: e.g., some definitions of the lattice become slightly more concise.

But now have redundant columns, each column deviating from the probability interpretation.

The 8th cyclotomic field

$\zeta_m = \exp(2\pi i/m)$ for $m \in \mathbf{Z}_{\geq 1}$.

e.g. $\zeta_8 = (1+i)/\sqrt{2}$; $\zeta_8^2 = \zeta_4 = i$.

$\mathbf{Q}(\zeta_8) = \mathbf{Q} + \mathbf{Q}\zeta_8 + \mathbf{Q}\zeta_8^2 + \mathbf{Q}\zeta_8^3$.

The 8th cyclotomic field

$\zeta_m = \exp(2\pi i/m)$ for $m \in \mathbf{Z}_{\geq 1}$.
e.g. $\zeta_8 = (1+i)/\sqrt{2}$; $\zeta_8^2 = \zeta_4 = i$.
$\mathbf{Q}(\zeta_8) = \mathbf{Q} + \mathbf{Q}\zeta_8 + \mathbf{Q}\zeta_8^2 + \mathbf{Q}\zeta_8^3$.

Fact: Each $x \in \mathbf{Q}(\zeta_8)^*$
factors uniquely as $r u^{e_u} \prod_{p \in P} p^{e_p}$
where $r \in \{1, \zeta_8, \ldots, \zeta_8^7\}$;
$P = \{1+\zeta_8, 1-\zeta_8-\zeta_8^2, \ldots\}$;
$u = 1+\zeta_8+\zeta_8^2$; $e_u \in \mathbf{Z}$; $e_p \in \mathbf{Z}$.

The 8th cyclotomic field

$\zeta_m = \exp(2\pi i/m)$ for $m \in \mathbf{Z}_{\geq 1}$.
e.g. $\zeta_8 = (1+i)/\sqrt{2}$; $\zeta_8^2 = \zeta_4 = i$.
$\mathbf{Q}(\zeta_8) = \mathbf{Q} + \mathbf{Q}\zeta_8 + \mathbf{Q}\zeta_8^2 + \mathbf{Q}\zeta_8^3$.

Fact: Each $x \in \mathbf{Q}(\zeta_8)^*$
factors uniquely as $r u^{e_u} \prod_{p \in P} p^{e_p}$
where $r \in \{1, \zeta_8, \ldots, \zeta_8^7\}$;
$P = \{1+\zeta_8, 1-\zeta_8-\zeta_8^2, \ldots\}$;
$u = 1+\zeta_8+\zeta_8^2$; $e_u \in \mathbf{Z}$; $e_p \in \mathbf{Z}$.

Why isn't u included in P?
Answer: We'll want to use P to
index various nontrivial valuations.
Exercise: u valuation is trivial.

Standard valuation power ∞_1:

$|x|_{\infty_1} = |x|^2$.

Standard valuation power ∞_1:
$|x|_{\infty_1} = |x|^2$.

Standard valuation power ∞_3:
$|x|_{\infty_3} = |\sigma_3(x)|^2$ where
$\sigma_3(a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3)$
$= a_0 + a_1\zeta_8^3 + a_2\zeta_8^6 + a_3\zeta_8^9$.
Exercise: $\sigma_3(xy) = \sigma_3(x)\sigma_3(y)$.

Standard valuation power ∞_1:
$|x|_{\infty_1} = |x|^2$.

Standard valuation power ∞_3:
$|x|_{\infty_3} = |\sigma_3(x)|^2$ where
$\sigma_3(a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3)$
$= a_0 + a_1\zeta_8^3 + a_2\zeta_8^6 + a_3\zeta_8^9$.
Exercise: $\sigma_3(xy) = \sigma_3(x)\sigma_3(y)$.

To see ∞_1, ∞_3 are inequivalent:
$|1 + \zeta_8|_{\infty_1} = 2 + \sqrt{2} > 1$,
$|1 + \zeta_8|_{\infty_3} = 2/(2 + \sqrt{2}) < 1$.

Standard valuation power ∞_1:
$|x|_{\infty_1} = |x|^2$.

Standard valuation power ∞_3:
$|x|_{\infty_3} = |\sigma_3(x)|^2$ where
$\sigma_3(a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3)$
$= a_0 + a_1\zeta_8^3 + a_2\zeta_8^6 + a_3\zeta_8^9$.
Exercise: $\sigma_3(xy) = \sigma_3(x)\sigma_3(y)$.

To see ∞_1, ∞_3 are inequivalent:
$|1 + \zeta_8|_{\infty_1} = 2 + \sqrt{2} > 1$,
$|1 + \zeta_8|_{\infty_3} = 2/(2 + \sqrt{2}) < 1$.

Standard valuation for $p \in P$:
$|x|_p = N(p)^{-e_p}$, using prime
power $N(p) = |p|_{\infty_1}|p|_{\infty_3}$.

$\{\infty_1, \infty_3\}$-integers:

$\mathbf{Z}[\zeta_8] = \mathbf{Z} + \mathbf{Z}\zeta_8 + \mathbf{Z}\zeta_8^2 + \mathbf{Z}\zeta_8^3$.

$\{\infty_1, \infty_3\}$-integers:
$\mathbf{Z}[\zeta_8] = \mathbf{Z} + \mathbf{Z}\zeta_8 + \mathbf{Z}\zeta_8^2 + \mathbf{Z}\zeta_8^3$.

$\{\infty_1, \infty_3\}$-units: $\zeta_8^{\{0,\ldots,7\}} u^{\mathbf{Z}}$.

$\{\infty_1, \infty_3\}$-integers:
$\mathbf{Z}[\zeta_8] = \mathbf{Z} + \mathbf{Z}\zeta_8 + \mathbf{Z}\zeta_8^2 + \mathbf{Z}\zeta_8^3$.

$\{\infty_1, \infty_3\}$-units: $\zeta_8^{\{0,\dots,7\}} u^{\mathbf{Z}}$.

$\{\infty_1, \infty_3\}$-unit lattice:
$(1.76\dots, -1.76\dots, 0, \dots)\mathbf{Z}$.

$\{\infty_1, \infty_3\}$-integers:
$\mathbf{Z}[\zeta_8] = \mathbf{Z} + \mathbf{Z}\zeta_8 + \mathbf{Z}\zeta_8^2 + \mathbf{Z}\zeta_8^3$.

$\{\infty_1, \infty_3\}$-units: $\zeta_8^{\{0,\ldots,7\}} u^{\mathbf{Z}}$.

$\{\infty_1, \infty_3\}$-unit lattice:
$(1.76\ldots, -1.76\ldots, 0, \ldots)\mathbf{Z}$.

Again increase S for more S-units.

$\{\infty_1, \infty_3, 1 + \zeta_8\}$-units:
$\zeta_8^{\{0,\ldots,7\}} u^{\mathbf{Z}} (1 + \zeta_8)^{\mathbf{Z}}$.

$\{\infty_1, \infty_3\}$-integers:
$\mathbf{Z}[\zeta_8] = \mathbf{Z} + \mathbf{Z}\zeta_8 + \mathbf{Z}\zeta_8^2 + \mathbf{Z}\zeta_8^3$.

$\{\infty_1, \infty_3\}$-units: $\zeta_8^{\{0,\ldots,7\}} u^{\mathbf{Z}}$.

$\{\infty_1, \infty_3\}$-unit lattice:
$(1.76\ldots, -1.76\ldots, 0, \ldots)\mathbf{Z}$.

Again increase S for more S-units.

$\{\infty_1, \infty_3, 1+\zeta_8\}$-units:
$\zeta_8^{\{0,\ldots,7\}} u^{\mathbf{Z}} (1+\zeta_8)^{\mathbf{Z}}$.

$\{\infty_1, \infty_3, 1+\zeta_8\}$-unit lattice:
$(1.76\ldots, -1.76\ldots, 0, \ldots)\mathbf{Z} +$
$(1.22\ldots, -0.53\ldots, -0.69\ldots, \ldots)\mathbf{Z}$.

Reasonably short basis
for the infinite-dimensional
lattice of $\mathbf{Q}(\zeta_8)^*$ logs,
shown truncated after 2 digits:

$$\begin{matrix} 1.76 & -1.76 & 0 & 0 & 0 & \ldots \\ 1.22 & -0.53 & -0.69 & 0 & 0 & \ldots \\ 1.09 & 1.09 & 0 & -2.19 & 0 & \ldots \\ 1.09 & 1.09 & 0 & 0 & -2.19 & \ldots \\ \vdots & & & & & \end{matrix}$$

Reasonably short basis
for the infinite-dimensional
lattice of $\mathbf{Q}(\zeta_8)^*$ logs,
shown truncated after 2 digits:

$$\begin{matrix} 1.76 & -1.76 & 0 & 0 & 0 & \ldots \\ 1.22 & -0.53 & -0.69 & 0 & 0 & \ldots \\ 1.09 & 1.09 & 0 & -2.19 & 0 & \ldots \\ 1.09 & 1.09 & 0 & 0 & -2.19 & \ldots \\ \vdots & & & & & \end{matrix}$$

Diagonal after 2 columns.
Compare to the lattice bases for
$\mathbf{Q}$, $\mathbf{Q}(i)$: diagonal after 1 column.

Reasonably short basis
for the infinite-dimensional
lattice of $\mathbf{Q}(\zeta_8)^*$ logs,
shown truncated after 2 digits:

$$\begin{matrix} 1.76 & -1.76 & 0 & 0 & 0 & \dots \\ 1.22 & -0.53 & -0.69 & 0 & 0 & \dots \\ 1.09 & 1.09 & 0 & -2.19 & 0 & \dots \\ 1.09 & 1.09 & 0 & 0 & -2.19 & \dots \\ \vdots \end{matrix}$$

Diagonal after 2 columns.
Compare to the lattice bases for
$\mathbf{Q}$, $\mathbf{Q}(i)$: diagonal after 1 column.

Exercise: Find shorter basis.

The 16th cyclotomic field

$\zeta_{16} = \exp(2\pi i/16)$ so $\zeta_{16}^8 = -1$.

$$\mathbf{Q}(\zeta_{16}) = \mathbf{Q} + \mathbf{Q}\zeta_{16} + \mathbf{Q}\zeta_{16}^2 + \mathbf{Q}\zeta_{16}^3 + \mathbf{Q}\zeta_{16}^4 + \mathbf{Q}\zeta_{16}^5 + \mathbf{Q}\zeta_{16}^6 + \mathbf{Q}\zeta_{16}^7.$$

The 16th cyclotomic field

$\zeta_{16} = \exp(2\pi i/16)$ so $\zeta_{16}^8 = -1$.

$$\mathbf{Q}(\zeta_{16}) = \mathbf{Q} + \mathbf{Q}\zeta_{16} + \mathbf{Q}\zeta_{16}^2 + \mathbf{Q}\zeta_{16}^3 + \mathbf{Q}\zeta_{16}^4 + \mathbf{Q}\zeta_{16}^5 + \mathbf{Q}\zeta_{16}^6 + \mathbf{Q}\zeta_{16}^7.$$

8th roots of -1 in $\mathbf{C}$:
$\zeta_{16}^{\pm 1}, \zeta_{16}^{\pm 3}, \zeta_{16}^{\pm 5}, \zeta_{16}^{\pm 7}$.

The 16th cyclotomic field

$\zeta_{16} = \exp(2\pi i/16)$ so $\zeta_{16}^8 = -1$.

$$\mathbf{Q}(\zeta_{16}) = \mathbf{Q} + \mathbf{Q}\zeta_{16} + \mathbf{Q}\zeta_{16}^2 + \mathbf{Q}\zeta_{16}^3 + \mathbf{Q}\zeta_{16}^4 + \mathbf{Q}\zeta_{16}^5 + \mathbf{Q}\zeta_{16}^6 + \mathbf{Q}\zeta_{16}^7.$$

8th roots of -1 in $\mathbf{C}$:
$\zeta_{16}^{\pm 1}, \zeta_{16}^{\pm 3}, \zeta_{16}^{\pm 5}, \zeta_{16}^{\pm 7}$.

Each odd integer j has a unique ring morphism $\sigma_j : \mathbf{Q}(\zeta_{16}) \to \mathbf{C}$ mapping ζ_{16} to ζ_{16}^j.

The 16th cyclotomic field

$\zeta_{16} = \exp(2\pi i/16)$ so $\zeta_{16}^8 = -1$.

$$\mathbf{Q}(\zeta_{16}) = \mathbf{Q} + \mathbf{Q}\zeta_{16} + \mathbf{Q}\zeta_{16}^2 + \mathbf{Q}\zeta_{16}^3 + \mathbf{Q}\zeta_{16}^4 + \mathbf{Q}\zeta_{16}^5 + \mathbf{Q}\zeta_{16}^6 + \mathbf{Q}\zeta_{16}^7.$$

8th roots of -1 in $\mathbf{C}$:
$\zeta_{16}^{\pm 1}, \zeta_{16}^{\pm 3}, \zeta_{16}^{\pm 5}, \zeta_{16}^{\pm 7}$.

Each odd integer j has a unique ring morphism $\sigma_j : \mathbf{Q}(\zeta_{16}) \to \mathbf{C}$ mapping ζ_{16} to ζ_{16}^j.

Define $|x|_{\infty_j} = |\sigma_j(x)|^2$.

The 16th cyclotomic field

$\zeta_{16} = \exp(2\pi i/16)$ so $\zeta_{16}^8 = -1$.

$$\mathbf{Q}(\zeta_{16}) = \mathbf{Q} + \mathbf{Q}\zeta_{16} + \mathbf{Q}\zeta_{16}^2 + \mathbf{Q}\zeta_{16}^3 + \mathbf{Q}\zeta_{16}^4 + \mathbf{Q}\zeta_{16}^5 + \mathbf{Q}\zeta_{16}^6 + \mathbf{Q}\zeta_{16}^7.$$

8th roots of -1 in $\mathbf{C}$:
$\zeta_{16}^{\pm 1}, \zeta_{16}^{\pm 3}, \zeta_{16}^{\pm 5}, \zeta_{16}^{\pm 7}$.

Each odd integer j has a unique ring morphism $\sigma_j : \mathbf{Q}(\zeta_{16}) \to \mathbf{C}$ mapping ζ_{16} to ζ_{16}^j.

Define $|x|_{\infty_j} = |\sigma_j(x)|^2$.

Inequivalent: $\infty_1, \infty_3, \infty_5, \infty_7$.

$\{\infty\}$-integers, meaning

$\{\infty_1, \infty_3, \infty_5, \infty_7\}$-integers:

$$\mathbf{Z}[\zeta_{16}] = \mathbf{Z} + \mathbf{Z}\zeta_{16} + \mathbf{Z}\zeta_{16}^2 + \mathbf{Z}\zeta_{16}^3 + \mathbf{Z}\zeta_{16}^4 + \mathbf{Z}\zeta_{16}^5 + \mathbf{Z}\zeta_{16}^6 + \mathbf{Z}\zeta_{16}^7.$$

$\{\infty\}$-integers, meaning
$\{\infty_1, \infty_3, \infty_5, \infty_7\}$-integers:

$$\mathbf{Z}[\zeta_{16}] = \mathbf{Z} + \mathbf{Z}\zeta_{16} + \mathbf{Z}\zeta_{16}^2 + \mathbf{Z}\zeta_{16}^3 + \mathbf{Z}\zeta_{16}^4 + \mathbf{Z}\zeta_{16}^5 + \mathbf{Z}\zeta_{16}^6 + \mathbf{Z}\zeta_{16}^7.$$

$\{\infty\}$-units: $\zeta_{16}^{\mathbf{Z}} u_1^{\mathbf{Z}} u_3^{\mathbf{Z}} u_5^{\mathbf{Z}}$ where

$u_1 = 1 + \zeta_{16} + \zeta_{16}^2$,
$u_3 = 1 + \zeta_{16}^3 + \zeta_{16}^6 = \sigma_3(u_1)$,
$u_5 = 1 + \zeta_{16}^5 + \zeta_{16}^{10} = \sigma_5(u_1)$.

$\{\infty\}$-integers, meaning $\{\infty_1, \infty_3, \infty_5, \infty_7\}$-integers:

$$\mathbf{Z}[\zeta_{16}] = \mathbf{Z} + \mathbf{Z}\zeta_{16} + \mathbf{Z}\zeta_{16}^2 + \mathbf{Z}\zeta_{16}^3 + \mathbf{Z}\zeta_{16}^4 + \mathbf{Z}\zeta_{16}^5 + \mathbf{Z}\zeta_{16}^6 + \mathbf{Z}\zeta_{16}^7.$$

$\{\infty\}$-units: $\zeta_{16}^{\mathbf{Z}} u_1^{\mathbf{Z}} u_3^{\mathbf{Z}} u_5^{\mathbf{Z}}$ where

$u_1 = 1 + \zeta_{16} + \zeta_{16}^2$,

$u_3 = 1 + \zeta_{16}^3 + \zeta_{16}^6 = \sigma_3(u_1)$,

$u_5 = 1 + \zeta_{16}^5 + \zeta_{16}^{10} = \sigma_5(u_1)$.

Exercise: $u_1 u_3 u_5 u_7 = -1$ where

$u_7 = 1 + \zeta_{16}^7 + \zeta_{16}^{14} = \sigma_7(u_1)$.

$\{\infty\}$-integers, meaning $\{\infty_1, \infty_3, \infty_5, \infty_7\}$-integers:

$$\mathbf{Z}[\zeta_{16}] = \mathbf{Z} + \mathbf{Z}\zeta_{16} + \mathbf{Z}\zeta_{16}^2 + \mathbf{Z}\zeta_{16}^3 + \mathbf{Z}\zeta_{16}^4 + \mathbf{Z}\zeta_{16}^5 + \mathbf{Z}\zeta_{16}^6 + \mathbf{Z}\zeta_{16}^7.$$

$\{\infty\}$-units: $\zeta_{16}^{\mathbf{Z}} u_1^{\mathbf{Z}} u_3^{\mathbf{Z}} u_5^{\mathbf{Z}}$ where

$u_1 = 1 + \zeta_{16} + \zeta_{16}^2$,

$u_3 = 1 + \zeta_{16}^3 + \zeta_{16}^6 = \sigma_3(u_1)$,

$u_5 = 1 + \zeta_{16}^5 + \zeta_{16}^{10} = \sigma_5(u_1)$.

Exercise: $u_1 u_3 u_5 u_7 = -1$ where $u_7 = 1 + \zeta_{16}^7 + \zeta_{16}^{14} = \sigma_7(u_1)$.

Logs of u_1, u_3, u_5, truncated:

2.09	1.13	−2.89	−0.33
1.13	−0.33	2.09	−2.89
−2.89	2.09	−0.33	1.13

In the infinite-dimensional lattice of $\mathbf{Q}(\zeta_{16})^*$ logs, a diagonal starts after the four ∞ columns:

$$\begin{array}{rrrrrr}
2.09 & 1.13 & -2.89 & -0.33 & 0 & 0 \\
1.13 & -0.33 & 2.09 & -2.89 & 0 & 0 \\
-2.89 & 2.09 & -0.33 & 1.13 & 0 & 0 \\
1.34 & 1.01 & 0.21 & -1.88 & -0.69 & 0 \\
1.94 & -0.68 & 0.98 & 0.58 & 0 & -2.8 \\
\vdots & & & & &
\end{array}$$

In the infinite-dimensional lattice of $\mathbf{Q}(\zeta_{16})^*$ logs, a diagonal starts after the four ∞ columns:

$$\begin{matrix} 2.09 & 1.13 & -2.89 & -0.33 & 0 & 0 \\ 1.13 & -0.33 & 2.09 & -2.89 & 0 & 0 \\ -2.89 & 2.09 & -0.33 & 1.13 & 0 & 0 \\ 1.34 & 1.01 & 0.21 & -1.88 & -0.69 & 0 \\ 1.94 & -0.68 & 0.98 & 0.58 & 0 & -2.8 \\ \vdots \end{matrix}$$

The general picture: Number of ∞ columns is between $n/2$ and n for a degree-n number field, and a diagonal appears almost immediately after the ∞ columns.