8 Theory of valuations

8.1 *p*-adic Numbers

Motivation:

Kronecker: "The natural numbers were given by God, but everything else is an invention of mankind."

Goethe: "Mathematicians are like Frenchmen: whatever you say to them they translate into their own language and forthwith it is something entirely different."

Claim: $1+2+4+\ldots = \sum_{n\geq 0} 2^n$

$$\underbrace{(1-2)}_{-1}\cdot \sum_{n\geq 0} 2^n = \sum_{n\geq 0} (2^n - 2^{n+1}) = \sum_{n\geq 0} 2^n - \sum_{n\geq 0} 2^{n+1}$$

$$= \sum_{n\geq 0} 2^n - \sum_{n\geq 1} 2^n = 1$$

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

$$
\begin{array}{r}
\ldots 7752 \\
+\ \ldots 3813 \\
\hline
\ldots 1565
\end{array}
$$

$$
\begin{array}{r}
\ldots 0000 \\
-\qquad 1 \\
\hline
\ldots 9999
\end{array}
$$

$\mathbb{Z}/10^n\mathbb{Z}$.

Fix an integer $b \geqslant 2$.

Fact 8.1.1: Any integer $n \geqslant 0$ can be written uniquely to base b as a finite sum

$$n = \sum_{i \geqslant 0}{}' a_i b^i \qquad \text{with} \quad a_i \in \{0, 1, \ldots, b-1\}.$$

Here the last k digits determine $n \bmod (b^k)$, and the last k digits of the sum or product of two integers $m, n \geqslant 0$ depend only on the last k digits of m and n.

Proposition 8.1.2: There is a natural injective ring homomorphism

$$\mathbb{Z} \hookrightarrow \bigtimes_{k \geqslant 0} (\mathbb{Z}/b^k\mathbb{Z}), \quad n \longmapsto (n + b^k\mathbb{Z})_k.$$

Proof: ring homo ✓

inj.: If $n \mapsto 0$ then $\forall k$: $b^k \mid n \Rightarrow n = 0$. qed.

Proposition 8.1.3: The image of this map is contained in the subring

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

$\mathbb{Z}/b^{k+1}\mathbb{Z} \longrightarrow \mathbb{Z}/b^k\mathbb{Z}$ is a ring homo.

$x + b^{k+1}\mathbb{Z} \longmapsto x + b^k\mathbb{Z}$

$$\sum_{i\geq 0} a_i b^i + (b^k)$$

Proposition 8.1.4: The following map is bijective:

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

Proof: $a_0, \ldots, a_{k-1}$ determine and are determined by the image in $\mathbb{Z}/b^k\mathbb{Z}$.

$\Rightarrow$ injective.

bijective

$$\{0,\ldots,b-1\}^{\{0,\ldots,k-1\}} \xrightarrow{\sim} \mathbb{Z}/b^k\mathbb{Z} \ni x_k + b^k\mathbb{Z}$$

$$\{0,\ldots,b-1\}^{\{0,\ldots,k\}} \xrightarrow{\sim} \mathbb{Z}/b^{k+1}\mathbb{Z} \ni x_{k+1} + b^{k+1}\mathbb{Z}$$

qed.

Observation 8.1.5: One computes with these systems (a_i) by hand in the same way as with non-negative integers to base b, except that the sequence of digits $\ldots a_2 a_1 a_0$ extends infinitely to the left. This is similar to the decimal expansion of a real number, but in this case the sequence of digits is unique.

Convention 8.1.6: One writes an element in the image of the above map as a formal power series

$$\boxed{\sum_{i \geqslant 0} a_i b^i.}$$

One computes with such expressions in the same way as with formal power series, except that one has to deal with the carry.

Proposition 8.1.7: (a) For any coprime integers $b, b' \geqslant 2$ there is a natural ring isomorphism

$$\mathbb{Z}_{bb'} \cong \mathbb{Z}_b \times \mathbb{Z}_{b'}.$$

(b) For any integer $r \geqslant 0$ there is a natural ring isomorphism

$$\mathbb{Z}_{b^r} \cong \mathbb{Z}_b.$$

Example:

$$\mathbb{Z}_{10} \cong \underset{1}{\underset{\cup}{\mathbb{Z}_2}} \times \underset{0}{\underset{\cup}{\mathbb{Z}_5}}.$$

$\rightsquigarrow$ reduces to b = prime.

Proof: (a)

$$\begin{tikzcd}
\vdots & \mathbb{Z}/(bb')^k\mathbb{Z} \arrow[r, "\sim"] \arrow[d, phantom, "\vdots"] & \mathbb{Z}/b^k\mathbb{Z} \times \mathbb{Z}/b'^k\mathbb{Z} & (\cdot\,,\,\cdot) \\
\vdots \arrow[u] & \mathbb{Z}/(bb')^{k+1}\mathbb{Z} \arrow[u, two heads] \arrow[r, "\sim"] \arrow[ur, phantom, "///"] & \mathbb{Z}/b^{k+1}\mathbb{Z} \times \mathbb{Z}/b'^{k+1}\mathbb{Z} \arrow[u, two heads] & (\cdot\,,\,\cdot) \arrow[u, mapsto]
\end{tikzcd}$$

(b)

$$\underbrace{\mathbb{Z}/(b^r)^k\mathbb{Z}} = \underbrace{\mathbb{Z}/b^{rk}\mathbb{Z}}$$

$5^{2^n} \bmod 10^k \rightsquigarrow 5^{2^n} \bmod 5^k$ goes to 0.

$5^{2^n} \bmod 2^k$

Fix $k \geq 1 \rightsquigarrow (\mathbb{Z}/2^k\mathbb{Z})^\times$ is a group of order $2^{k-1} \Rightarrow$ Every element has order dividing 2^{k-1}

$\Rightarrow 5^{2^n} \bmod (2^k) = \bar{1}$ for all $n \geq k-1$. Thus $5^{2^n} \to 1$ in $\mathbb{Z}_2$.

qed.

Throughout the following we therefore assume that $b = p$ is a prime number.

Definition 8.1.8: The elements of $\mathbb{Z}_p$ are called $\boxed{\textit{p-adic integers.}}$

Proposition 8.1.9: A system of polynomials $f_1, \dots, f_r \in \mathbb{Z}_p[X_1, \dots, X_m]$ has a common solution in $(\mathbb{Z}_p)^m$ if and only if their residue classes modulo (p^k) have a common solution in $(\mathbb{Z}/p^k\mathbb{Z})^m$ for all $k \geqslant 0$.

Proof: "$\Rightarrow$" ✓

"$\Leftarrow$" Let $S_k := \{ (\bar{x}_1, \dots, \bar{x}_m) \in \underbrace{(\mathbb{Z}/p^k\mathbb{Z})^m}_{\text{finite}} \mid \forall i : f_i(\bar{x}_1, \dots, \bar{x}_m) = 0 \text{ in } \mathbb{Z}/p^k\mathbb{Z} \}$.

Assume $\forall$: $S_k \neq \emptyset$.

$\forall k' \geq k$: Map : $S_{k'} \xrightarrow{\pi_k^{k'}} S_k$, $(\bar{x}_1, \dots, \bar{x}_m) \mapsto (\bar{x}_1 \bmod p^k, \dots,)$

Each S_k is finite.

For any k consider the subsets $\underbrace{S_k}_{\text{finite}} \supset \underbrace{\pi_k^{k+1}(S_{k+1})} \supset \underbrace{\pi_k^{k+2}(S_{k+2})}_{\text{nonempty}} \supset \dots$

$\Rightarrow T_k := \bigcap_{k' \geq k} \pi_k^{k'}(S_{k'})$ nonempty.

$S_{k+1} \supset \pi_k^{k+1}(S_{k+2}) \supset \dots$

$\pi_k^{k+1}(T_{k+1}) = T_k$

$t_k = (x_{1,k} + p^k\mathbb{Z}, \dots, x_{m,k} + p^k\mathbb{Z})$

Choose $t_k \in T_k$ and then $\pi_k^{k+1}(t_{k+1}) = t_k$. Now $\forall i$ $\underline{x}_i := (x_{i,k} + p^k\mathbb{Z})_{k \geq 0} \in \mathbb{Z}_p$.

$\forall j : f_j(\underline{x}_1, \dots, \underline{x}_m) = 0$

qed.

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

(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.

Proof: (a) $\underline{x} = \text{“}\sum_{i\geq 0} x_i p^i\text{”} \Rightarrow p\underline{x} = \text{“}\sum_{i\geq 0} x_i p^{i+1}\text{”} = \text{“}\sum_{i\geq 1} x_{i-1} p^i\text{”}$

$\Rightarrow p\mathbb{Z}_p = \{\text{“}\sum x_i p^i\text{”} \mid x_0 = 0\}$.

$\forall\, \underline{x} \in \mathbb{Z}_p^\times \Rightarrow$ its image in $\mathbb{Z}/p^k\mathbb{Z}$ is a unit for all $k \Rightarrow \underline{x} \notin p\mathbb{Z}_p$.

Take $\underline{x} = \text{“}\sum x_i p^i\text{”}$ with $x_0 \neq 0 \Rightarrow \forall k \geq 0: \sum_{i=0}^{k-1} x_i p^i + p^k\mathbb{Z} \in (\mathbb{Z}/p^k\mathbb{Z})^\times$.

i.e. the equation $\underline{x}\cdot Y - 1 = 0$ has a solution in $\mathbb{Z}/p^k\mathbb{Z}$ for all k.

$\Rightarrow$ it has a solution in $\mathbb{Z}_p$.

(b) $\mathbb{Z}_p/p\mathbb{Z}_p \xleftarrow{\sim} \{0, \dots, p-1\}$
$\quad \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ = field.
$\Rightarrow p\mathbb{Z}_p$ max. ideal.

$\mathfrak{m} \subset \mathbb{Z}_p$ max. ideal $\Rightarrow \mathfrak{m} \cap \mathbb{Z}_p^\times = \emptyset \overset{(a)}{\Rightarrow} \mathfrak{m} \subset p\mathbb{Z}_p = $ max.

$\Rightarrow \mathfrak{m} = p\mathbb{Z}_p$.

(c) For any nonzero ideal $\mathfrak{a} \subset \mathbb{Z}_p$ take $\mathfrak{a} \ni \underset{\neq 0}{\underline{x}} = $ "$\sum_{i \geq 0} x_i p^i$" with $j := \min\{i \geq 0 \mid x_i \neq 0\}$ minimal.

Then $\underline{u} :=$ "$\sum_{i \geq 0} x_{i+j} p^i$" $\in \mathbb{Z}_p^\times$.

and $\underline{x} = p^j \cdot \underline{u} \in \mathfrak{a} \Rightarrow p^j \in \mathfrak{a}$.

By the choice of j we have $\mathfrak{a} \subset p^j \mathbb{Z}_p$ $\Big] \Rightarrow \mathfrak{a} = p^j \mathbb{Z}_p$.

(d) $\mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/p^k\mathbb{Z}$ for $k > 0 \Rightarrow 1 \neq 0$ in $\mathbb{Z}_p$.

$\underline{x}, \underline{y} \in \mathbb{Z}_p \setminus \{0\} \Rightarrow$ $\underline{x} = p^j \cdot \underline{u}$, $\underline{y} = p^k \cdot \underline{v}$ for $j, k \geq 0$, $\underline{u}, \underline{v} \in \mathbb{Z}_p^\times$

$\Rightarrow \underline{x}\,\underline{y} = \underbrace{p^{j+k}}_{\neq 0} \cdot \underbrace{\underline{u} \cdot \underline{v}}_{\in \mathbb{Z}_p^\times}$

because it is non-zero mod $p^{j+k+1}\mathbb{Z}$,