Reminder: Fix a prime number p. The ring of *p-adic integers* is the subring

$$\mathbb{Z}/p^k\mathbb{Z} \Uparrow \mathbb{Z}/p^{k+1}\mathbb{Z} \Uparrow \vdots$$

$$\boxed{\mathbb{Z}_p := \underbrace{\left\{ (x_k + p^k\mathbb{Z})_k \in \bigtimes_{k\geqslant 0} (\mathbb{Z}/p^k\mathbb{Z}) \;\middle|\; \forall k \geqslant 0 \colon x_k \equiv x_{k+1} \bmod (p^k) \right\}}_{=: \varprojlim_k \mathbb{Z}/p^k\mathbb{Z}}.}$$

The following map is bijective:

$$\boxed{\bigtimes_{k\geqslant 0} \{0, 1, \ldots, p-1\} \longrightarrow \mathbb{Z}_p, \quad (a_i)_i \longmapsto \left(\sum_{i=0}^{k-1} a_i p^i + p^k\mathbb{Z} \right)_k.} = \sum_{i\geq 0} a_i p^i$$

Proposition 8.1.10: (a) The set of units of $\mathbb{Z}_p$ is $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus p\mathbb{Z}_p$.

(b) The ideal (p) of $\mathbb{Z}_p$ is the unique maximal ideal.

(c) Every non-zero ideal of $\mathbb{Z}_p$ is generated by p^r for a unique integer $r \geqslant 0$.

(d) The ring $\mathbb{Z}_p$ is a principal ideal domain.

$$1+2+4+8+\ldots = \sum_{i\geq 0} 2^i \in \mathbb{Z}_2$$

$$(1-2)\cdot \sum_{i\geq 0} 2^i \overset{?}{=} \sum_{i\geq 0} 2^i - \sum_{i\geq 0} 2^{i+1} = \sum_{i\geq 0} 2^i - \sum_{i\geq 1} 2^i = 1$$

$$\Rightarrow \sum_{i\geq 0} 2^i = -1.$$

$p=11$

$$\begin{array}{r} \ldots 00.1172 \\ \ldots 110.1311 \\ \hline \ldots 10.2483 \end{array}$$

Definition 8.1.11: The ring of formal Laurent series with finite principal part

$$\mathbb{Q}_p := \left\{ \sum_{i\in\mathbb{Z}} a_i p^i \;\middle|\; \begin{array}{l} \text{all } a_i \in \{0,1,\ldots,p-1\} \\ \text{and } a_i = 0 \text{ for all } i \ll 0 \end{array} \right\}$$

with the addition and multiplication defined as above. The elements of $\mathbb{Q}_p$ are called *(rational) p-adic numbers.*

Proposition 8.1.12: We have $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}] = \mathrm{Quot}(\mathbb{Z}_p)$.

Proof: $\mathbb{Q}_p = \bigcup_{n\geq 0} \frac{1}{p^n}\cdot\mathbb{Z}_p$ with $\frac{1}{p^n}\mathbb{Z}_p = \left\{ \sum_{i\geq -n} a_i p^i \;\middle|\; \text{all } a_i \in \{0,\ldots,p-1\} \right\}$.

$\Rightarrow \mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$.

$\mathbb{Q}_p$ is a field: To show $\forall x \in \mathbb{Q}_p \setminus \{0\} : \exists y \in \mathbb{Q}_p : xy = 1$.

$x = \sum_{i\geq d} a_i p^i$ with $a_d \neq 0$.

$\Rightarrow x = p^d \cdot u$ for $u = \sum_{i\geq 0} a_{i+d} p^i$

Now $u \in \mathbb{Z}_p^\times$.

$\Rightarrow y = p^{-d}\cdot u^{-1}$ ✓. qed.

Remark 8.1.13: Again the digits of a rational p-adic number are uniquely determined, and one computes with them by hand in the same way as with real numbers by writing them with a decimal point as $\ldots a_2 a_1 a_0 . a_{-1} \ldots a_k$ for some $k \ll 0$.

Remark 8.1.14: We have $\mathrm{card}(\mathbb{Q}_p) = \mathrm{card}(\mathbb{Z}_p) = \mathrm{card}(\mathbb{R})$.

$|\mathbb{Z}_p| = p^\omega = |\mathbb{R}|$.

$|\mathbb{Z}_p| \leq |\mathbb{Q}_p| \leq \sum_{n\geq 0} |\frac{1}{p^n}\mathbb{Z}_p| = \omega \cdot p^\omega = p^\omega$.

Proposition 8.1.15: We have

(a) $\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mathbb{Z}_p^\times$. ✓ ← as above.

(b) $\mu(\mathbb{Q}_p) = \begin{cases} \mu_{p-1} & \text{if } p > 2, \\ \mu_2 & \text{if } p = 2. \end{cases}$ ✓ ✓

(c) $\mathbb{Z}_p^\times = \begin{cases} \mu_{p-1} \times (1 + p\mathbb{Z}_p) & \text{if } p > 2, \\ \mu_2 \times (1 + 4\mathbb{Z}_2) & \text{if } p = 2. \end{cases}$ ✓ ✓

(d) The second factor in (c) is isomorphic to $\mathbb{Z}_p$.

$\mu(\mathbb{Q}_p) = \{u \in \mathbb{Z}_p^\times \mid \exists n \geq 1 : u^n = 1\}$.

$(\mathbb{Z}/p^k\mathbb{Z})^\times$? for $k \geq 1$.

$(\mathbb{Z}/p^k\mathbb{Z})^\times$ abelian group of order $(p-1)p^{k-1}$

$$0 \to \underbrace{\frac{1+p\mathbb{Z}}{p^k\mathbb{Z}}}_{\text{order } p^{k-1}} \to \underbrace{(\mathbb{Z}/p^k\mathbb{Z})^\times} \to \underbrace{\mathbb{F}_p^\times}_{\substack{\text{order } p-1 \\ \text{cyclic.}}} \to 0$$

$$\Rightarrow (\mathbb{Z}/p^k\mathbb{Z})^\times = \frac{1+p\mathbb{Z}}{p^k\mathbb{Z}} \times G_k$$

$$(\mathbb{Z}/p^{k+1}\mathbb{Z})^\times = \frac{1+p\mathbb{Z}}{p^{k+1}\mathbb{Z}} \times G_{k+1}$$

cyclic of order $p-1$.

$\Rightarrow \mathbb{Z}_p^\times = (1+p\mathbb{Z}_p, \cdot) \times \mu_{p-1}$.

Choose generators ξ_k of $\frac{1+p\mathbb{Z}}{p^k\mathbb{Z}}$ with $\xi_{k+1} \mapsto \xi_k$,

$\rightsquigarrow$ iso. $\mathbb{Z}_p \xrightarrow{\sim} 1 + p\mathbb{Z}_p$

$(a_k + p^k\mathbb{Z}) \mapsto (\xi_k^{a_k})_{k \geq 0}$.

Claim: p odd $\Rightarrow [1+p]$ generates $\frac{1+p\mathbb{Z}}{p^k\mathbb{Z}}$.

Proof: $[1+ap] \in \mathbb{Z}/p^k\mathbb{Z}$, $a \in \mathbb{Z}$; $k \geq 3$

$$[1+ap]^p = \left[\sum_{i=0}^{p} \binom{p}{i} a^i p^i\right] = \left[1 + ap^2 + \sum_{i \geq 2} \cdots\right]$$

$i \geq 2 \Rightarrow p^3 \mid \binom{p}{i} \cdot p^i$ because $p > 2$.

$= \left[1 + ap^2 \cdot (1 + \text{something divisible by } p)\right]$

$= [1]$ iff $p^k \mid ap^2 \Leftrightarrow p^{k-1} \mid ap$.

$\Rightarrow \{\xi \in (\mathbb{Z}/p^k\mathbb{Z})^\times \mid \xi^p = 1\}$ has order p.

Use elementary divisor theory. qed

Similarly: $(1+4\mathbb{Z}_2, \cdot) \cong \mathbb{Z}_2$.

$$(1+2a)^2 = 1+4a+4a^2$$

$$(1+4a)^2 = 1+8a+16a^2 = 1+8a(\underline{\underline{1+2a}})$$

$$(\mathbb{Z}/2^k\mathbb{Z})^\times = \{\pm 1\} \times \frac{1+4\mathbb{Z}}{2^k\mathbb{Z}} \quad k \geq 2$$

8.2 Valuations

Definition 8.2.1: A *(non-trivial rank 1) valuation* on a field K is a map

$$K \to \mathbb{R} \cup \{\infty\}, \quad x \mapsto v(x)$$

with the properties

(a) For any $x \in K$ we have $v(x) = \infty$ if and only if $x = 0$.

(b) For any $x, y \in K$ we have $v(xy) = v(x) + v(y)$. ⟵ $v: K^\times \longrightarrow \mathbb{R}$ homo

(c) For any $x, y \in K$ we have $v(x + y) \geqslant \min\{v(x), v(y)\}$.

(d) There exists $x \in K$ with $v(x) \notin \{0, \infty\}$.

Remark 8.2.2: The map with $v(0) = \overset{\infty}{\cancel{0}}$ and $v(x) = 0$ for all $x \neq 0$ is called the *trivial valuation*. Some of the results below also hold for it, and sometimes one allows it as well, but we exclude it without further mention.

subgroup.

complete by (d)

Definition 8.2.3: (a) A valuation v is called *discrete* if $v(K^\times)$ is discrete in $\mathbb{R}$. $\Rightarrow$ lattice $\Rightarrow$ $v(K^\times) = \mathbb{Z}\cdot\xi$ for $\xi > 0$.

$\Downarrow$

(b) A discrete valuation v is called *normalized* if $v(K^\times) = \mathbb{Z}$.

(c) Two valuations v and v' are called *equivalent* if $v' = c \cdot v$ for some constant $c > 0$. $\Rightarrow$ $v'(K^\times) = \mathbb{Z}\cdot c\xi$.

Proposition 8.2.4: Every discrete valuation is equivalent to a unique normalized valuation.

↑ Take $c = \xi^{-1}$.

Proposition 8.2.5: Let A be a Dedekind ring with quotient field K, and let $\mathfrak{p}$ be a maximal ideal of A. For any $x \in K^\times$ let $\mathrm{ord}_\mathfrak{p}(x)$ denote the exponent of $\mathfrak{p}$ in the prime factorization of the fractional ideal (x), and set $\mathrm{ord}_\mathfrak{p}(0) := \infty$. Then $\mathrm{ord}_\mathfrak{p}$ is a normalized discrete valuation on K.

Proof: (a) ✓

(b) $\mathrm{ord}_\mathfrak{p}(xy) = \mathrm{ord}_\mathfrak{p}(x) + \mathrm{ord}_\mathfrak{p}(y)$ ✓

(c) $\mathrm{ord}_\mathfrak{p}(x+y) \geq \min\{\mathrm{ord}_\mathfrak{p}(x), \mathrm{ord}_\mathfrak{p}(y)\}$.

(d) For any $x \in \mathfrak{p} \setminus \mathfrak{p}^2$ we have $\mathrm{ord}_\mathfrak{p}(x) = 1$

$(x) = \prod \mathfrak{q}^{r_\mathfrak{q}}$, $(y) = \prod \mathfrak{q}^{s_\mathfrak{q}}$ $\Rightarrow (xy) = \prod \mathfrak{q}^{r_\mathfrak{q}+s_\mathfrak{q}}$

$(x+y) \subset (x,y) = \prod \mathfrak{q}^{\min\{r_\mathfrak{q}, s_\mathfrak{q}\}}$.

for $x, y \in A$ by gcd.

Generalize to $x, y \in K^\times$ by dividing by $z \in A^\times$.

gcd

Examples 8.2.6: Consider a field k and a prime p.

(a) The polynomial ring $A = k[t]$ with $K = k(t)$ and $\mathfrak{p} = (t-a)$ for some $a \in A$.

(b) The field $K = k(t)$ with $v(f/g) := \deg(g) - \deg(f)$ for any $f, g \in k[t] \setminus \{0\}$.

Exercise.

(c) The power series ring $A = k[[t]]$ with $K = k((t))$ and $\mathfrak{p} = (t)$.

(d) The ring $A = \mathbb{Z}$ with $K = \mathbb{Q}$ and $\mathfrak{p} = (p)$.

(e) The ring $A = \mathbb{Z}_p$ with $K = \mathbb{Q}_p$ and $\mathfrak{p} = (p)$.

$A' := k[\frac{1}{t}] \Rightarrow \mathrm{Quot}(A') = k(t)$

$\mathfrak{p}' = (\frac{1}{t}) \Rightarrow \boxed{\mathrm{ord}_{\mathfrak{p}'} = v}$ in (b)

Basic Properties 8.2.7: For any valuation v on K we have:

(a) For any $x \in K^\times$ and $n \in \mathbb{Z}$ we have $v(x^n) = n \cdot v(x)$.

(b) For any root of unity $\zeta \in K$ we have $v(\zeta) = 0$.

(c) For any $x \in K$ and $n \in \mathbb{Z}$ we have $v(nx) \geq v(x)$.

(d) For any $x, y \in K$ we have $v(x+y) = \min\{v(x), v(y)\}$ if $v(x) \neq v(y)$.

$\zeta^n = 1,\ n \geq 1 \Rightarrow n \cdot v(\zeta) = v(\zeta^n)$
$= v(1) = 0$
$\Rightarrow v(\zeta) = 0.$

In particular $v(-1) = 0$
$\Rightarrow v(-x) = v(-1) + v(x)$
$= v(x).$

$n \geq 1$: induction on n:
$v((n+1)x) = v(nx + x) \geq \min\{v(nx), v(x)\} \geq v(x)$

$n = 0$: $v(0) = \infty \geq v(x)$

$n < 0$: $v(nx) = v(-nx)$ ✓

Suppose $v(x+y) > \min\{v(x), v(y)\}$

$\Rightarrow v(y) = v((x+y) + (-x))$
$\geq \min\{v(x+y), v(-x)\}$
$= \min\{v(x+y), v(x)\}$
$= v(x)$

$\Rightarrow v(y) \geq v(x)$
Similarly $v(x) \geq v(y)$. $\Big] \Rightarrow v(x) = v(y)$

qed

Proposition-Definition 8.2.8: For any valuation v on K we have:

(a) The subset $\mathcal{O}_v := \{x \in K : \boxed{v(x) \geqslant 0}\}$ is a subring, called the *valuation ring* associated to v.

(b) We have $\mathrm{Quot}(\mathcal{O}_v) = K$.

(c) We have $\mathcal{O}_v^\times := \{x \in K : v(x) = 0\}$.

(d) The subset $\mathfrak{m}_v := \{x \in K : v(x) > 0\}$ is the unique maximal ideal of $\mathcal{O}_v$.

(e) If the valuation is discrete, then $\mathcal{O}_v$ is a principal ideal domain.

Proof:

(a) $\mathcal{O}_v \ni 0, 1$, closed under $+, \cdot$.

(b) $\forall x \in K^\times$: $v(x) \geq 0 \Rightarrow x \in \mathcal{O}_v$ ✓

$v(x) < 0 \Rightarrow v\left(\frac{1}{x}\right) > 0 \Rightarrow \frac{1}{x} \in \mathcal{O}_v \Rightarrow x \in \mathrm{Quot}(\mathcal{O}_v)$.

(c) $x \in \mathcal{O}_v^\times \Leftrightarrow \left[v(x) \geq 0 \wedge \underbrace{v\left(\tfrac{1}{x}\right) \geq 0}_{\Updownarrow\ v(x) \leq 0} \right] \Leftrightarrow v(x) = 0$.

(d) $\mathfrak{m}_v$ is an ideal.

$\mathcal{O}_v \setminus \mathfrak{m}_v = \mathcal{O}_v^\times \Rightarrow$ maximal.

$\mathfrak{m}' \subset \mathcal{O}_v$ any max. ideal $\Rightarrow \mathfrak{m}' \cap \mathcal{O}_v^\times = \emptyset \Rightarrow \mathfrak{m}' \subset \mathfrak{m}_v \Rightarrow \mathfrak{m}' = \mathfrak{m}_v$.

(e) WLOG v normalized. Pick $\pi \in K$ with $v(\pi) = 1$.

$K^\times = \pi^{\mathbb{Z}} \times \mathcal{O}_v^\times$. $\Rightarrow$ any nonzero ideal of $\mathcal{O}_v$ is (π^n) for unique $n \geq 0$.

q.e.d.