汕頭大學
SHANTOU UNIVERSITY

本科毕业论文（设计）

题　目：Witt 向量简介

学　　院：理学院

系　　别：数学系

专业年级：2017 级数学与应用数学

学生姓名：吴　彬

学　　号：2017061033

指导教师：陈　哲

完成时间：2021 年 5 月

汕头大学本科生毕业论文（设计）诚信承诺书

本人承诺呈交的毕业论文（设计）《Witt 向量简介》是在指导教师的指导下，独立开展研究取得的成果，文中引用他人的观点和材料，均在文后按顺序列出其参考文献，论文（设计）使用的数据真实可靠。

本人签名：吴　彬

日　　期：2021 年 5 月

Witt 向量简介

摘要

本文研究了整数环 $\mathbb{Z}$ 关于赋值结构的完备化结果在环同构意义下的另一种代数表示. 我们先介绍环上的赋值概念, 然后引入赋值等价这个二元关系, 并在 Ostrowski 定理的帮助下将 $\mathbb{Z}$ 上赋值的研究范围缩小到三种典型结构. 在指出 $\mathbb{Z}$ 只关于其中的 p-进赋值不完备之后, 我们对其完备化得到一个精简的结果: $\mathbb{Z}_p$. 之后我们研究了其剩余域 $\mathbb{F}_p$ 上的一种特殊环结构: Witt 环 $\mathcal{W}(\mathbb{F}_p)$, 并借助 Teichmüller 提升 τ_e 实现了 $\mathcal{W}(\mathbb{F}_p)$ 与 $\mathbb{Z}_p$ 的环同构.

关键词: Witt **向量** Teichmüller **提升** Ostrowski **定理** p-**进赋值**

An introduction to Witt vectors

Abstract

This paper studies an isomorphic representation of the completion of integer ring $\mathbb{Z}$ under the structure of valuation. First we introduce the concept of valuation and equivalence between valuations as a binary relation. With the help of Ostrowski Theorem we narrow down the range of valuations on $\mathbb{Z}$ to three classic types. Then we point out that $\mathbb{Z}$ only is not completed under p-adic valuation, after which we complete it and have a simple result: $\mathbb{Z}_p$. Then on its residue field $\mathbb{F}_p$ we study a special ring: Witt ring $\mathcal{W}(\mathbb{F}_p)$. Finally we successfully use Teichmüller lift τ_e to build isomorphism between $\mathcal{W}(\mathbb{F}_p)$ and $\mathbb{Z}_p$.

Key Words: Witt vectors Teichmüller lift Ostrowski Theorem p-adic valuation

目录

前言

在进入正文前, 首先声明该文除去一些关键的思路和证明, 也存在一部分**完全由本人给出的证明过程或例子**, 涉及但不限于以下内容:

§ 1.1 命题 1.1.2, 推论 1.1.7, 命题 1.1.9.

§ 1.2 命题 1.2.4, 命题 1.2.5, 命题 1.2.6, 命题 1.2.7, 命题 1.2.8, 命题 1.2.9, 引理 1.2.10, 引理 1.2.11, 推论 1.2.14.

§ 1.3 例子 1.3.2, 例子 1.3.3, 命题 1.3.5, 例子 1.3.6, 例子 1.3.7, 例子 1.3.8, 例子 1.3.9, 命题 1.3.11, 命题 1.3.12, 命题 1.3.13, 定理 1.3.15.

§ 2.1 命题 2.1.1, 推论 2.1.2, 定理 2.1.3.

§ 2.2 命题 2.2.1, 命题 2.2.3, 命题 2.2.5, 命题 2.2.10, 推论 2.2.11, 例子 2.2.13, 例子 2.2.14.

§ 3.1 命题 3.1.4, 命题 3.1.8, 命题 3.1.11

§ 3.2 命题 3.2.1, 命题 3.2.2, § 3.2.1 中除去引理 3.2.1.11 的剩余部分, 引理 3.2.2.6, 推论 3.2.2.7, § 3.2.3 全部的证明过程.

§ 3.3 命题 3.3.1.3, 定理 3.3.1.4.

注意虽然上面的内容的证明或例子完全由本人提供, 但是这些命题, 定理, 例子的提出也有部分是来源于或者启发于文后所录的一些参考文献. 包括关键思路和定理的提供和证明, 每一小节的最核心的参考文献如下.

§ 1 Neukirch [3], Enochs [1].

§ 2 李文威 [12].

§ 3 李文威 [12], Witt [5], Serre [4].

文中具体涉及到引用的地方也会再次特别标注出来.

1 整数环 $\mathbb{Z}$ 的完备化

基于柯西列收敛意义的“完备化”一词在不同的学科有着不同的定义. 具体到我们研究的整数集 $\mathbb{Z}$, 若将其视为一个带有度量 [14, 第二章 § 1] 的集合, 则其完备化是在“度量”意义下的, 完备化的结果是完备度量空间 [14, 第七章 § 4]; 若将其视为一个带有范数 [8, 第六章 § 3] 的线性空间结构, 则其完备化是在“范数”意义下的, 完备化的结果是完备赋范线性空间 [8, 第六章 § 5]. 而本文我们将整数集 $\mathbb{Z}$ 视为一个环结构, 所讨论的“完备化”是在“赋值”意义下的. 以下第 1 小节我们先介绍关于赋值的一些数学基础, 然后在第 2 小节聚焦于 $\mathbb{Z}$ 的分式域 $\mathbb{Q}$ 上的赋值, 在等价意义下对所关注的赋值种类的范围进行收缩, 最后在第 3 小节简单讨论一下 $\mathbb{Z}$ 的完备化问题.

1.1 环上赋值基础

我们先引入与完备化相关的一个核心概念: 赋值.

定义 1.1.1 设 $\Re$ 是一个环. 称单射 $|\bullet| : \Re \mapsto \mathbb{R}_{\geq 0}$ 是 $\Re$ 上的一个**赋值**, 若 $|\bullet|$ 满足

1. $|x| = 0. \iff x = \mathbf{0}$;
2. $|xy| = |x|\,|y|\,,\ \forall x,\ y \in \Re$;
3. $|x + y| \leq |x| + |y|\,,\ \forall x,\ y \in \Re$.

基于上面的定义, 环上赋值有如下几个基本的性质.

命题 1.1.2 环 $\Re$ 上的赋值 $|\bullet|$ 满足以下的性质 *(1), (2), (3)*. 特别地, 若 $\Re = \mathbb{K}$ 是一个域, 则额外满足性质 *(4)*.

1. $|\mathbf{1}| = 1$;
2. $|-\mathbf{1}| = 1$;
3. $|-x| = |x|\,,\ \forall x \in \Re$;
4. $\left|\dfrac{x}{y}\right| = \dfrac{|x|}{|y|},\ \forall x \in \mathbb{K},\ \forall y \in \mathbb{K}_{\neq \mathbf{0}}$.

证明

1. 由定义*1.1.1*条件 *(2)*, 成立

$$|r| \times |\mathbf{1}| = |r \times \mathbf{1}| = |r|\,,\ \forall r \in \Re. \tag{1.1.1}$$

规定 $r \neq \mathbf{0}$, 由定义*1.1.1*条件 *(1)*, 成立

$$|r| \neq 0. \tag{1.1.2}$$

在式 *(1.1.2)* 的基础上, 将式 *(1.1.1)* 两边同时除以 $|r|$, 即可得到 $|\mathbf{1}| = 1$.

2. 由定义*1.1.2*条件 *(2),* 对于 $-\mathbf{1} \in \Re$, 成立

$$|\mathbf{1}| = |(-\mathbf{1}) \times (-\mathbf{1})| = |-\mathbf{1}| \times |-\mathbf{1}|,$$

即有 $|-\mathbf{1}|^2 = 1$. 由于 $|-\mathbf{1}| \geq 0$, 因此只能是 $|-\mathbf{1}| = 1$.

3. 由定义*1.1.1*条件 *(2),* 成立

$$|-r| = |(-\mathbf{1})\, r| = |-\mathbf{1}|\, |r| = |r|, \ \forall r \in \Re.$$

4. $\forall x \in \mathbb{K}$, $\forall y \in \mathbb{K}_{\neq \mathbf{0}}$, 有 $x/y \in \mathbb{K}$, 且 $|y| \neq 0$. 由定义*1.1.1*条件 *(2),* 成立

$$|x| = \left|\frac{x}{y} y\right| = \left|\frac{x}{y}\right| |y|. \implies \left|\frac{x}{y}\right| = \frac{|x|}{|y|}.$$

至此, 明所欲证. □

我们想要对环上的众多赋值进行梳理. 借由以下定义, 我们从一个角度对含幺环上的赋值进行二分类.

定义 1.1.3 设 $\Re$ 是一个含幺环, $|\bullet|$ 是 $\Re$ 上的一个赋值. 记

$$\boldsymbol{n} := \underbrace{\mathbf{1} + \mathbf{1} + \cdots + \mathbf{1}}_{n\text{个}}, \ \forall n \in \mathbb{Z}_{>0},$$

其中 $\mathbf{1}$ 是 $\Re$ 的幺元.

1. 称 $|\bullet|$ 具有**非阿基米德性**, 若 $\exists M \in \mathbb{R}_{\geq 0}$, 使得 $\forall n \in \mathbb{Z}_{>0}$, $|\boldsymbol{n}| \leq M$;

2. 否则称 $|\bullet|$ 具有**阿基米德性**, 即 $\forall M \in \mathbb{R}_{\geq 0}$, $\exists n \in \mathbb{Z}$, 使得 $|\boldsymbol{n}| > M$.

在这样的分类视角下, 参考 J. Neukirch [3, Proposition 3.6], 我们指出非阿基米德赋值存在以下一个很好的等价数学表示.

命题 1.1.4 设 $\Re$ 是一个含幺环, $|\bullet|$ 是 $\Re$ 上的一个非阿基米德赋值, 当且仅当 $|\bullet|$ 满足**强三角不等式**

$$|\boldsymbol{x} + \boldsymbol{y}| \leq \max\{|\boldsymbol{x}|, \ |\boldsymbol{y}|\}, \ \forall x, \ y \in \mathbb{Z}.$$

证明

1. 先证明 $\Leftarrow$ 方向的推理是成立的.

已知成立

$$|\boldsymbol{x} + \boldsymbol{y}| \leq \max\{|\boldsymbol{x}|, \ |\boldsymbol{y}|\}, \ \forall x, \ y \in \mathbb{Z}. \tag{1.1.3}$$

(a) 第一步, 我们指出成立

$$\begin{gathered}|\boldsymbol{x_1}+\boldsymbol{x_2}+\cdots+\boldsymbol{x_n}|\leq\max\{|\boldsymbol{x_1}|,\ |\boldsymbol{x_2}|,\ \ldots,\ |\boldsymbol{x_n}|\},\\ \forall n\in\mathbb{Z}_{>0},\ \forall x_1,\ x_2,\ \ldots,\ x_n\in\mathbb{Z}.\end{gathered}\tag{1.1.4}$$

当 $n=1$ 时, 显然有 $|\boldsymbol{x_1}|=\max\{|\boldsymbol{x_1}|\}$.
假设 $n=k$ 时成立

$$|\boldsymbol{x_1}+\boldsymbol{x_2}+\cdots+\boldsymbol{x_k}|\leq\max\{|\boldsymbol{x_1}|,\ |\boldsymbol{x_2}|,\ \ldots,\ |\boldsymbol{x_k}|\}.\tag{1.1.5}$$

由式 *(1.1.3)* 和式 *(1.1.5)*, 有

$$\begin{aligned}&|\boldsymbol{x_1}+\boldsymbol{x_2}+\cdots+\boldsymbol{x_k}+\boldsymbol{x_{k+1}}|.\\ =&|(\boldsymbol{x_1}+\boldsymbol{x_2}+\cdots+\boldsymbol{x_k})+\boldsymbol{x_{k+1}}|.\\ \leq&\max\{\max\{|\boldsymbol{x_1}|,\ |\boldsymbol{x_2}|,\ \ldots,\ |\boldsymbol{x_k}|\},\ |\boldsymbol{x_{k+1}}|\}.\\ =&\max\{|\boldsymbol{x_1}|,\ |\boldsymbol{x_2}|,\ \ldots,\ |\boldsymbol{x_k}|,\ |\boldsymbol{x_{k+1}}|\}.\end{aligned}$$

由第一数学归纳法 *[10, § 1.3.3]*, 式 *(1.1.4)* 成立.

(b) 第二步, 我们指出成立

$$|\boldsymbol{n}|\leq 1,\ \forall n\in\mathbb{Z}_{>0}.$$

事实上, $\forall n\in\mathbb{Z}_{>0}$, 由第一步的结论有

$$|\boldsymbol{n}|=\left|\underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{n个}\right|\leq\max\{|\mathbf{1}|,\ \ldots,\ |\mathbf{1}|\}=1.$$

由定义*1.1.3*, $|\bullet|$ 具有非阿基米德性.

2. 再证明 $\Rightarrow$ 方向的推理是成立的.
此方向下, 已知 $|\bullet|$ 具有非阿基米德性.

(a) 第一步, 我们指出成立

$$\begin{gathered}|\boldsymbol{x}+\boldsymbol{y}|\leq M^{\frac{1}{n}}(1+n)^{\frac{1}{n}}\max\{|\boldsymbol{x}|,\ |\boldsymbol{y}|\},\\ \forall n\in\mathbb{Z}_{>0},\ \forall x,\ y\in\mathbb{Z},\ \exists M\in\mathbb{R}_{\geq 0}.\end{gathered}\tag{1.1.6}$$

事实上, 由于 $|\bullet|$ 具有非阿基米德性, 根据定义*1.1.3*, 成立

$$|\boldsymbol{n}|\leq M,\ \exists M\in\mathbb{R}_{\geq 0},\ \forall n\in\mathbb{Z}_{>0}.\tag{1.1.7}$$

由于 $\forall v\in\{1,\ \ldots,\ n\}$, 组合数 $\binom{n}{v}\in\mathbb{Z}_{>0}$[1] *[15, 第一章 § 5]*, 由式 *(1.1.7)*, 自然也就成立

$$\left|\binom{n}{v}\right|\leq M.\tag{1.1.8}$$

[1]组合数是正整数的严格证明详见附录A.1.

$\forall x,\ y \in \mathbb{Z}$, 不妨令 $|\boldsymbol{x}| \geq |\boldsymbol{y}| \geq 0$, 成立

$$|\boldsymbol{x}|^v |\boldsymbol{y}|^{n-v} \leq |\boldsymbol{x}|^v |\boldsymbol{x}|^{n-v} = |\boldsymbol{x}|^n,\ \forall v \in \{1,\ \ldots,\ n\}. \tag{1.1.9}$$

考虑 $|\boldsymbol{x}+\boldsymbol{y}|^n$, 由定义*1.1.1*条件 *(2)*, 有

$$|\boldsymbol{x}+\boldsymbol{y}|^n = \underbrace{|\boldsymbol{x}+\boldsymbol{y}| \ldots |\boldsymbol{x}+\boldsymbol{y}|}_{n\text{个}} = |(\boldsymbol{x}+\boldsymbol{y})^n|. \tag{1.1.10}$$

由定义*1.1.1*条件 *(2)*, 条件 *(3)*, 式 *(1.1.8)*, 式 *(1.1.9)*, 成立

$$\begin{aligned}
|(\boldsymbol{x}+\boldsymbol{y})^n| &= \left|\sum_{v=0}^{n} \binom{n}{v} \boldsymbol{x}^v \boldsymbol{y}^{n-v}\right|. \\
&\leq \sum_{v=0}^{n} \left|\binom{n}{v} \boldsymbol{x}^v \boldsymbol{y}^{n-v}\right|. \\
&= \sum_{v=0}^{n} \left|\binom{n}{v}\right| |\boldsymbol{x}|^v |\boldsymbol{y}|^{n-v}. \\
&\leq \sum_{v=0}^{n} M |\boldsymbol{x}|^n = M(n+1) |\boldsymbol{x}|^n,
\end{aligned}$$

即得到

$$|(\boldsymbol{x}+\boldsymbol{y})^n| \leq M(n+1) |\boldsymbol{x}|^n. \tag{1.1.11}$$

由式 *(1.1.10)* 和式 *(1.1.11)* 即可得到

$$|\boldsymbol{x}+\boldsymbol{y}|^n \leq M(n+1) |\boldsymbol{x}|^n = M(n+1) (\max\{|\boldsymbol{x}|,\ |\boldsymbol{y}|\})^n. \tag{1.1.12}$$

式 *(1.1.12)* 两边同时开 n 次方, 即可得式 *(1.1.6)* 成立.

(b) 第二步, 我们分别计算 $\lim_{n\to\infty} M^{1/n}$ 和 $\lim_{n\to\infty} (1+n)^{1/n}$.

对于 $M^{1/n}$, 显然有 $\lim_{n\to\infty} M^{1/n} = 1$.

对于 $(1+n)^{1/n}$, 先考虑其对数 $\ln(1+n)^{1/n} = \frac{\ln(1+n)}{n}$. 由洛必达法则 *[7, 第六章 § 2]*, 有

$$\lim_{n\to\infty} \frac{\ln(1+n)}{n} = \lim_{n\to\infty} \frac{1}{1+n} = 0.$$

于是有

$$\lim_{n\to\infty} (1+n)^{\frac{1}{n}} = \lim_{n\to\infty} \mathsf{e}^{\frac{1}{n}\ln(1+n)} = \mathsf{e}^{\lim_{n\to\infty} \frac{1}{n}\ln(1+n)} = \mathsf{e}^0 = 1.$$

(c) 第三步, 我们指出成立

$$|\boldsymbol{x}+\boldsymbol{y}| \leq \max\{|\boldsymbol{x}|,\ |\boldsymbol{y}|\}. \tag{1.1.13}$$

事实上, 基于第二步, 令式 *(1.1.6)* 两边的 $n \to \infty$, 即有

$$|\boldsymbol{x}+\boldsymbol{y}| \leq M^{\frac{1}{n}} (1+n)^{\frac{1}{n}} \max\{|\boldsymbol{x}|,\ |\boldsymbol{y}|\} \to \max\{|\boldsymbol{x}|,\ |\boldsymbol{y}|\}\ (n \to \infty).$$

由极限的保不等式性 *[7, 定理 2.5]*, 式 *(1.1.13)* 成立.

至此, 明所欲证. □

推论 1.1.5 设 $\Re$ 是一个含幺环, $|\bullet|$ 是 $\Re$ 上的一个非阿基米德赋值. $\forall x_1,\ x_2,\ \cdots,\ x_n \in \mathbb{Z}\ (1 \leq n < \infty)$, 成立

$$|\boldsymbol{x_1} + \boldsymbol{x_2} + \cdots + \boldsymbol{x_n}| \leq \max\{|\boldsymbol{x_i}| :\ i = 1,\ 2,\ \cdots,\ n\}.$$

证明 $n = 1$ 时结论是显然的. $n = 2$ 时结论已由命题*1.1.4*给出. 假设 $n = k$ 时成立

$$|\boldsymbol{x_1} + \boldsymbol{x_2} + \cdots + \boldsymbol{x_k}| \leq \max_{1 \leq i \leq k} \{|\boldsymbol{x_i}|\}. \tag{1.1.14}$$

由于 $|\bullet|$ 是非阿基米德的, 根据命题*1.1.4*和式 *(1.1.14)*, 有

$$\begin{aligned}
&|\boldsymbol{x_1} + \boldsymbol{x_2} + \cdots + \boldsymbol{x_k} + \boldsymbol{x_{k+1}}|. \\
=&|(\boldsymbol{x_1} + \boldsymbol{x_2} + \cdots + \boldsymbol{x_k}) + \boldsymbol{x_{k+1}}|. \\
\leq&\max\{|\boldsymbol{x_1} + \boldsymbol{x_2} + \cdots + \boldsymbol{x_k}|,\ |\boldsymbol{x_{k+1}}|\}. \\
\leq&\max\left\{\max_{1 \leq i \leq k} \{|\boldsymbol{x_i}|\},\ |\boldsymbol{x_{k+1}}|\right\}. \\
=&\max_{1 \leq i \leq k+1} \{|\boldsymbol{x_i}|\}.
\end{aligned}$$

由第一数学归纳法, 推论得证. □

更进一步地, 我们可以得到关于含幺环上非阿基米德赋值的一个很好的性质.

命题 1.1.6 设 $\Re$ 是一个含幺环, $|\bullet|$ 是 $\Re$ 上的一个赋值. 若 $|\bullet|$ 具有非阿基米德性, 则 $\forall x,\ y \in \mathbb{Z}$, 当 $|\boldsymbol{x}| \neq |\boldsymbol{y}|$ 时成立**严格三角等式**

$$|\boldsymbol{x} + \boldsymbol{y}| = \max\{|\boldsymbol{x}|,\ |\boldsymbol{y}|\}.$$

证明 由于 $|\boldsymbol{x}| \neq |\boldsymbol{y}|$, 不失一般性地规定 $|\boldsymbol{x}| > |\boldsymbol{y}|$. $|\bullet|$ 是非阿基米德的, 由命题*1.1.4*, $\forall x,\ y \in \mathbb{Z}$, 成立

$$|\boldsymbol{x} + \boldsymbol{y}| \leq \max\{|\boldsymbol{x}|,\ |\boldsymbol{y}|\}. \tag{1.1.15}$$

在上式中令 $\boldsymbol{x} := \boldsymbol{x} + \boldsymbol{y} \in \Re$, $\boldsymbol{y} := -\boldsymbol{y} \in \Re$, 得到

$$|\boldsymbol{x}| = |(\boldsymbol{x} + \boldsymbol{y}) - \boldsymbol{y}| \leq \max\{|\boldsymbol{x} + \boldsymbol{y}|,\ |-\boldsymbol{y}|\} = \max\{|\boldsymbol{x} + \boldsymbol{y}|,\ |\boldsymbol{y}|\}. \tag{1.1.16}$$

由式 *(1.1.15)*, 式 *(1.1.16)*, 成立

$$|\boldsymbol{x}| \leq \max\{|\boldsymbol{x} + \boldsymbol{y}|,\ |\boldsymbol{y}|\} \leq \max\{|\boldsymbol{x}|,\ |\boldsymbol{y}|\} = |\boldsymbol{x}|. \tag{1.1.17}$$

基于式 *(1.1.17)*, 成立以下推理

$$\left.\begin{matrix}\max\{|\boldsymbol{x} + \boldsymbol{y}|,\ |\boldsymbol{y}|\} = |\boldsymbol{x}|. \\ |\boldsymbol{x}| > |\boldsymbol{y}|.\end{matrix}\right\} \implies |\boldsymbol{x} + \boldsymbol{y}| = |\boldsymbol{x}| = \max\{|\boldsymbol{x}|,\ |\boldsymbol{y}|\}.$$

至此, 明所欲证. □

推论 1.1.7 设 $\mathfrak{R}$ 是一个含幺环, $|\bullet|$ 是 $\mathfrak{R}$ 上的一个非阿基米德赋值. $\forall n \in \mathbb{Z}_{\geq 2}$, $\forall x_1, x_2, \cdots, x_n \in \mathbb{Z}$, 若它们的赋值两两不等, 即 $\forall i \neq j \in \{1,\ 2,\ \cdots,\ n\}$, $|\boldsymbol{x_i}| \neq |\boldsymbol{x_j}|$, 则成立

$$\left|\sum_{k=1}^{n} \boldsymbol{x_k}\right| = \max_{1\leq k\leq n} \{|\boldsymbol{x_k}|\}.$$

证明

1. 第一步, 我们指出 $\forall n \in \mathbb{Z}_{\geq 2}$, 在成立条件

$$\forall x_1,\ x_2,\ \cdots,\ x_n \in \mathbb{Z},\ \text{s.t.}\, |x_i| \neq |x_j|,\ \forall i \neq j, \tag{1.1.18}$$

的前提下, 成立

$$\left|\sum_{\substack{1\leq k\leq n\\ k\neq k_0}} \boldsymbol{x_k}\right| \neq |\boldsymbol{x_{k_0}}|,\ \forall k_0 \in \{1,\ 2,\ \cdots,\ n\}, \tag{1.1.19}$$

并记 $X := \{x_1,\ x_2,\ \cdots,\ x_n \in \mathbb{Z}\}$.

任意挑选 2 个满足条件 *(1.1.18)* 的 $x_{i,1},\ x_{i,2} \in X$, 显然有 $|\boldsymbol{x_{i,1}}| \neq |\boldsymbol{x_{i,2}}|$.

假设任意挑选满足条件 *(1.1.18)* 的 $j\,(<n)$ 个 $x_{i,1},\ x_{i,2},\ \cdots,\ x_{i,j} \in X$, 均成立

$$\left|\sum_{\substack{1\leq k\leq j\\ k\neq k_0}} \boldsymbol{x_{i,k}}\right| \neq |\boldsymbol{x_{i,k_0}}|,\ \forall k_0 \in \{1,\ 2,\ \cdots,\ j\}. \tag{1.1.20}$$

则任意挑选 $j+1$ 个满足条件 *(1.1.18)* 的 $x_{i,1},\ x_{i,2},\ \cdots,\ x_{i,j},\ x_{i,j+1} \in X$, $\forall k_0 \in \{1,\ 2,\ \cdots,\ j+1\}$, 再任取 $k_1 \in \{1,\ 2,\ \cdots,\ j+1\}$ 满足 $k_1 \neq k_0$, 由式 *(1.1.20)*, 命题*1.1.6*, 条件 *(1.1.18)*, 成立

$$\left|\sum_{\substack{1\leq k\leq j+1\\ k\neq k_0}} \boldsymbol{x_{i,k}}\right| = \left|\left(\sum_{\substack{1\leq k\leq j+1\\ k\neq k_0,k_1}} \boldsymbol{x_{i,k}}\right) + \boldsymbol{x_{i,k_1}}\right| = \max\left\{\left|\sum_{\substack{1\leq k\leq j+1\\ k\neq k_0,k_1}} \boldsymbol{x_{i,k}}\right|, |\boldsymbol{x_{i,k_1}}|\right\} \neq |\boldsymbol{x_{i,k_0}}|.$$

由第一数学归纳法, 式 *(1.1.19)* 成立.

2. 第二步, 基于第一步的结论, 并根据命题*1.1.6*, 成立

$$\begin{aligned}
\left|\sum_{k=1}^{n} \boldsymbol{x_k}\right| &= \left|\left(\sum_{k=1}^{n-1} \boldsymbol{x_k}\right) + \boldsymbol{x_n}\right|. \\
&= \max\left\{\left|\sum_{k=1}^{n-1} \boldsymbol{x_k}\right|, |\boldsymbol{x_n}|\right\}. \\
&= \max\left\{\max\left\{\left|\sum_{k=1}^{n-2} \boldsymbol{x_k}\right|, |\boldsymbol{x_{n-1}}|\right\}, |\boldsymbol{x_n}|\right\} = \max\left\{\left|\sum_{k=1}^{n-2} \boldsymbol{x_k}\right|, |\boldsymbol{x_{n-1}}|, |\boldsymbol{x_n}|\right\}. \\
&= \cdots. \\
&= \max_{1\leq k\leq n} \{|\boldsymbol{x_k}|\}.
\end{aligned}$$

至此, 明所欲证. □

对含幺环上众多赋值进行分类和性质探讨后, 我们想引入“等价”概念对这些赋值建立起联系, 以实现进一步的梳理. 等价概念的建立需要借助拓扑学基础, 于是我们参考尤承业 [9, 第一章 § 1], 先引入相关的基本概念.

定义 1.1.8 设 X 是一个集合, 称 X 上的一个映射 $d:\ X\times X\mapsto \mathbb{R}_{\geq 0}$ 是一个**度量**, 若 d 满足:

1. $d(x,y)=0. \iff x=y$;
2. $d(x,y)=d(y,x),\ \forall x,\ y\in X$;
3. $d(x,z)\leq d(x,y)+d(y,z),\ \forall x,\ y,\ z\in X$.

当集合 X 上规定了一个度量 d 后, 称 X 为**度量空间**, 记作 (X,d).

当集合 X 是带赋值 $|\bullet|$ 的环结构时, 我们考虑以下的一类特殊度量.

命题 1.1.9 设 $\Re$ 是一个环, $|\bullet|$ 是 $\Re$ 上的一个赋值. 定义映射 d

$$d(x,y):=|x-y|,\ \forall x,\ y\in\Re,$$

则 d 是 $\Re$ 上的一个度量, 称为**由 $\Re$ 上赋值 $|\bullet|$ 定义的度量**.

证明 $\forall x,\ y\in\Re$, 有 $|x-y|\geq 0$, 因此映射 d 可以表示为 $d:\ \Re\times\Re\mapsto\mathbb{R}_{\geq 0}$.

$$d(x,y)=0. \iff |x-y|=0. \iff x-y=0. \iff x=y,$$

满足定义 *(1.1.8)* 条件 *(1)*.

$$d(x,y)=|x-y|=|y-x|=d(y,x),\ \forall x,\ y\in\Re,$$

满足定义 *(1.1.8)* 条件 *(2)*.
由定义*1.1.1*条件 *(3)*, 成立

$$\begin{aligned} d(x,z)=|x-z|&=|(x-y)+(y-z)|. \\ &\leq |x-y|+|y-z|=d(x,y)+d(y,z),\ \forall x,\ y,\ z\in\Re, \end{aligned}$$

满足定义 *(1.1.8)* 条件 *(3)*.
综上, d 是 $\Re$ 上的一个度量. □

在度量意义下, 对一个环 $\Re$ 里面的点列的收敛性进行以下严格定义.

定义 1.1.10 设 $\Re$ 是一个环, $|\bullet|$ 是 $\Re$ 上的一个赋值, d 是 $|\bullet|$ 定义的度量. 对于一个可数无穷序列 $\{x_n\}$, 称 $\{x_n\}$ **依度量 d 收敛于点** $a\in\Re$, 若满足

$$\lim_{n\to\infty} d(x_n,a)=0.$$

基于度量, 我们可以定义出以下的一种拓扑结构.

定义 1.1.11 设 (X,d) 是一个度量空间. $\forall \varepsilon>0$, $\forall x_0\in X$, 记

$$B\left(x_0,\varepsilon\right):=\left\{x\in X:\ d\left(x_0,x\right)<\varepsilon\right\},$$

称

$$\tau_d:=\left\{\bigcup_{x\in\mathcal{I}}B\left(x,\varepsilon_x\right):\ \mathcal{I}\subseteq X,\ \varepsilon_x>0\right\}$$

为 X 上的**度量拓扑**.

有了度量拓扑这个结构, 我们就可以定义联系不同赋值的一种纽带: 赋值等价.

定义 1.1.12 设 $\Re$ 是一个环, $|\bullet|_1$ 和 $|\bullet|_2$ 是 $\Re$ 上的两个赋值, d_1 和 d_2 分别是由 $|\bullet|_1$ 和 $|\bullet|_2$ 定义的度量, τ_1 和 τ_2 分别是度量空间 $(\Re,d_1)$ 和 $(\Re,d_2)$ 的度量拓扑. 称 $|\bullet|_1$ 与 $|\bullet|_2$ 满足**赋值等价**, 若 $\tau_1=\tau_2$. 此时可记 $|\bullet|_1\cong|\bullet|_2$.

赋值等价的原始定义是基于度量拓扑结构的, 实际应用起来不太方便. 为此, 参考了 J. Neukirch [3, Proposition 3.3], 在域的范围内我们指出存在以下几种应用性较强的, 意义等价的表述.

命题 1.1.13 设 $\mathbb{K}$ 是一个域, $|\bullet|_1$ 和 $|\bullet|_2$ 是 $\mathbb{K}$ 上的两个赋值, 则以下三种说法是等价的.

1. $|\bullet|_1$ 和 $|\bullet|_2$ 等价 ;
2. $|x|_1<1.\iff|x|_2<1$;
3. $\exists s\in\mathbb{R}_{\geq0}$, 使得 $\forall x\in\mathbb{K}$, $|x|_1=|x|_2^{\,s}$.

注记 若 $\mathbb{K}=\Re$ 只是一个环而不是域, 根据下面具体的证明过程, 还是能够成立推理 $(3)\Longrightarrow(1)\Longrightarrow(2)$.

证明 记 $|\bullet|_1$ 和 $|\bullet|_2$ 定义的度量为 d_1 和 d_2, 相应的度量拓扑为 τ_1 和 τ_2.

1. $(3)\Longrightarrow(1)$

   (a) 我们指出成立 $\tau_1=\tau_2$.

   $\forall B_1\left(x_0,\varepsilon\right)=\left\{x\in\mathbb{K}:\ d_1\left(x_0,x\right)<\varepsilon\right\}\in\tau_1$, 其中 $\varepsilon\in\mathbb{R}_{>0}$, (3) 的成立蕴含

   $$d_1\left(x_0,x\right)=|x_0-x|_1=|x_0-x|_2^{\,s}<\varepsilon,\ \forall x\in B_1\left(x_0,\varepsilon\right),\ \exists s\in\mathbb{R}_{\geq0}.\tag{1.1.21}$$

   i. 当 $s\neq0$ 时即有

   $$|x_0-x|_2<\varepsilon^{1/s},\ \varepsilon^{1/s}\in\mathbb{R}_{>0}.$$

   因此 $B_1\left(x_0,\varepsilon\right)=B_2\left(x_0,\varepsilon^{1/s}\right)\in\tau_2$.

   ii. 当 $s=0$ 时, $d_1\left(x_0,x\right)=|x_0-x|_2^{\,0}=1$.

A. 若 $0<\varepsilon\leq 1$, 则 $B_1(x_0,\varepsilon)=\varnothing\in\tau_2$.

B. 若 $\varepsilon>1$, 则 $d_1(x_0,x)<\varepsilon$ 恒成立, $B_1(x_0,\varepsilon)=\mathbb{K}\in\tau_2$.

综上可推得 $\tau_1\subseteq\tau_2$. 同理可证得 $\tau_2\subseteq\tau_1$. 因此即可证得 $\tau_1=\tau_2$.

(b) 在前一步的基础上, 由定义 *(1.1.12)*, $|\cdot|_1$ 与 $|\cdot|_2$ 等价.

2. $(1)\Longrightarrow(2)$

(a) 第一步, 我们指出成立

$$x\text{的赋值}|x|<1.\iff\{x^n\}_{n\in\mathbb{Z}_{>0}}\text{依赋值}|\cdot|\text{定义的度量}d\text{收敛于}0\in\mathbb{K},\ \forall x\in\mathbb{K}.$$

i. 已知 $|x|<1$, 结合定义*1.1.1*的第 *(2)* 条, 则有

$$|x^n-0|=|x^n|=|x|^n\to 0\ (n\to\infty).$$

ii. 反之, 已知 $\{x^n\}_{n\in\mathbb{Z}_{>0}}$ 依度量 d 收敛于 $0\in\mathbb{K}$.

A. 若 $|x|=1$, 则有

$$|x^n-0|=|x|^n=1\ (n\to\infty),$$

即 0 不是 $\{x^n\}_{n\in\mathbb{Z}_{>0}}$ 的收敛点, 矛盾.

B. 若 $|x|>1$, 则有

$$|x^n-0|=|x|^n\to\infty\ (n\to\infty),$$

即 0 不是 $\{x^n\}_{n\in\mathbb{Z}_{>0}}$ 的收敛点, 矛盾.

由反证法, 得出 $|x|<1$.

(b) 第二步, 我们指出在 *(1)* 成立的条件下, 成立

$$\begin{aligned}&\{x^n\}_{n\in\mathbb{Z}_{>0}}\text{依度量}d_1\text{收敛于}0\in\mathbb{K}.\\\iff&\{x^n\}_{n\in\mathbb{Z}_{>0}}\text{依度量}d_2\text{收敛于}0\in\mathbb{K}.\end{aligned}$$

i. 已知 $\{x^n\}_{n\in\mathbb{Z}_{>0}}$ 依度量 d_1 收敛于 0, 则有

$$\lim_{n\to\infty}|x^n-0|_1=\lim_{n\to\infty}|x|_1{}^n=0.$$

在度量空间 $(\mathbb{K},d_1)$ 中, 对每一个 x^n, 构造球形区域

$$B_n\left(0,\ |x|_1{}^n+\frac{1}{n}\right)\in\tau_1,$$

简记为 B_n, 有 $x^n\in B_n$, 且成立

$$\lim_{n\to\infty}B_n\left(0,\ |x|_1{}^n+\frac{1}{n}\right)=\{0\}.\tag{1.1.22}$$

由于 $|\bullet|_1$ 与 $|\bullet|_2$ 等价, 因此 $\tau_1 = \tau_2$, 有 $\forall n \in \mathbb{Z}_{>0}$, $B_n \in \tau_2$, 即在度量空间 $(\mathbb{K}, d_2)$ 中, 也存在序列 $\{B_n\}$. 记

$$\begin{aligned} {d_2}^{(n)} &:= |x^n - 0|_2 = {|x|_2}^n, \\ {d_{\sup}}^{(n)} &:= \sup_{b \in B_n} |b - 0| = \sup_{b \in B_n} |b|. \end{aligned}$$

式 *(1.1.22)* 蕴含

$${d_{\sup}}^{(n)} \to 0 \ (n \to \infty). \tag{1.1.23}$$

由于 $x^n \in B_n$, 成立

$$0 \leq {d_2}^{(n)} \leq {d_{\sup}}^{(n)}. \tag{1.1.24}$$

式 *(1.1.23)* 和 *(1.1.24)* 蕴含 $\lim_{n\to\infty} {d_2}^{(n)} = 0$, 因此 $\{x^n\}_{n\in\mathbb{Z}_{>0}}$ 依度量 d_2 收敛于 0.

ii. 同理可证得若 $\{x^n\}_{n\in\mathbb{Z}_{>0}}$ 依度量 d_2 收敛于 0, 则 $\{x^n\}_{n\in\mathbb{Z}_{>0}}$ 依度量 d_1 收敛于 0, 因此二者等价.

(c) 第三步, 基于第一步和第二步, 成立以下等价关系

$$\begin{aligned} & |x|_1 < 1. \\ \Longleftrightarrow\ & \{x^n\}_{n\in\mathbb{Z}_{>0}} \text{依度量} d_1 \text{收敛于} 0. \\ \Longleftrightarrow\ & \{x^n\}_{n\in\mathbb{Z}_{>0}} \text{依度量} d_2 \text{收敛于} 0. \\ \Longleftrightarrow\ & |x|_2 < 1. \end{aligned}$$

3. (2) $\Longrightarrow$ (3)

(a) 若 $|\bullet|_1$ 满足 $\forall x \in \mathbb{K}_{\neq 0}$, $|x|_1 = 1$, 显然 $\exists s = 0 \in \mathbb{R}_{\geq 0}$, 使得 $\forall x \in \mathbb{K}$, 恒成立 $|x|_1 = {|x|_2}^0$.

(b) 若 $|\bullet|_1$ 满足 $\exists y \in \mathbb{K}$, $|y|_1 \neq 1$, 不失一般性地令 $|y|_1 < 1$ (若 $|y|_1 > 1$, 则 $|1/y|_1 < 1$), 固定该点 y , $\forall x \in \mathbb{K}$, 讨论以下情况.

i. 情况一

$x \neq 0$, 则 $\exists \alpha \in \mathbb{R}$ 使得 $|x|_1 = {|y|_1}^\alpha$. 由实数理论 *[7, 附录 II]*, 存在无限逼近 α 的一列有理数序列, 更具体地, 存在 $\{m_i/n_i\}$ 满足 $\forall i$, $m_i \in \mathbb{Z}$, $n_i \in \mathbb{Z}_{>0}$, $m_i/n_i < \alpha$, 且 $\lim_{i\to\infty} m_i/n_i = \alpha$. 结合命题*1.1.2*的性质 *(4)*, 成立

$$\begin{aligned} & |x|_1 = {|y|_1}^\alpha < {|y|_1}^{m_i/n_i}. \\ \Longrightarrow\ & {|x|_1}^{n_i} < {|y|_1}^{m_i}. \\ \Longrightarrow\ & \left|\frac{x^{n_i}}{y^{m_i}}\right|_1 = \frac{{|x|_1}^{n_i}}{{|y|_1}^{m_i}} < 1. \end{aligned} \tag{1.1.25}$$

根据式 *(1.1.25)* 和条件 *(2)*, 推得

$$\left|\frac{x^{n_i}}{y^{m_i}}\right|_2 < 1,$$

也就有

$$\frac{|x|_2^{\,n_i}}{|y|_2^{\,m_i}} < 1. \implies |x|_2 < |y|_2^{\,m_i/n_i}.$$

令 $i \to \infty$, 则得到 $|x|_2 \le |y|_2^{\,\alpha}$. 同样由实数理论, 存在一列有理数序列 $\{r_i/t_i\}$ 满足 $\forall i,\ r_i \in \mathbb{Z},\ t_i \in \mathbb{Z}_{>0},\ r_i/t_i > \alpha$, 且 $\lim_{i\to\infty} r_i/t_i = \alpha$. 同理可推得 $|x|_2 \ge |y|_2^{\,\alpha}$. 因此有 $|x|_2 = |y|_2^{\,\alpha}$.
条件 *(2)* 和 $|y|_1 < 1$ 蕴含 $|y|_2 < 1$, 于是 $\log|y|_1,\ \log|y|_2 \neq 0$. 于是可将 α 表示为

$$\alpha = \frac{\log|x|_1}{\log|y|_1} = \frac{\log|x|_2}{\log|y|_2}. \tag{1.1.26}$$

A. 若 $|x|_2 \neq 1$, 即 $\log|x|_2 \neq 0$, 则式 *(1.1.26)* 可以进一步推出

$$\frac{\log|x|_1}{\log|x|_2} = \frac{\log|y|_1}{\log|y|_2} =: s. \tag{1.1.27}$$

$|y|_1 < 1$ 且 $|y|_2 < 1$ 蕴含 $\log|y|_1,\ \log|y|_2 < 0$, 由式 *(1.1.27)*, $s > 0$, 且由于 y 是固定的, s 是一个与 x 取值无关的常数. 显然成立

$$|x|_1 = |x|_2^{\,s},\ s > 0. \tag{1.1.28}$$

B. 若 $|x|_2 = 1$, 则 $\log|x|_2 = 0$, 由式 *(1.1.26)*, $\log|x|_1 = 0$, $|x|_1 = 1$, 也满足式 *(1.1.28)*.

ii. 情况二

$x = 0$, 有 $|0|_1 = |0|_2 = 0$, 显然也满足式 *(1.1.28)*.

(c) 综上, $\exists s \in \mathbb{R}_{\ge 0}$, 使得 $\forall x \in \mathbb{K}$, $|x|_1 = |x|_2^{\,s}$. □

至此, 我们便介绍完了赋值的数学概貌.

1.2 三个特殊赋值与 Ostrowski 定理

在 § 1.1 节建立起环上赋值的类别基础和联系桥梁后, 我们先将目光转移到有理数域 $\mathbb{Q}$, 研究其上的一些经典的赋值结构, 然后通过赋值等价的桥梁得以间接地窥探 $\mathbb{Q}$ 上所有的赋值结构, 以至间接地窥探整数环 $\mathbb{Z}$ 上所有的赋值结构, 方便后面 § 1.3 节研究 $\mathbb{Z}$ 的完备化. 以下我们先介绍三种典型的映射结构.

定义 1.2.1 设 $\Re$ 是一个环. 单射 $|\bullet|$:

$$|x| = \begin{cases} 1, \ x \in \Re_{\neq \mathbf{0}}, \\ 0, \ x = \mathbf{0}, \end{cases}$$

称为**平凡绝对值**, 记为 $|\bullet|_{\clubsuit}$.

定义 1.2.2 有理数域 $\mathbb{Q}$ 上的单射 $|\bullet|$:

$$|x| = x \bullet \operatorname{sgn}(x) = \begin{cases} x, \ x > 0, \\ 0, \ x = 0, \\ -x, \ x < 0, \end{cases}$$

称为**普通绝对值**, 记为 $|\bullet|_{\infty}$.

定义 1.2.3 设 p 是一个素数. $\forall a = b/c \in \mathbb{Q}_{\neq 0}$ 且 $b, \ c \in \mathbb{Z}_{\neq 0}$, 令 $p^m \| b$ [2] , $p^n \| c$, $b = p^m b'$, $c = p^n c'$. 显然有 $m, \ n < \infty$, 且成立

$$a = \frac{b}{c} = \frac{p^m b'}{p^n c'} = p^{m-n} \frac{b'}{c'}, \ \gcd(b'c', p) = 1.$$

称 $|\bullet|_p$ 是 $\mathbb{Q}$ 上的 p-**进绝对值**, 若满足

$$|a|_p = \begin{cases} p^{n-m}, \ a \in \mathbb{Q}_{\neq 0}, \\ 0, \ a = 0. \end{cases}$$

注记 上面定义的 p-进绝对值是狭义的, 该定义可拓展到特征不为 p 的一般环 $\Re$ 上. 记 $\boldsymbol{p} := \sum_{i=1}^{p} \mathbf{1} \in \Re$, 令 $\boldsymbol{p}^n \| a \in \Re$, $n \in \mathbb{Z} \cup \{\infty\}$, 定义

$$|a|_{\boldsymbol{p}} := \begin{cases} p^{-n}, \ a \neq \mathbf{0}, \\ 0, \ a = \mathbf{0}. \end{cases}$$

称 $|\bullet|_{\boldsymbol{p}}$ 是**广义的** p-**进绝对值**.

我们指出, 以上列举的这三种绝对值都可以视为 $\mathbb{Q}$ 上的赋值结构.

命题 1.2.4 $\mathbb{Q}$ 上的平凡绝对值 $|\bullet|_{\clubsuit}$ 是 $\mathbb{Q}$ 上的赋值. 此时也称 $|\bullet|_{\clubsuit}$ 是 $\mathbb{Q}$ 上的**平凡赋值**.

[2]表示 $p^m \mid b$ 但 $p^{m+1} \nmid b$, 下同.

证明 由 $|\bullet|_{\clubsuit}$ 的定义*1.2.1*, 显然成立

$$|x|_{\clubsuit} = 0. \iff x = 0,$$

满足定义*1.1.1*的条件 *(1)*.

$\forall x,\ y \in \mathbb{Q}$, 进行分类讨论如下:

1. 当 $x,\ y$ 均不为 0 时, 成立

$$\begin{aligned} xy \neq 0. &\implies |xy|_{\clubsuit} = 1 = 1 \times 1 = |x|_{\clubsuit} \cdot |y|_{\clubsuit}, \\ |x+y|_{\clubsuit} &\leq 1 < 1 + 1 = |x|_{\clubsuit} + |y|_{\clubsuit}. \end{aligned}$$

2. 当 $x,\ y$ 至少有一个为 0 时, 不妨令 $y = 0$, 则成立

$$\begin{aligned} xy = 0. &\implies |xy|_{\clubsuit} = 0 = 1 \times 0 = |x|_{\clubsuit} \cdot |y|_{\clubsuit}, \\ |y|_{\clubsuit} \geq 0. &\implies |x+y|_{\clubsuit} = |x|_{\clubsuit} \leq |x|_{\clubsuit} + |y|_{\clubsuit}. \end{aligned}$$

因此 $|\bullet|_{\clubsuit}$ 满足定义*1.1.1*的条件 *(2)* 和 *(3)*.

综上, $|\bullet|_{\clubsuit}$ 是域 $\mathbb{Q}$ 上的赋值. □

命题 1.2.5 $\mathbb{Q}$ 上的普通绝对值 $|\bullet|_{\infty}$ 是 $\mathbb{Q}$ 上的赋值. 此时也称 $|\bullet|_{\infty}$ 是 $\mathbb{Q}$ 上的**普通赋值**.

证明 结论是显然的. □

命题 1.2.6 $\mathbb{Q}$ 上的 p-进绝对值 $|\bullet|_p$ 是 $\mathbb{Q}$ 上的赋值. 此时也称 $|\bullet|_p$ 是 $\mathbb{Q}$ 上的 p-**进赋值**.

证明 根据定义*1.2.3*, 显然有 $|\bullet|_p :\ \mathbb{Q} \mapsto \mathbb{R}_{\geq 0}$. $\forall a_{1,2} \in \mathbb{Q}_{\neq 0}$, 将其记为以下形式

$$\begin{gathered} a_{1,2} = p^{n_{1,2}} \frac{{b_{1,2}}'}{{c_{1,2}}'}, \\ \exists b_{1,2} \in \mathbb{Z},\ \exists c_{1,2} \in \mathbb{Z}_{\neq 0},\ \gcd\left({b_{1,2}}'{c_{1,2}}', p\right) = 1. \end{gathered}$$

1. 由于 $|0|_p = 0$, 而 $|a_1|_p = p^{-n_1} \neq 0$, 因此满足定义*1.1.1*的条件 *(1)*.

2. 一方面, 成立

$$|a_1 a_2|_p = \left| \left(p^{n_1} \frac{{b_1}'}{{c_1}'} \right) \left(p^{n_2} \frac{{b_2}'}{{c_2}'} \right) \right|_p = \left| p^{n_1+n_2} \frac{{b_1}'{b_2}'}{{c_1}'{c_2}'} \right|_p. \tag{1.2.1}$$

另一方面, 成立推理

$$\left.\begin{aligned} \gcd\left({b_1}'{c_1}', p\right) = 1. \\ \gcd\left({b_2}'{c_2}', p\right) = 1. \end{aligned}\right\} \implies \gcd\left(\left({b_1}'{b_2}'\right)\left({c_1}'{c_2}'\right), p\right) = 1. \tag{1.2.2}$$

由式 *(1.2.1)*, 式 *(1.2.2)* 和定义*1.2.3*, 成立

$$|a_1 a_2|_p = p^{-(n_1+n_2)} = p^{-n_1} p^{-n_2} = |a_1|_p |a_2|_p,$$

满足定义*1.1.1*的条件 *(2)*.

3. 不妨令 $n_1 = \min\{n_1,\ n_2\}$. 一方面, 成立

$$\begin{aligned} a_1 + a_2 = p^{n_1}\frac{b_1{}'}{c_1{}'} + p^{n_2}\frac{b_2{}'}{c_2{}'} = p^{n_1}\frac{b_1{}'c_2{}' + p^{n_2-n_1}b_2{}'c_1{}'}{c_1{}'c_2{}'}, \\ b_1{}'c_2{}' + p^{n_2-n_1}b_2{}'c_1{}' \in \mathbb{Z},\ c_1{}'c_2{}' \in \mathbb{Z}_{\neq 0}. \end{aligned} \tag{1.2.3}$$

另一方面, 成立推理

$$\left.\begin{aligned} &\gcd(b_1{}'c_1{}', p) = 1. \\ &\gcd(b_2{}'c_2{}', p) = 1. \end{aligned}\right\} \implies \left.\begin{aligned} &\gcd(c_1{}', p) = 1. \\ &\gcd(c_2{}', p) = 1. \end{aligned}\right\} \implies \gcd(c_1{}'c_2{}', p) = 1. \tag{1.2.4}$$

令 $p^k \big\| (a_1 + a_2)$, 由式 *(1.2.3)*, 式 *(1.2.4)* 和定义*1.2.3*, 有 $k \geq n_1$, 成立

$$\begin{aligned} |a_1 + a_2|_p =& p^{-k} \leq p^{-n_1}. \\ =& p^{-\min\{n_1,\ n_2\}} = p^{\max\{-n_1,\ -n_2\}}. \\ =& \max\left\{p^{-n_1},\ p^{-n_2}\right\} = \max\left\{|a_1|_p,\ |a_2|_p\right\}. \end{aligned} \tag{1.2.5}$$

由于 $|a_1|_p,\ |a_2|_p \geq 0$, 因此又成立

$$\max\left\{|a_1|_p,\ |a_2|_p\right\} \leq |a_1|_p + |a_2|_p,$$

从而满足定义*1.1.1*的条件 *(3)*.

综上, $|\bullet|_p$ 是 $\mathbb{Q}$ 上的赋值. □

在明确了 $|\bullet|_\clubsuit$, $|\bullet|_\infty$, $|\bullet|_p$ 都是 $\mathbb{Q}$ 上的赋值结构后, 基于 § 1.1 节提供的分类标准, 我们进一步确定这三个赋值的类别.

命题 1.2.7 $\mathbb{Q}$ 上的平凡赋值 $|\bullet|_\clubsuit$ 是非阿基米德赋值.

证明 结论是显然的. □

命题 1.2.8 $\mathbb{Q}$ 上的普通赋值 $|\bullet|_\infty$ 是阿基米德赋值.

证明 $\forall M \in \mathbb{R}_{\geq 0}$, $\exists n = [M] + 1 \in \mathbb{Z}_{>0} \subseteq \mathbb{Q}$, 使得 $|n|_\infty = [M] + 1 > M$, 故普通赋值 $|\bullet|_\infty$ 具有阿基米德性. □

命题 1.2.9 $\mathbb{Q}$ 上的 p-进赋值 $|\bullet|_p$ 是非阿基米德赋值.

证明 $\forall n \in \mathbb{Z}_{>0} \subseteq \mathbb{Q}$, 令 $p^k \big\| n$, 其中 $k \in \mathbb{Z}_{\geq 0}$, 此时有

$$|n|_p = |n/1|_p = p^{0-k} = p^{-k} \leq 1.$$

故 p-进赋值 $|\bullet|_p$ 具有非阿基米德性. 或者直接根据命题*1.2.6*中的式 *(1.2.5)* 和命题*1.1.4*, 直接得出其非阿基米德性. □

完成了 $|\cdot|_{\clubsuit}$, $|\cdot|_{\infty}$, $|\cdot|_p$ 的归类后, 我们打算将有理数域 $\mathbb{Q}$ 上的其他赋值通过“赋值等价”与这三个赋值建立联系, 而这个联系已经由 A. Ostrowski [3] 给出 [3, Chapter II § 3]. 为了说明 Ostrowski 在这方面的工作, 下面先给出几个奠基性的引理.

引理 1.2.10 设 $\|\cdot\|$ 是有理数域 $\mathbb{Q}$ 上的非阿基米德赋值, 则集合 $I := \{a \in \mathbb{Z} : \|a\| < 1\}$ 是整数环 $\mathbb{Z}$ 的双边理想.

证明 记整数环结构为 $(\mathbb{Z}, +, \times)$.

1. 首先, $I = \{a \in \mathbb{Z} : \|a\| < 1\}$ 显然满足 $I \subseteq \mathbb{Z}$.

2. 其次, 我们指出

$$(I, +) \text{ 是一个交换群.}$$

(a) $\forall a,\ b \in I$, 一方面, 有 $a,\ b \in \mathbb{Z}$, 成立 $\|a\|, \|b\| < 1$.
另一方面, 由 $\mathbb{Z}$ 关于 $+$ 的运算封闭性, 有 $a + b \in \mathbb{Z}$. 由于 $\|\cdot\|$ 是非阿基米德的, 根据命题*1.1.4*, 有

$$\|a + b\| \leq \max\{\|a\|, \|b\|\} < 1.$$

因此有 $a + b \in I$.

(b) I 关于 $+$ 的结合律和交换律继承于 $\mathbb{Z}$.

(c) $\|0\| = 0 < 1$, 即 I 也包含 $\mathbb{Z}$ 的加法单位元 0.

(d) $\forall a \in I$ 满足 $\|a\| < 1$, 有

$$\|-a\| = \|-1\| \|a\| = \|a\| < 1,$$

即 $\exists (-a) \in I$, 使得 $a + (-a) = 0 \in I$.

3. 最后, 我们指出成立

$$I\mathbb{Z} \subseteq I,\ \mathbb{Z}I \subseteq I.$$

$\forall n \in \mathbb{Z}_{>0}$, 由于 $\|\cdot\|$ 是非阿基米德的, 根据推论*1.1.5*, 有

$$\|n\| = \|1 + \cdots + 1\| \leq \max\{\|1\|, \cdots, \|1\|\} = \|1\| = 1.$$

而 $\|-n\| = \|-1\| \|n\| = \|n\|$, $\|0\| = 0$, 因此 $\forall n \in \mathbb{Z}$, $\|n\| \leq 1$.
基于此, $\forall a \in I$, $\|a\| < 1$, 成立 $\|an\| = \|a\| \|n\| < 1$, 蕴含 $an \in I$, $I\mathbb{Z} \subseteq I$. 同理可证得 $\mathbb{Z}I \subseteq I$.

综上, I 是 $\mathbb{Z}$ 的双边理想. □

引理 1.2.11 $p\mathbb{Z}$ 是整数环 $\mathbb{Z}$ 的一个极大理想.

[3] Alexander Ostrowski, 1893.9—1986.11, 著名东欧数学家.

证明 记整数环结构为 $(\mathbb{Z},+,\times)$.

1. 第一步, 我们指出

$$p\mathbb{Z}\text{是整数环}\mathbb{Z}\text{的双边理想.}$$

(a) 首先显然有 $p\mathbb{Z}\subseteq\mathbb{Z}$.

(b) 其次证明 $(p\mathbb{Z},+)$ 是一个交换群.

i. $\forall pa_1,\ pa_2\in p\mathbb{Z},\ a_1,\ a_2\in\mathbb{Z}$, 由 $\mathbb{Z}$ 关于 $+$ 的运算封闭性有 $a_1+a_2\in\mathbb{Z}$, 从而成立

$$pa_1+pa_2=p\left(a_1+a_2\right)\in p\mathbb{Z}.$$

ii. $p\mathbb{Z}$ 关于 $+$ 的结合律和交换律继承于 $\mathbb{Z}$.

iii. $0\in p\mathbb{Z}$, 且 $\forall pa\in p\mathbb{Z},\ \exists p\left(-a\right)\in p\mathbb{Z}$, 使得 $pa+p\left(-a\right)=0$.

(c) 然后证明成立 $\left(p\mathbb{Z}\right)\mathbb{Z}\subseteq p\mathbb{Z}$ 且 $\mathbb{Z}\left(p\mathbb{Z}\right)\subseteq p\mathbb{Z}$.
$\forall pa\in\mathbb{Z},\ a\in\mathbb{Z},\ \forall b\in\mathbb{Z}$, 由 $\mathbb{Z}$ 关于 $\times$ 运算的封闭性, $a\times b\in\mathbb{Z}$, 因此成立

$$(pa)\times b=p\left(a\times b\right)\in p\mathbb{Z},$$

即有 $\left(p\mathbb{Z}\right)\mathbb{Z}\subseteq p\mathbb{Z}$. 同理可证得 $\mathbb{Z}\left(p\mathbb{Z}\right)\subseteq p\mathbb{Z}$.

于是 $p\mathbb{Z}$ 是整数环 $\mathbb{Z}$ 的双边理想.

2. 第二步, 我们指出

$$\text{理想}p\mathbb{Z}\text{是}\mathbb{Z}\text{的极大理想.}$$

假设 $p\mathbb{Z}$ 不是 $\mathbb{Z}$ 的极大理想, 则存在真理想 $I\subset\mathbb{Z}$ 满足 $p\mathbb{Z}\subset I$, 即 $\exists a\in I\subset\mathbb{Z}$, $a\notin p\mathbb{Z}$, 即 $p\nmid a$, $\gcd\left(p,a\right)=1$.
对素数 $p\in p\mathbb{Z}\subset I$ 和整数 $a\in I$ 作辗转相除法, 由初等数论的知识 *[15, 第一章 § 2]*, $\exists s,t\in\mathbb{Z}$, 使得

$$ps+at=\gcd\left(p,a\right)=1.$$

由于 I 是 $\mathbb{Z}$ 的双边理想, 有 $ps\in I$, $at\in I$, $1\in I$. 此时有 $I\mathbb{Z}=\mathbb{Z}\subseteq I\subseteq\mathbb{Z}$, 即 $I=\mathbb{Z}$, 这与假设 $I\subset\mathbb{Z}$ 矛盾. 由反证法, 不存在真理想 $I\subset\mathbb{Z}$ 满足 $p\mathbb{Z}\subset I$, I 就是整数环 $\mathbb{Z}$ 的极大理想. □

引理 1.2.12 设 $\|\bullet\|$ 是有理数域 $\mathbb{Q}$ 上的赋值, 则成立等式

$$\|m\|^{1/\log m}=\|n\|^{1/\log n},\ \forall n,\ m\in\mathbb{Z}_{>1}.$$

证明 $\forall n,\ m\in\mathbb{Z}_{>1}$, 将 m 记为 n-进制数形式

$$m=a_0+a_1n+\cdots+a_rn^r,$$

其中 $a_i \in \{0,\ 1,\ \cdots,\ n-1\}$, $n^r \leq m$ 即 $r \leq \log m/\log n$. 由定义*1.1.1*, $\|\bullet\|$ 满足三角不等式性质, 有

$$\|a_i\| = \left\| \underbrace{1+\cdots+1}_{a_i\text{个}} \right\| \leq \underbrace{\|1\|+\cdots+\|1\|}_{a_i\text{个}} = a_i \|1\| = a_i < n.$$

因此成立以下不等式

$$\begin{aligned} \|m\| &\leq \sum_{i=0}^{r} \|a_i\| \cdot \|n\|^i. \\ &\leq \sum_{i=0}^{r} n \cdot \|n\|^r. \\ &= (1+r)\, n \cdot \|n\|^r. \\ &\leq \left(1+\frac{\log m}{\log n}\right) n \cdot \|n\|^{\log m/\log n}. \end{aligned} \tag{1.2.6}$$

令式 *(1.2.6)* 中的 $m = m^k$, $k \in \mathbb{Z}_{\geq 0}$, 则有

$$\begin{aligned} \|m\|^k &= \left\|m^k\right\|. \\ &\leq \left(1+\frac{\log m^k}{\log n}\right) n \cdot \|n\|^{\log m^k/\log n}. \\ &= \left(1+\frac{\log m}{\log n}k\right) n \cdot \|n\|^{k\log m/\log n}. \end{aligned} \tag{1.2.7}$$

式 *(1.2.7)* 两边同时开 k 次方, 得到

$$\|m\| \leq \left(1+\frac{\log m}{\log n}k\right)^{1/k} n^{1/k} \|n\|^{\log m/\log n}. \tag{1.2.8}$$

计算得极限值

$$\lim_{k\to\infty} \frac{1}{k} \ln\left(1+\frac{\log m}{\log n}k\right) = \lim_{k\to\infty} \frac{\log m/\log n}{1+k\log m/\log n} = 0. \tag{1.2.9}$$

式 *(1.2.9)* 蕴含了

$$\lim_{k\to\infty} \left(1+\frac{\log m}{\log n}k\right)^{1/k} = e^0 = 1. \tag{1.2.10}$$

令式 *(1.2.8)* 中 $k \to \infty$, 结合式 *(1.2.10)*, 即可得到

$$\|m\| \leq \|n\|^{\log m/\log n}. \implies \|m\|^{1/\log m} \leq \|n\|^{1/\log n}.$$

在上述证明过程中, 交换 m 和 n 的地位, 可得到 $\|m\|^{1/\log m} \geq \|n\|^{1/\log n}$. 于是证得 $\|m\|^{1/\log m} = \|n\|^{1/\log n}$. □

有了以上的引理, 现在正式引入 Ostrowski **定理**如下.

定理 1.2.13 (A. Ostrowski) 有理数域 $\mathbb{Q}$ 上除去平凡赋值的任一非阿基米德赋值 $\|\bullet\|$ 等价于某一个具有非阿基米德性的 p-进赋值 $|\bullet|_p$（p 是素数）, 任一阿基米德赋值 $\|\bullet\|$ 等价于具有阿基米德性的普通赋值 $|\bullet|_\infty$.

证明

1. 我们先讨论 $\mathbb{Q}$ 上非阿基米德赋值的情况.

(a) 第一步, 任取 $\mathbb{Q}$ 上一个非平凡的非阿基米德赋值 $\|\bullet\|$, 我们指出成立

$$\|p\| < 1,\ \exists 素数 p \in \mathbb{Z} \subset \mathbb{Q}.$$

事实上, $\forall n \in \mathbb{Z}$, 由推论*1.1.5*, 成立

$$\|n\| = \|1 + \cdots + 1\| \leq 1. \tag{1.2.11}$$

若 $\mathbb{Z}$ 上所有素数 p 均满足 $\|p\| = 1$, 则一方面, $\forall n \in \mathbb{Z}_{>1}$, 由算数基本定理 *[15, 第一章 § 4]*, 存在素数 $p_1,\ p_2,\ \cdots,\ p_m \in \mathbb{Z}$ 和 $\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_m > 0$, 使得

$$n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_m}^{\alpha_m}. \tag{1.2.12}$$

式 *(1.2.12)* 蕴含了

$$\begin{aligned}\|n\| &= \left\|{p_1}^{\alpha_1}{p_2}^{a_2}\cdots{p_m}^{\alpha_m}\right\|. \\ &= \|{p_1}^{\alpha_1}\|\,\|{p_2}^{\alpha_2}\|\cdots\|p_m\|^{\alpha_m}. \\ &= \|p_1\|^{\alpha_1}\|p_2\|^{\alpha_2}\cdots\|p_m\|^{\alpha_m}. \\ &= 1\times 1\times\cdots\times 1. \\ &= 1.\end{aligned} \tag{1.2.13}$$

另一方面, 由定义*1.1.1*的第 *(1)* 条, 有

$$\|0\| = 0. \tag{1.2.14}$$

由命题*1.1.2*的性质 *(1)*, 有

$$\|1\| = 1. \tag{1.2.15}$$

由式 *(1.2.13)*, 式 *(1.2.14)*, 式 *(1.2.15)* 和命题*1.1.2*的性质 *(4)*, $\forall a = b/c \in \mathbb{Q}$, 其中 $b \in \mathbb{Z}$, $c \in \mathbb{Z}_{\neq 0}$, 有

$$\|a\| = \left\|\frac{b}{c}\right\| = \frac{\|b\|}{\|c\|} = \begin{cases}1,\ b \neq 0, \\ 0,\ b = 0.\end{cases} \tag{1.2.16}$$

式 *(1.2.16)* 意味着 $\|\bullet\|$ 是平凡赋值, 矛盾. 由反证法, 至少存在一个素数 p 满足 $\|p\| \neq 1$. 由式 *(1.2.11)*, 成立 $\|p\| < 1$.

(b) 第二步, 我们指出成立

$$p\mathbb{Z} = \{a \in \mathbb{Z} :\ \|a\| < 1\} =: I. \tag{1.2.17}$$

i. 首先我们证明 $p\mathbb{Z} \subseteq I$.

$\forall a = pb \in p\mathbb{Z} \subset \mathbb{Z}$, 其中 $b \in \mathbb{Z}$, 成立

$$\|a\| = \|pb\| = \|p\| \, \|b\| < 1 \times \|b\| \leq 1 \times 1 = 1.$$

于是有 $p\mathbb{Z} \subseteq I$.

ii. 然后我们证明 $I \subseteq p\mathbb{Z}$.

由引理*1.2.10*, I 是 $\mathbb{Z}$ 的双边理想; 由引理*1.2.11*, $p\mathbb{Z}$ 是 $\mathbb{Z}$ 的极大理想, 因此只能是 $I \subseteq p\mathbb{Z}$.

综上, 式 *(1.2.17)* 成立.

(c) 第三步, 我们指出成立

$$\|a\| = |a|_p^{\,s}, \ \forall a \in \mathbb{Z}, \ \exists s > 0. \tag{1.2.18}$$

将 a 中的素因子 p 提取出来, 即将 a 表为 $a = bp^m$, 其中 $m \in \mathbb{Z}_{\geq 0}$, $b \in \mathbb{Z}$, $p \nmid b$. 于是有 $b \notin p\mathbb{Z} = I$. 结合式 *(1.2.11)*, 得到 $\|b\| = 1$. 成立

$$\begin{aligned} \|a\| = \|bp^m\| &= \|b\| \, \|p\|^m = 1 \times \|p\|^m. \\ &= \left(p^{\log_p \|p\|}\right)^m = \left(p^{-m}\right)^{-\log\|p\|/\log p} = |a|_p^{\,-\log\|p\|/\log p}. \end{aligned}$$

由第一步, $\|p\| < 1$, 因此 $\exists s = -\log\|p\| / \log p > 0$, 使得式 *(1.2.18)* 成立.

(d) 第四步, 我们将第三步中的结论推广到有理数域 $\mathbb{Q}$ 的情况.

任取 $\forall a = b/c \in \mathbb{Q}$, 其中 $b \in \mathbb{Z}$, $c \in \mathbb{Z}_{\neq 0}$, 成立

$$\|a\| = \left\|\frac{b}{c}\right\| = \frac{\|b\|}{\|c\|} = \frac{|b|_p^{\,s}}{|c|_p^{\,s}} = \left(\frac{|b|_p}{|c|_p}\right)^s = \left|\frac{b}{c}\right|_p^{\,s} = |a|_p^{\,s},$$

其中 $s = -\log\|p\| / \log p$.

至此, 根据命题*1.1.13*, $\mathbb{Q}$ 上任一个非平凡的非阿基米德赋值 $\|\bullet\|$ 等价于某一个 p-进赋值 $|\bullet|_p$.

2. 我们再来讨论 $\mathbb{Q}$ 上阿基米德赋值的情况. $\forall a = m/n \in \mathbb{Q}$, 其中 $m \in \mathbb{Z}$, $n \in \mathbb{Z}_{\neq 0}$.

(a) 先关注 m, $n > 1$ 的情况.

由引理*1.2.12*, 可令

$$\|m\|^{1/\ln m} = \|n\|^{1/\ln n} = c_0. \tag{1.2.19}$$

由于 $m > 1$, $1/\ln m > 0$, $\|m\| > 0$, 有 $c_0 > 1$, 因此 $\exists s \in \mathbb{R}_{>0}$, 使得

$$e^s = c_0. \tag{1.2.20}$$

联立式 *(1.2.19)*, 式 *(1.2.20)*, 解得

$$\|m\| = e^{s\ln m}, \ \|n\| = e^{s\ln n}.$$

于是有

$$\|a\| = \left\|\frac{m}{n}\right\| = \frac{\|m\|}{\|n\|} = \frac{e^{s\ln m}}{e^{s\ln n}} = e^{s\ln\frac{m}{n}} = e^{s\ln a} = a^s,$$

其中 $a = m/n > 0$. 因此存在一常数 $s = \ln c_0 \in \mathbb{R}_{>0}$ 使得

$$\|a\| = |a|_\infty{}^s. \tag{1.2.21}$$

(b) 然后将式 *(1.2.21)* 的适用范围推广到 $m \geq 0,\ n \geq 1$. 只需要补充讨论以下情况.

i. 当 $m = 0$ 时, 由定义*1.1.1*, 自然有

$$\|0\| = 0 = |0|_\infty = |0|_\infty{}^s.$$

ii. 当 $m = n = 1$ 时, 由命题*1.1.2*性质 *(1)*, 有

$$\left\|\frac{1}{1}\right\| = \|1\| = 1 = |1|_\infty = |1|_\infty{}^s.$$

iii. 当 $m > 1$ 且 $n = 1$ 时, 有

$$\|a\| = \|m\| = e^{s\ln m} = m^s = |m|_\infty{}^s = |a|_\infty{}^s.$$

iv. 当 $m = 1$ 且 $n > 1$ 时, 有

$$\|a\| = \left\|\frac{1}{n}\right\| = \frac{\|1\|}{\|n\|} = \frac{1}{e^{s\ln n}} = \left(\frac{1}{n}\right)^s = \left|\frac{1}{n}\right|_\infty{}^s = |a|_\infty{}^s.$$

(c) 最后将式 *(1.2.21)* 的适用范围推广到 $a < 0$ 的情况.

当 $a < 0$ 时, 有 $-a > 0$, 由命题*1.1.2*的性质 *(3)*, 成立

$$\|a\| = \|-a\| = |-a|_\infty{}^s = |a|_\infty{}^s.$$

至此, 证得 $\forall a \in \mathbb{Q}, \exists s = \ln c_0 \in \mathbb{R}_{>0}$ 使得 $\|a\| = |a|_\infty{}^s$. 根据命题*1.1.13*, $\mathbb{Q}$ 上任一个阿基米德赋值 $\|\bullet\|$ 等价于普通赋值 $|\bullet|_\infty$. □

推论 1.2.14 (A. Ostrowski) 整数环 $\mathbb{Z}$ 上除去平凡赋值的任一非阿基米德赋值 $\|\bullet\|_{fa}$ 等价于某一个具有非阿基米德性的 p-进赋值 $|\bullet|_p$（p 是素数）, 任一阿基米德赋值 $\|\bullet\|_a$ 等价于具有阿基米德性的普通赋值 $|\bullet|_\infty$.

证明 基于推理

$$
\begin{aligned}
&\mathbb{Q}\text{上}\begin{cases}\|\bullet\|_{fa}\cong|\bullet|_p,\\ \|\bullet\|_a\cong|\bullet|_\infty.\end{cases}\\
\xRightarrow{\text{命题1.1.13}}&\begin{cases}\|x\|_{fa}<1.\Leftrightarrow|x|_p<1,\ \forall x\in\mathbb{Q},\\ \|x\|_a<1.\Leftrightarrow|x|_\infty<1,\ \forall x\in\mathbb{Q}.\end{cases}\\
\xRightarrow{\mathbb{Z}\subset\mathbb{Q}}&\begin{cases}\|x\|_{fa}<1.\Leftrightarrow|x|_p<1,\ \forall x\in\mathbb{Z},\\ \|x\|_a<1.\Leftrightarrow|x|_\infty<1,\ \forall x\in\mathbb{Z}.\end{cases}\\
\xRightarrow{\text{命题1.1.13}}&\mathbb{Z}\text{上}\begin{cases}\|\bullet\|_{fa}\cong|\bullet|_p,\\ \|\bullet\|_a\cong|\bullet|_\infty,\end{cases}
\end{aligned}
$$

该推论成立. □

由于赋值等价涉及到同一个环上的两个不同的赋值, 因此我们可以将赋值等价视为赋值间的一种二元关系. 设 $|\bullet|_1$, $|\bullet|_2$, $|\bullet|_3$ 是环 $\Re$ 上的赋值.

1. $\forall x\in\Re$, 显然有 $|x|_1<1.\Leftrightarrow|x|_1<1$, 由命题1.1.13, $|\bullet|_1$ 和 $|\bullet|_1$ 等价, 说明赋值等价具有**自反性**.
2. 显然 $|\bullet|_1\cong|\bullet|_2.\ \Leftrightarrow\ |\bullet|_2\cong|\bullet|_1$. 说明赋值等价具有**对称性**.
3. 若 $|\bullet|_1$ 与 $|\bullet|_2$ 等价, $|\bullet|_2$ 与 $|\bullet|_3$ 等价, 则成立

   $$|x|_1<1.\iff|x|_2<1.\iff|x|_3<1,$$

   由命题1.1.13, $|\bullet|_1$ 和 $|\bullet|_3$ 等价, 说明赋值等价具有**传递性**.

由此可见, 赋值等价可视为一种等价关系, 能够对一个环上的赋值进行分划, 产生等价类. 结合 Ostrowski 定理, 我们可对整数环 $\mathbb{Z}$ 上的所有赋值进行分划并得到下列等价类:

1. 单独一个平凡赋值 $|\bullet|_\clubsuit$ 构成的集合:

   $$\Upsilon_\clubsuit:=\left\{|\bullet|_\clubsuit\right\}.$$

2. 由 $\mathbb{Z}$ 上某些非平凡的非阿基米德赋值构成的集合 [4] :

   $$
   \begin{aligned}
   \Upsilon_2&:=\left\{|\bullet|:\ |\bullet|\cong|\bullet|_2\right\},\\
   \Upsilon_3&:=\left\{|\bullet|:\ |\bullet|\cong|\bullet|_3\right\},\\
   \Upsilon_5&:=\left\{|\bullet|:\ |\bullet|\cong|\bullet|_5\right\},\\
   \Upsilon_7&:=\left\{|\bullet|:\ |\bullet|\cong|\bullet|_7\right\},\\
   &\cdots\cdots\cdots\cdots
   \end{aligned}
   $$

   以上所有的 Υ_p 中的 p 是素数.

[4]这里并没有讨论不同 Υ_p 之间交集是否为空, 即是否存在素数 $p_1\neq p_2$, 而 Υ_{p_1} 和 Υ_{p_2} 是同个集合的问题, 但这无伤大雅, 此处略过.

3. 由 $\mathbb{Z}$ 上所有的阿基米德赋值构成的集合:

$$\Upsilon_\infty := \{|\bullet| : \ |\bullet| \cong |\bullet|_\infty\}.$$

至此, 本小节实现了整数环 $\mathbb{Z}$ 上的赋值在赋值等价意义下的范围收缩.

1.3 $\mathbb{Z}$ 的一种完备化结果

基于 § 1.1 节给出的赋值概念, 我们给出赋值意义下的柯西列定义.

定义 1.3.1 设 $\Re$ 是一个环, $|\bullet|$ 是 $\Re$ 上的一个赋值, $\{a_n\}_{n\in\mathbb{N}}$ 是 $\Re$ 中的一个序列. 称 $\{a_n\}_{n\in\mathbb{N}}$ 为环 $\Re$ 上的一个**关于赋值 $|\bullet|$ 的柯西列**, 若 $\forall\varepsilon>0$, $\exists N\in\mathbb{N}$, 使得

$$|a_n-a_m|<\varepsilon,\ \forall n,\ m\geq N.$$

例子 1.3.2 带 p-进赋值的整数环 $\left(\mathbb{Z},|\bullet|_p\right)$ 上的序列

$$1,\ p,\ p^2,\ p^3,\ \cdots,$$

是柯西列.

证明 不妨令 $m,\ n\in\mathbb{Z}_{\geq 0}$, $n>m$, 根据命题*1.1.4*, 成立

$$|p^n-p^m|_p\leq\max\left\{|p^n|_p,\ |-p^m|_p\right\}=p^{-m}.$$

$\forall\varepsilon>0$, 并限制 $\varepsilon<1$, 令 $p^{-m}<\varepsilon$, 得到 $-m<\log_p\varepsilon$ 即

$$m>-\log_p\varepsilon>0.$$

于是 $\exists N=\left[-\log_p\varepsilon\right]+1\in\mathbb{Z}_{>0}$, 成立

$$|p^n-p^m|_p<\varepsilon,\ \forall m,\ n\geq N.$$

由定义*1.3.1*, 序列 $\{p^n\}_{n\in\mathbb{Z}_{\geq 0}}$ 是一个柯西列. □

例子 1.3.3 带 p-进赋值的整数环 $\left(\mathbb{Z},|\bullet|_p\right)$ 上的序列

$$\sum_{v=0}^{0}a_vp^v,\ \sum_{v=0}^{1}a_vp^v,\ \sum_{v=0}^{2}a_vp^v,\ \cdots,\ \sum_{v=0}^{n}a_vp^v,\ \cdots,$$

其中 $\forall v\in\mathbb{Z}_{\geq 0}$, $a_v\in\{0,\ 1,\ \cdots,\ p-1\}$, 是一个柯西列.

证明 不妨令 $m,\ n\in\mathbb{Z}_{\geq 0}$, $n>m$. 根据推论*1.1.5*, 成立

$$\left|\sum_{v=0}^{n}a_vp^v-\sum_{v=0}^{m}a_vp^v\right|_p=\left|\sum_{v=m+1}^{n}a_vp^v\right|_p\leq\max_{m+1\leq v\leq n}\left\{|a_vp^v|_p\right\}.\tag{1.3.1}$$

由于 $a_v\in\{0,\ 1,\ \cdots,\ p-1\}$,

1. 当 $a_v\neq 0$ 时有

$$p^v\|\,a_vp^v.\implies|a_vp^v|_p=p^{-v}.$$

2. 当 $a_v=0$ 时有

$$|a_vp^v|_p=|0|_p=0.$$

由此成立

$$\max_{m+1\leq v\leq n}\left\{\left|a_vp^v\right|_p\right\}\leq\frac{1}{p^{m+1}}<\frac{1}{p^m}. \tag{1.3.2}$$

$\forall\varepsilon>0$ 并限制 $\varepsilon<1$ [5] , 令 $p^{-m}<\varepsilon$, 得到 $-m<\log_p\varepsilon$ 即

$$m>-\log_p\varepsilon>0.$$

于是由式 *(1.3.1)*, 式 *(1.3.2)*, $\exists N=\left[-\log_p\varepsilon\right]+1\in\mathbb{Z}_{>0}$, 成立

$$\left|\sum_{v=0}^{n}a_vp^v-\sum_{v=0}^{m}a_vp^v\right|_p<\varepsilon,\ \forall n,\ m\geq N.$$

根据定义*1.3.1*, $\left\{\sum_{v=0}^{n}a_vp^v\right\}_{n\in\mathbb{Z}_{\geq0}}$ 是一个柯西列. □

对于环 $\Re$ 上的一个序列 $\{a_n\}_{n\in\mathbb{N}}$ 的收敛性问题, 我们给出如下界定.

定义 1.3.4 设 $\Re$ 是一个环, $|\bullet|$ 是 $\Re$ 上的一个赋值, $\{a_n\}_{n\in\mathbb{N}}$ 是 $\Re$ 中的一个序列. 称 $\{a_n\}_{n\in\mathbb{N}}$ **关于赋值 $|\bullet|$ 是收敛的**, 若满足

$$\lim_{n\to\infty}|a_n-a|=0,\ \exists a\in\Re.$$

此时称 a 是序列 $\{a_n\}_{n\in\mathbb{N}}$ 的**收敛点**.

命题 1.3.5 设 $\{a_n\}_{n\in\mathbb{N}}$ 是 $(\Re,|\bullet|)$ 中的一个序列. 若 $\{a_n\}_{n\in\mathbb{N}}$ 收敛, 则其收敛点唯一.

证明 设 $r,\ s\in\Re$ 均为序列 $\{a_n\}_{n\in\mathbb{N}}$ 的收敛点, 则成立

$$0\leq|r-s|=|(r-a_n)+(a_n-s)|\leq|a_n-r|+|a_n-s|\to0+0=0\ \ (n\to\infty),$$

上式蕴含了 $r-s=0$ 即 $r=s$. □

例子 1.3.6 带 p-进赋值的整数环 $\left(\mathbb{Z},|\bullet|_p\right)$ 上的序列

$$1,\ p,\ p^2,\ p^3,\ \cdots.$$

是收敛的.

证明 由于

$$\lim_{n\to\infty}|p^n-0|_p=\lim_{n\to\infty}|p^n|_p=\lim_{n\to\infty}p^{-n}=0.$$

因此序列 $\{p^n\}_{n\in\mathbb{Z}_{\geq0}}$ 是收敛的, 收敛点是 0. □

根据定义1.3.4, 带赋值的环 $(\Re,|\bullet|)$ 上的一个序列 $\{a_n\}_{n\in\mathbb{N}}$ 如果不收敛, 则可能是不存在收敛点, 或者存在收敛点 a 但是 $a\notin\Re$. 为了帮助理解, 以下给出几个具体的例子.

[5] $\varepsilon<1$ 下的结果也能满足 $\varepsilon\geq1$ 的情况.

例子 1.3.7 (收敛点在环外) 考虑定义域是带普通赋值有理数域 $(\mathbb{Q}, |\bullet|_\infty)$ 的函数

$$f(x) = x^2 - 2.$$

我们通过二分法 *[11, 第五章 § 2]* 创建一个无限逼近 f 在 $x > 0$ 的零点

$$\sqrt{2} = 1.4142135623731\cdots$$

的一个有理小数序列 $\{a_n\}_{n\in\mathbb{N}}$.

由于 $f(1) = -1 < 0$, $f(2) = 2 > 0$, 因此将二分法的初始区间定为 $(1, 2)$. 执行二分法得到有理小数逼近值序列 $\{a_n\}_{n\in\mathbb{N}}$ 的过程用表格表示如下.

k	a_k	b_k	x_k	$f(x_k)$	a_k
1	1	2	$\frac{1+2}{2} = 1.5$	0.25	1
2	1	1.5	$\frac{1+1.5}{2} = 1.25$	-0.4375	1.25
3	1.25	1.5	$\frac{1.25+1.5}{2} = 1.375$	-0.1094	1.375
4	1.375	1.5	$\frac{1.375+1.5}{2} = 1.4375$	0.0664	1.4375
5	1.375	1.4375	$\frac{1.375+1.4375}{2} = 1.40625$	-0.0225	1.40625
6	1.40625	1.4375	$\frac{1.40625+1.4375}{2} = 1.421875$	0.0217	1.421875
7	1.40625	1.421875	$\frac{1.40625+1.421875}{2} = 1.4140625$	-0.0004	1.4140625
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

显然, 序列

$$1,\ 1.25,\ 1.375,\ 1.4375,\ 1.40625,\ 1.421875,\ 1.4140625,\ \cdots$$

是有理数域 $(\mathbb{Q}, |\bullet|_\infty)$ 上的序列, $\sqrt{2}$ 是该序列的收敛点, 但是 $\sqrt{2} \notin \mathbb{Q}$, 因此该序列是不收敛的.

例子 1.3.8 (收敛点不存在) 带普通赋值的有理数域 $(\mathbb{Q}, |\bullet|_\infty)$ 上的序列

$$1,\ p,\ p^2,\ p^3,\ \cdots,$$

是不收敛的.

证明 $\forall x \in \mathbb{Q}$, 由于素数 $p > 1$, 成立

$$\infty \leftarrow \left||p|_\infty^{\,n} - |x|_\infty\right|_\infty \le |p^n - x|_\infty \le |p|_\infty^{\,n} + |x|_\infty \to \infty \ (n \to \infty),$$

由极限的迫敛性 *[7, 第二章 § 2]*, 有

$$\lim_{n\to\infty} |p^n - x|_\infty = \infty \neq 0,$$

即 $\mathbb{Q}$ 上的任一点都不是序列 $\{p^n\}_{n\in\mathbb{Z}_{\ge 0}}$ 的收敛点. 因此序列 $\{p^n\}_{n\in\mathbb{Z}_{\ge 0}}$ 是不收敛的. □

例子 1.3.9 (收敛点不存在) 带 p-进赋值 $(p > 2)$ 的有理数域 $\left(\mathbb{Q}, |\bullet|_p\right)$ 上的序列

$$\sum_{v=0}^{0} a_v p^v,\ \sum_{v=0}^{1} a_v p^v,\ \sum_{v=0}^{2} a_v p^v,\ \cdots,\ \sum_{v=0}^{n} a_v p^v,\ \cdots,$$

其中 $\forall v \in \mathbb{Z}_{\ge 0}$, $a_v \in \{0,\ 1,\ \cdots,\ p-1\}$, 不是收敛的.

证明 我们指出总有

$$\lim_{n\to\infty}\left|\sum_{v=0}^{n}a_vp^v-x\right|_p\neq 0,\ \forall x\in\mathbb{Q}. \tag{1.3.3}$$

事实上, $\forall x=b/c\in\mathbb{Q}$, 其中 $b\in\mathbb{Z}$, $c\in\mathbb{Z}_{\neq 0}$, 先将 $b<\infty$ 表为 p-进数形式

$$b=b_0+b_1p+b_2p^2\cdots+b_sp^s,$$

其中 $b_0,\ b_1,\ \cdots,\ b_m\in\{0,\ \pm1,\ \cdots,\ \pm(p-1)\}$（当 $b>0$ 时均取非负数, 当 $b<0$ 时均取非正数）, $s\in\mathbb{Z}_{\geq 0}$. 将 c 中的素因子 p 提取出来, 得到 $c=p^rc'$, 其中 $r\in\mathbb{Z}_{\geq 0}$. 于是可以将 x 表为

$$x=\frac{1}{c'}\left(b_0p^{-r}+b_1p^{-r+1}+b_2p^{-r+2}+\cdots+b_sp^{-r+s}\right).$$

1. 若 $-r+s<0$ 即 $r>s$, 则有

$$\left|\sum_{v=0}^{n}a_vp^v-x\right|_p=\left|\sum_{u=0}^{s}\frac{-b_u}{c'}p^{-r+u}+\sum_{v=0}^{n}a_vp^v\right|_p. \tag{1.3.4}$$

由于 $a_v,\ |b_u|_\infty\in\{0,\ 1,\ \cdots,\ p-1\}$, $\gcd(a_v,p)=1$, $\gcd(b_u,p)=1$, $\gcd(c',p)=1$, 因此有

$$\left|\frac{-b_u}{c'}p^{-r+u}\right|_p=p^{r-u},\ |a_vp^v|=p^{-v}.$$

由推论*1.1.7*, 有

$$\left|\sum_{u=0}^{s}\frac{-b_u}{c'}p^{-r+u}+\sum_{v=0}^{n}a_vp^v\right|_p=\max_{\substack{0\leq u\leq s\\0\leq v\leq n}}\left\{p^{r-u},\ p^{-v}\right\}=p^r, \tag{1.3.5}$$

由式 *(1.3.4), (1.3.5)*, 即有

$$\left|\sum_{v=0}^{n}a_vp^v-x\right|_p=p^r\to p^r\neq 0\ \ (n\to\infty). \tag{1.3.6}$$

2. 若 $-r+s\geq 0$ 即 $r\leq s$, 不妨限制 $n>-r+s$, 则有

$$\left|\sum_{v=0}^{n}a_vp^v-x\right|_p=\left|\sum_{w=0}^{r-1}\frac{-b_w}{c'}p^{-r+w}+\sum_{v=0}^{-r+s}\left(a_v-\frac{b_{r+v}}{c}\right)p^v+\sum_{u=-r+s+1}^{n}a_up^u\right|_p, \tag{1.3.7}$$

其中

$$\mathbb{Z}\ni\left|\sum_{v=0}^{-r+s}\left(a_v-\frac{b_{r+v}}{c}\right)p^v\right|_\infty\leq\sum_{v=0}^{-r+s}2(p-1)p^v<2p^{-r+s+1}.$$

又 $p>2$, 这意味着

$$\frac{1}{p^{s-r}}<\left|\sum_{v=0}^{-r+s}\left(a_v-\frac{b_{r+v}}{c}\right)p^v\right|_p\leq 1.$$

由推论*1.1.7*, 有

$$\begin{aligned}&\left|\sum_{w=0}^{r-1}\frac{-b_w}{c'}p^{-r+w}+\sum_{v=0}^{-r+s}\left(a_v-\frac{b_{r+v}}{c}\right)p^v+\sum_{u=-r+s+1}^{n}a_up^u\right|_p\\&=\max_{\substack{0\le w\le r-1\\-r+s+1\le u\le n}}\left\{p^{r-w},\ \left|\sum_{v=0}^{-r+s}\left(a_v-\frac{b_{r+v}}{c}\right)p^v\right|_p,\ p^{-u}\right\}\\&=p^r.\end{aligned}\tag{1.3.8}$$

由式 *(1.3.7), (1.3.8),* 此时也成立式 *(1.3.6).*

综上两点, 式 *(1.3.3)* 成立, $\mathbb{Q}$ 上的任一点都不是序列 $\{\sum_{v=0}^{n}a_vp^v\}_{n\in\mathbb{Z}_{\ge0}}$ 的收敛点, 该序列是不收敛的. □

基于环上柯西列的定义和环上序列收敛的定义, 我们界定一个环的完备性如下.

定义 1.3.10 设 $\Re$ 是一个环, $|\bullet|$ 是 $\Re$ 上的一个赋值. 称 $\Re$ **关于赋值** $|\bullet|$ **具有完备性**, 若 $\Re$ 上的任一个柯西列 $\{a_n\}_{n\in\mathbb{N}}$ 关于赋值 $|\bullet|$ 是收敛的. 此时也称 $\Re$ 是一个**完备环**.

有了完备性的定义后, 我们来研究整数环 $\mathbb{Z}$ 在不同的赋值 $|\bullet|$ 下是否是完备的. 首先, 我们研究带平凡赋值的整数环 $\left(\mathbb{Z},|\bullet|_{\clubsuit}\right)$.

命题 1.3.11 带平凡赋值的整数环 $\left(\mathbb{Z},|\bullet|_{\clubsuit}\right)$ 是完备的.

证明 由平凡赋值的定义*1.2.1,*

$$|x|_{\clubsuit}=\begin{cases}1,\ x\neq0,\\0,\ x=0.\end{cases}\tag{1.3.9}$$

在 $\left(\mathbb{Z},|\bullet|_{\clubsuit}\right)$ 中任取一个柯西列 $\{a_n\}_{n\in\mathbb{N}}$, 令 $\varepsilon_0\in(0,1)$, 由柯西列的定义*1.3.1,* $\exists N\in\mathbb{N}$, 使得

$$|a_n-a_m|_{\clubsuit}<\varepsilon_0,\ \forall m,\ n\ge N.\tag{1.3.10}$$

式 *(1.3.10)* 中令 $m=N$, 得到

$$|a_n-a_N|_{\clubsuit}<\varepsilon_0<1,\ \forall n\ge N.$$

结合式 *(1.3.9),* 得到

$$a_n-a_N=0.\implies a_n=a_N,\ \forall n\ge N,$$

即序列 $\{a_n\}_{n\ge N}$ 是一个常数列, 显然柯西列 $\{a_n\}_{n\in\mathbb{N}}$ 收敛, 收敛点为 a_N. 由 $\{a_n\}_{n\in\mathbb{N}}$ 的任意性, $\left(\mathbb{Z},|\bullet|_{\clubsuit}\right)$ 是完备的. □

然后, 我们研究带阿基米德赋值的整数环 $(\mathbb{Z},|\bullet|)$ 的完备性. 基于 § 1.2 节得到的 Ostrowski 定理, $|\bullet|$ 和 $\mathbb{Z}$ 上的普通赋值 $|\bullet|_\infty$ 是等价的. 于是我们在赋值等价的联系下只需要研究带普通赋值的整数环 $(\mathbb{Z},|\bullet|_\infty)$ 即可.

命题 1.3.12 带普通赋值的整数环 $(\mathbb{Z}, |\bullet|_\infty)$ 是完备的.

证明 整数环 $\mathbb{Z}$ 是离散的, 即 $\forall x,\ y \in \mathbb{Z}$, 成立

$$|x-y|_\infty = \begin{cases} 0, & x = y, \\ \geq 1, & x \neq y. \end{cases} \tag{1.3.11}$$

在 $(\mathbb{Z}, |\bullet|_\infty)$ 中任取一个柯西列 $\{a_n\}_{n\in\mathbb{N}}$, 令 $\varepsilon_0 \in (0,1)$, 由柯西列的定义*1.3.1*, $\exists N \in \mathbb{N}$, 使得

$$|a_n - a_m|_\infty < \varepsilon_0,\ \forall m,\ n \geq N. \tag{1.3.12}$$

式 *(1.3.12)* 中令 $m = N$, 得到

$$|a_n - a_N| < \varepsilon_0,\ \forall n \geq N.$$

结合式 *(1.3.11)*, 得到

$$a_n - a_N = 0. \implies a_n = a_N,\ \forall n \geq N,$$

即序列 $\{a_n\}_{n\geq N}$ 是一个常数列, 显然柯西列 $\{a_n\}_{n\in\mathbb{N}}$ 收敛, 收敛点为 a_N. 由 $\{a_n\}_{n\in\mathbb{N}}$ 的任意性, $(\mathbb{Z}, |\bullet|_\infty)$ 是完备的. □

最后, 我们研究带非平凡的非阿基米德赋值的整数环 $(\mathbb{Z}, |\bullet|)$ 的完备性. 同样基于 § 1.2 节得到的 Ostrowski 定理, $|\bullet|$ 和 $\mathbb{Z}$ 上的某一个 p-进赋值 $|\bullet|_p$ 是等价的. 于是我们在赋值等价的联系下只需要研究带 p-进赋值的整数环 $\left(\mathbb{Z}, |\bullet|_p\right)$ 即可. 而这次得出的结果与前两种的截然相反.

命题 1.3.13 $\left(\mathbb{Z}, |\bullet|_p\right)$ 不是完备的.

证明 这里只对 $p > 2$ 的情况作出讨论 [6] . 对于 $\left(\mathbb{Z}, |\bullet|_p\right) \subset \left(\mathbb{Q}, |\bullet|_p\right)$ 上的序列

$$\sum_{v=0}^{0} a_v p^v,\ \sum_{v=0}^{1} a_v p^v,\ \sum_{v=0}^{2} a_v p^v,\ \cdots,\ \sum_{v=0}^{n} a_v p^v,\ \cdots,$$

其中 $\forall v \in \mathbb{Z}_{\geq 0}$, $a_v \in \{0,\ 1,\ \cdots,\ p-1\}$, 例子*1.3.3*说明了该序列是柯西列; 例子*1.3.9*说明了该序列是不收敛的. 因此由定义*1.3.10*, $\left(\mathbb{Z}, |\bullet|_p\right)$ 不是完备的. □

对于一个不完备的环 $\mathfrak{R}$, 我们可以在其中添加其他元素, 使得原来没有收敛点的柯西列出现收敛点, 或者使得原来收敛点在环外的柯西列的收敛点在扩充后的环内, 同时保证新产生的柯西列也是收敛的. 有关该过程的数学概念的严格定义如下.

定义 1.3.14 设 $|\bullet|$, $|\bullet|_\bigstar$ 分别是环 $\mathfrak{R}$, $\mathfrak{R}_\bigstar$ 上的赋值, 称 $\mathfrak{R}_\bigstar$ 是 $\mathfrak{R}$ 的**完备化**, 若同时满足:

1. (环嵌入意义下) $\mathfrak{R} \subseteq \mathfrak{R}_\bigstar$;

[6] 只要将例子1.3.9中的序列中的所有 a_v 再限制 $a_v < p-1$, 即可用来证明 $p = 2$ 的情况. 具体细节读者可以仿例1.3.9的过程进行推演.

2.（环嵌入意义下）$\mathfrak{R}_\bigstar$ 上的赋值 $|\bullet|_\bigstar$ 在 $\mathfrak{R}$ 中的表现恰好就是 $|\bullet|$, 记为 $|\bullet|_\bigstar\Big|_{\mathfrak{R}} = |\bullet|$;

3. $\mathfrak{R}_\bigstar$ 关于赋值 $|\bullet|_\bigstar$ 是完备的.

注记 该定义中并没有要求 $(\mathfrak{R}, |\bullet|)$ 是不完备的, 因此我们可以将一个本身完备的环再作进一步的完备化, 得到一个依然完备的扩充环. 例如, 由命题*1.3.12*, $(\mathbb{Z}, |\bullet|_\infty)$ 是完备的, 而 $(\mathbb{R}, |\bullet|_\infty)$ 或者 $(\mathbb{C}, |\bullet|_\infty)$ 都可以作为其进一步的完备化.

而对于完备化的构造手段, 参考 Fesenko [2, Proposition 4.2], 我们指出可以通过构建一个特别的商环来表示带赋值 $|\bullet|$ 的环 $\mathfrak{R}$ 的完备化. 具体地说, 记

$$\mathfrak{C} := \left\{\{a_n\} : \{a_n\}是\mathfrak{R}中的柯西列\right\},$$
$$\mathfrak{m} := \left\{\{a_n\} : \lim_{n\to\infty} |a_n| = 0\right\}.$$

得到一个带赋值 $|\bullet|_\bigstar$ [7] 的商环 [8] $(\mathfrak{C}/\mathfrak{m})$, 其中

$$\mathfrak{C}/\mathfrak{m} = \left\{\{a_n\} + \mathfrak{m} : \{a_n\}是\mathfrak{R}中的柯西列\right\},$$
$$|x|_\bigstar := \lim_{n\to\infty} |a_n| \in \mathbb{R}_{\geq 0},\ \forall x = \{a_n\} + \mathfrak{m} \in \mathfrak{C}/\mathfrak{m}.$$

有如下的定理.

定理 1.3.15 $\left(\mathfrak{C}/\mathfrak{m}, |\bullet|_\bigstar\right)$ 是 $(\mathfrak{R}, |\bullet|)$ 的完备化.

证明

1. 首先我们考虑如何将环 $\mathfrak{R}$ 嵌入到商环 $\mathfrak{C}/\mathfrak{m}$ 中. 可以将环 $\mathfrak{R}$ 中的元素 a 同 $\mathfrak{C}/\mathfrak{m}$ 中的剩余类 $\{a\} + \mathfrak{m}$ 联系起来, 得到嵌入 φ:

$$\varphi : \begin{array}{ccc} \mathfrak{R} & \mapsto & \mathfrak{C}/\mathfrak{m} \\ a & \mapsto & \{a\} + \mathfrak{m} \end{array},$$

其中 $\{a\} + \mathfrak{m}$ 实质上就是

$$\left\{\{a_n\} : \{a_n\}是\mathfrak{R}中收敛到a的柯西列\right\}.$$

因此我们建立起环 $\mathfrak{R}$ 与 $\mathfrak{C}/\mathfrak{m}$ 的子环 $\wp := \{\{a\} + \mathfrak{m} : a \in \mathfrak{R}\} \subseteq \mathfrak{C}/\mathfrak{m}$ 的同构. 定义*1.3.14*的条件 *(1)* 满足. 在此意义上, $\forall \{a\} + m \in \wp$, 有

$$|\{a\} + m|_\bigstar = \lim_{n\to\infty} |a| = |a|.$$

定义*1.3.14*的条件 *(2)* 满足.

2. 任取 $\mathfrak{C}/\mathfrak{m}$ 中的一个柯西列

$$\left\{\left\{a_n^{(m)}\right\}_{n\in\mathbb{N}} + \mathfrak{m}\right\}_{m\in\mathbb{N}} = \left\{a_n^{(1)}\right\} + \mathfrak{m},\ \left\{a_n^{(2)}\right\} + \mathfrak{m},\ \cdots,\ \left\{a_n^{(m)}\right\} + \mathfrak{m},\ \cdots,$$

我们指出该柯西列一定收敛, 满足定义*1.3.14*的条件 *(3)*.

[7] 有关 $|\bullet|_\bigstar$ 的存在性, 良定义问题以及 $|\bullet|_\bigstar$ 确实是一个赋值结构的问题分别参见附录A.2的命题A.2.3, 命题A.2.4, 命题A.2.5.

[8] 事实上, $\mathfrak{C}$ 是一个含幺交换环, $\mathfrak{m}$ 是 $\mathfrak{C}$ 的双边理想, 具体参见附录A.2的命题A.2.1和命题A.2.2.

(a) 现在我们来尝试构造出它的收敛点.

- 对 $m=1$, 由于 $\left\{a_n^{(1)}\right\}$ 是柯西列, 因此 $\exists s_1 \in \mathbb{N}$, 使得

$$\left|a_n^{(1)} - a_m^{(1)}\right| < \frac{1}{1} = 1,\ \forall m,\ n \geq s_1.$$

  并令 $s(1) = s_1$.
- 对 $m=2$, 由于 $\left\{a_n^{(2)}\right\}$ 是柯西列, 因此 $\exists s_2 \in \mathbb{N}$, 使得

$$\left|a_n^{(2)} - a_m^{(2)}\right| < \frac{1}{2},\ \forall m,\ n \geq s_2.$$

  并令 $s(2) = \max\{s_2,\ s(1)+1\}$.
- ……
- 对 $m=k$, 由于 $\left\{a_n^{(k)}\right\}$ 是柯西列, 因此 $\exists s_k \in \mathbb{N}$, 使得

$$\left|a_n^{(k)} - a_m^{(k)}\right| < \frac{1}{k},\ \forall m,\ n \geq s_k.$$

  并令 $n(k) = \max\{s_k,\ s(k-1)+1\}$.
- ……

由此我们得到了一个序列

$$\left\{a_{s(k)}^{(k)}\right\}_{k\in\mathbb{N}} = a_{s(1)}^{(1)},\ a_{s(2)}^{(2)},\ \cdots,\ a_{s(k)}^{(k)},\ \cdots,$$

其中 $s(1) < s(2) < s(3) < \cdots$, 且 $s(k) \geq k,\ \forall k \in \mathbb{N}$.

(b) 我们将证明 $\left\{a_{s(k)}^{(k)}\right\}_{k\in\mathbb{N}}$ 是一个柯西列, 即有 $\left\{a_{s(k)}^{(k)}\right\}_{k\in\mathbb{N}} \in \mathfrak{C}$.

i. 一方面, 由上面的构造过程, $\forall N \in \mathbb{N}$, 成立

$$\left|a_n^{(N)} - a_m^{(N)}\right| < \frac{1}{N},\ \forall m,\ n \geq s(N). \tag{1.3.13}$$

$\forall \varepsilon > 0$, $\exists M_1 \in \mathbb{N}$, 使得 $1/M_1 < \varepsilon/2$. $\forall i \geq M_1$, 由式 *(1.3.13)*, 成立

$$\left|a_n^{(i)} - a_m^{(i)}\right| < \frac{1}{i} \leq \frac{1}{M_1} < \frac{\varepsilon}{2},\ \forall m,\ n \geq s(i). \tag{1.3.14}$$

再规定 $j \geq i$, 则有 $s(j) \geq s(i)$, 替换掉式 *(1.3.14)* 中的 m, n, 得到

$$\left|a_{s(i)}^{(i)} - a_{s(j)}^{(i)}\right| < \frac{\varepsilon}{2},\ \forall j \geq i \geq M_1. \tag{1.3.15}$$

ii. 另一方面, $\left\{\left\{a_n^{(m)}\right\}_{n\in\mathbb{N}} + \mathfrak{m}\right\}_{m\in\mathbb{N}}$ 是 $\mathfrak{C}/\mathfrak{m}$ 中关于赋值 $|\cdot|_\bigstar$ 的柯西列, 即 $\forall \varepsilon > 0$, $\exists M_2 \in \mathbb{N}$, 使得

$$\left|\left\{a_n^{(i)} - a_n^{(j)}\right\} + \mathfrak{m}\right|_\bigstar = \lim_{n\to\infty}\left|a_n^{(i)} - a_n^{(j)}\right| < \frac{\varepsilon}{2},\ \forall i,\ j \geq M_2. \tag{1.3.16}$$

式 *(1.3.16)* 中令 $n = s(j)$, 即有

$$\lim_{s(j)\to\infty}\left|a_{s(j)}^{(i)} - a_{s(j)}^{(j)}\right| < \frac{\varepsilon}{2},\ \forall i,\ j \geq M_2. \tag{1.3.17}$$

式 *(1.3.17)* 蕴含 $\exists M_3 \in \mathbb{N}$, 使得

$$\left|a_{s(j)}^{(i)} - a_{s(j)}^{(j)}\right| < \frac{\varepsilon}{2},\ \forall s\left(j\right) \geq M_3,\ \forall i,\ j \geq M_2.$$

规定 $j \geq i \geq \max\left\{M_2,\ M_3\right\}$, 则有 $s\left(j\right) \geq s\left(M_3\right) \geq M_3$, 成立

$$\left|a_{s(j)}^{(i)} - a_{s(j)}^{(j)}\right| < \frac{\varepsilon}{2},\ \forall j \geq i \geq \max\left\{M_2,\ M_3\right\}. \tag{1.3.18}$$

iii. 综上, 由式 *(1.3.15)* 和式 *(1.3.18)*, $\forall \varepsilon > 0$, $\exists M = \max\left\{M_1,\ M_2,\ M_3\right\}$, 成立

$$\begin{aligned}
&\left|a_{s(i)}^{(i)} - a_{s(j)}^{(j)}\right| \\
=&\left|\left(a_{s(i)}^{(i)} - a_{s(j)}^{(i)}\right) + \left(a_{s(j)}^{(i)} - a_{s(j)}^{(j)}\right)\right| \\
\leq&\left|a_{s(i)}^{(i)} - a_{s(j)}^{(i)}\right| + \left|a_{s(j)}^{(i)} - a_{s(j)}^{(j)}\right| \\
<&\frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,\ \forall j \geq i \geq M.
\end{aligned}$$

即 $\left\{a_{s(k)}^{(k)}\right\}_{k\in\mathbb{N}}$ 是一个柯西列, $\left\{a_{s(k)}^{(k)}\right\}_{k\in\mathbb{N}} \in \mathfrak{C}$.

(c) 我们将证明 $\left\{a_{s(m)}^{(m)}\right\}_{m\in\mathbb{N}} + \mathfrak{m}$ 是 $\mathfrak{C}/\mathfrak{m}$ 中柯西列 $\left\{\left\{a_n^{(m)}\right\}_{n\in\mathbb{N}} + \mathfrak{m}\right\}_{m\in\mathbb{N}}$ 的收敛点.

事实上, 由于

$$\left|a_n^{(m)} - a_{s(m)}^{(m)}\right| < \frac{1}{m},\ \forall n \geq s\left(m\right).$$

因此成立

$$0 \leq \left|\left\{a_n^{(m)} - a_{s(m)}^{(m)}\right\} + \mathfrak{m}\right|_\bigstar = \lim_{n\to\infty}\left|a_n^{(m)} - a_{s(m)}^{(m)}\right| \leq \frac{1}{m} \to 0\ \left(m \to \infty\right),$$

即有

$$\begin{aligned}
&\lim_{m\to\infty}\left|\left\{a_n^{(m)} - a_{s(m)}^{(m)}\right\} + \mathfrak{m}\right|_\bigstar = 0. \\
\Longleftrightarrow&\lim_{m\to\infty}\left|\left(\left\{a_n^{(m)}\right\} + \mathfrak{m}\right) - \left(\left\{a_{s(m)}^{(m)}\right\} + \mathfrak{m}\right)\right|_\bigstar = 0.
\end{aligned}$$

至此, 明所欲证. □

定理 1.3.16 $\left(\Re, |\cdot|\right)$ 的完备化在环同构意义下只有 $\left(\mathfrak{C}/\mathfrak{m}, |\cdot|_\bigstar\right)$ 一种.

证明 参见 *Fesenko [2, Proposition 4.2].* □

环 $\left(\Re, |\cdot|\right)$ 的完备化 $\left(\mathfrak{C}/\mathfrak{m}, |\cdot|_\bigstar\right)$ 通常不能给出一个比较清晰的代数结构. 为了完备化结果的直观表达, 我们引入下面的定义和引理.

定义 1.3.17 设 $\Re$ 是一个环, 给定 $\Re$ 的一个双边理想降链

$$\Re = I_0 \supseteq I_1 \supseteq \cdots \supseteq I_n \supseteq \cdots,$$

则一定存在满射环同态

$$\Re/I_1 \xleftarrow{\lambda_1} \Re/I_2 \xleftarrow{\lambda_2} \Re/I_3 \xleftarrow{\lambda_3} \cdots,$$

称

$$\varprojlim_n \Re/I_n := \left\{ (x_n)_{n\in\mathbb{N}} \in \prod_{n=1}^{\infty} \Re/I_n :\ \lambda_n(x_{n+1}) = x_n,\ n = 1, 2, \cdots \right\}$$

为环 $\Re/I_n$ 的**投影极限**，其中

$$\prod_{n=1}^{\infty} \Re/I_n = \left\{ (x_n)_{n\in\mathbb{N}} :\ x_n \in \Re/I_n \right\}.$$

引理 1.3.18 投影极限 $\varprojlim_n \Re/I_n$ 一定存在且在同构意义下是唯一的.

证明 参见 *Enochs [1, Definition 1.6.9 和 Theorem 1.6.10].* □

引理 1.3.19 环 $\Re$ 关于赋值 $|\bullet|$ 的完备化 $\mathfrak{C}/\mathfrak{m}$ 与 $\Re$ 的投影极限 $\varprojlim_n \Re/I_n$ 存在环同构, 即成立

$$\varprojlim_n \Re/I_n \xrightarrow{\sim} \mathfrak{C}/\mathfrak{m}.$$

证明 参见 *Enochs [1, Theorem 1.6.7].* □

基于此, 不妨在带 p-进赋值的整数环 $\left(\mathbb{Z}, |\bullet|_p\right)$ 中选择以下的一个理想降链 [9]

$$\mathbb{Z} \supseteq p\mathbb{Z} \supseteq p^2\mathbb{Z} \supseteq \cdots \supseteq p^n\mathbb{Z} \supseteq \cdots,$$

于是由引理1.3.19, $\left(\mathbb{Z}, |\bullet|_p\right)$ 的完备化结果可以表示成

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \left\{ (x_n)_{n\in\mathbb{N}} :\ x_n \in \{0,\ 1,\ \cdots,\ p^n - 1\},\ \lambda_n(x_{n+1}) = x_n \right\}$$

称为 $\left(\mathbb{Z}, |\bullet|_p\right)$ 的p-**进完备化**. 其上的加法 $+$ 和乘法 $\times$ 的定义为

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} := (a_n + b_n \mod p^n)_{n\in\mathbb{N}},$$
$$(a_n)_{n\in\mathbb{N}} \times (b_n)_{n\in\mathbb{N}} := (a_n \times b_n \mod p^n)_{n\in\mathbb{N}}.$$

其上的赋值 $|\bullet|_\bigstar$ 的定义为

$$\left|(x_n)_{n\in\mathbb{N}}\right|_\bigstar := \lim_{n\to\infty} |x_n|_p.$$

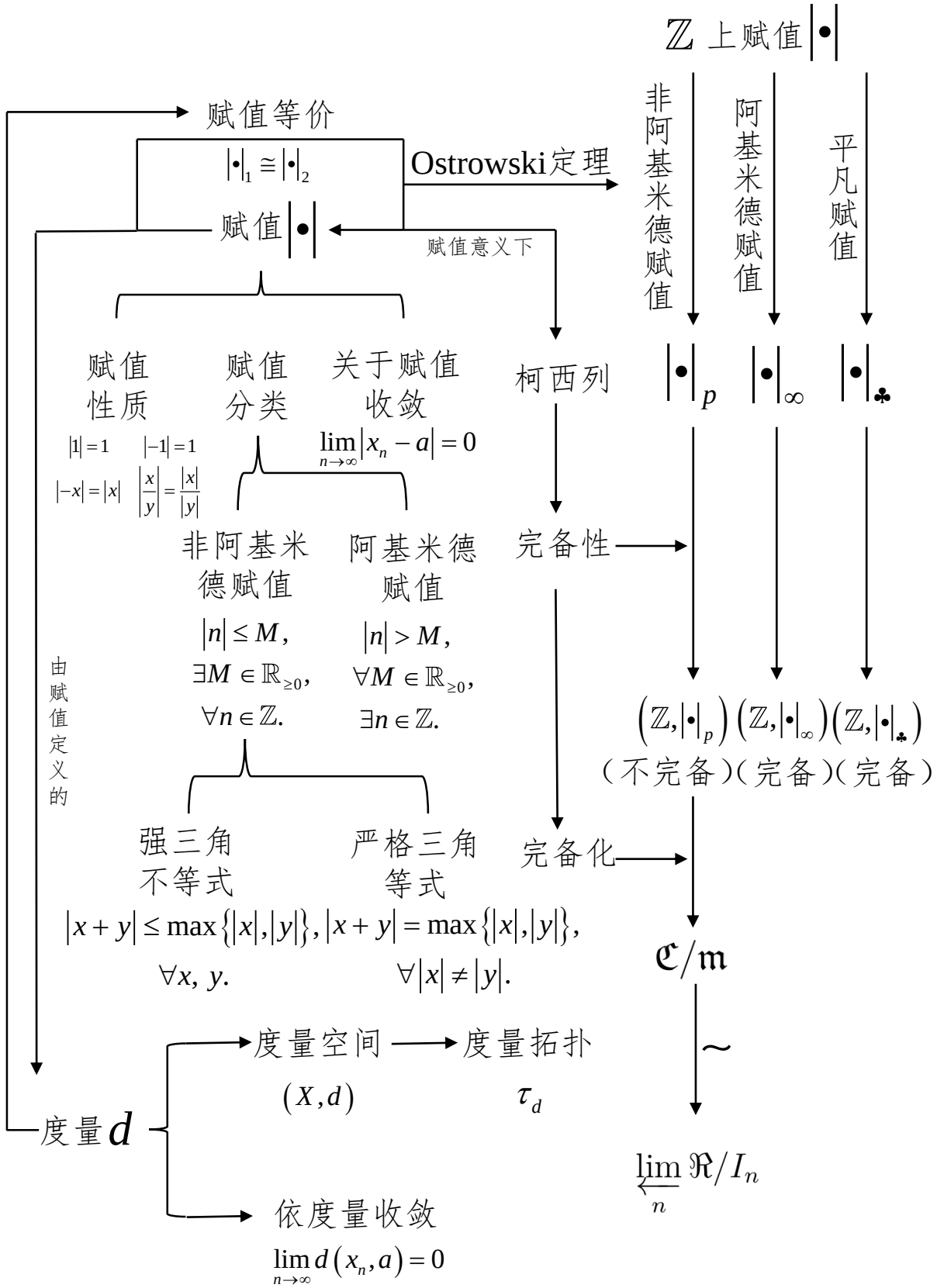
且由定理1.3.16和引理1.3.18, 在同构意义下该表示是唯一的.

至此, 我们得到了 $\left(\mathbb{Z}, |\bullet|_p\right)$ 完备化的一种比较清晰的结构表示:

$$\left(\varprojlim_n \mathbb{Z}/p^n\mathbb{Z},\ |\bullet|_\bigstar\right).$$

[9] 这种选取方法的妙处在后续的介绍中会有所体现.

1.4 本节小结


$\mathbb{Z}$ 上赋值 $|\bullet|$
非阿基米德赋值
阿基米德赋值
平凡赋值
赋值等价
$|\bullet|_1 \cong |\bullet|_2$
Ostrowski定理
赋值 $|\bullet|$
赋值意义下
赋值性质
赋值分类
关于赋值收敛
$\lim_{n\to\infty}|x_n - a| = 0$
$|1|=1$ $|-1|=1$
$|-x|=|x|$ $\left|\frac{x}{y}\right|=\frac{|x|}{|y|}$
柯西列
$|\bullet|_p$ $|\bullet|_\infty$ $|\bullet|_\clubsuit$
非阿基米德赋值
$|n| \le M,$
$\exists M \in \mathbb{R}_{\ge 0},$
$\forall n \in \mathbb{Z}.$
阿基米德赋值
$|n| > M,$
$\forall M \in \mathbb{R}_{\ge 0},$
$\exists n \in \mathbb{Z}.$
完备性
由赋值定义的
$\left(\mathbb{Z},|\bullet|_p\right)$ $\left(\mathbb{Z},|\bullet|_\infty\right)$ $\left(\mathbb{Z},|\bullet|_\clubsuit\right)$
（不完备）（完备）（完备）
强三角不等式
严格三角等式
$|x+y| \le \max\{|x|,|y|\},$
$\forall x, y.$
$|x+y| = \max\{|x|,|y|\},$
$\forall |x| \ne |y|.$
完备化
$\mathfrak{C}/\mathfrak{m}$
$\sim$
$\varprojlim_n \Re/I_n$
度量空间
(X,d)
度量拓扑
τ_d
度量 d
依度量收敛
$\lim_{n\to\infty} d(x_n, a) = 0$

2 Witt 向量引入

§ 1 节得到的 $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ 中的每个元素是一个可数无穷序列 $(x_n)_{n\in\mathbb{N}}$, 代数结构比较清晰, 但是序列中任何两个不同的元素 x_i, x_j 包含了重叠的信息. 具体地说, 若 $i \leq j$, 则 x_i 的所有信息都囊括于 x_j 中. 于是我们首先寻求一种更典型的, 更精简的代数结构来表示 $\left(\mathbb{Z}, |\bullet|_p\right)$ 的完备化. 这就是 § 2.1 节的工作, 得到的精简结构为 $\mathbb{Z}_p$. 进一步地, 我们想要探索元素依然为可数无穷序列 $(y_n)_{n\in\mathbb{N}}$, 但是元素分量形式 (或者规律) 和环结构都与 $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ 不同的另一种环结构, 使之与 $\mathbb{Z}_p$ 呈环同构, 从而拓展 $\mathbb{Z}_p$ 的表示方式. § 2.2 节的工作就是为这种全新的代数结构作数学逻辑上的引入.

2.1 $\mathbb{Z}_p$ 表示法

选取 $\mathbb{Z}$ 的一个双边理想降链

$$\mathbb{Z} \supset p\mathbb{Z} \supset p^2\mathbb{Z} \supset \cdots,$$

存在相应的满射环同态

$$\Re/I_1 \xleftarrow{\lambda_1} \Re/I_2 \xleftarrow{\lambda_2} \Re/I_3 \xleftarrow{\lambda_3} \cdots,$$

并由此构造得到 $\left(\mathbb{Z}, |\bullet|_p\right)$ 的一个完备化 $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$. 源于 $\lambda(x_{n+1}) = x_n$, $n = 1,\ 2,\ \cdots$ 的限制, $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ 中的每个元素位置在后的分量完全囊括了位置在前分量的信息. 一种形象化理解的方式是将可数无穷序列 $(x_n)_{n\in\mathbb{N}} \in \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ 视为一种崭新的数, 记为 a. (x_n) 与 a 之间成立关系

$$x_n = a \mod p^n,$$

即有

$$\begin{aligned}
&x_1 = a \mod p,\\
&x_2 = a \mod p^2 = x_1 + a_1 p,\ a_1 \in \{0,\ 1,\ \cdots,\ p-1\},\\
&x_3 = a \mod p^3 = x_2 + a_2 p^2 = x_1 + a_1 p + a_2 p^2,\ a_2 \in \{0,\ 1,\ \cdots,\ p-1\},\\
&\quad \cdots\cdots .
\end{aligned}$$

因此, 我们不妨缩小研究范围, 只考虑每个 $(x_n)_{n\in\mathbb{N}} \in \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ 的第 ∞ 个分量 [10], 即考虑以下集合

$$\begin{aligned}
\mathbb{Z}_p :&= \left\{ \lim_{n\to\infty} x_n :\ (x_n)_{n\in\mathbb{N}} \in \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \right\}.\\
&= \left\{ \sum_{v=0}^{\infty} a_v p^v :\ a_v \in \{0,\ 1,\ \cdots,\ p-1\},\ \forall v \in \mathbb{N} \right\}.
\end{aligned}$$

[10] 更具体地说, 是考虑 (x_n) 的第 ∞ 个分量的级数形式, 而非其求和结果.

基于 § 1.3 节得出的结果, $\mathbb{Z}_p$ 上的加法运算 $\oplus$ 和乘法运算 $\otimes$ 为

$$\sum_{v=0}^{\infty} a_v p^v \oplus \sum_{v=0}^{\infty} b_v p^v := \sum_{v=0}^{\infty} a_v p^v + \sum_{v=0}^{\infty} b_v p^v \mod \left(\lim_{n\to\infty} p^v \right) = \sum_{v=0}^{\infty} (a_v + b_v) p^v,$$
$$\sum_{v=0}^{\infty} a_v p^v \otimes \sum_{v=0}^{\infty} b_v p^v := \sum_{v=0}^{\infty} a_v p^v \times \sum_{v=0}^{\infty} b_v p^v \mod \left(\lim_{n\to\infty} p^v \right) = \sum_{v=0}^{\infty} \left(\sum_{i+j=v} a_i \times b_j \right) p^v,$$

由此可见 $\oplus$, $\otimes$ 实质上分别就是平凡运算 $+$, $\times$, 后续对二者不加区分. 此时更加典范的表达为

$$\sum_{v=0}^{\infty} a_v p^v + \sum_{v=0}^{\infty} b_v p^v := \sum_{v=0}^{\infty} c_v p^v,\ c_v = \begin{cases} a_0 + b_0 \mod p,\ v = 0, \\ \dfrac{1}{p^v} \left(\displaystyle\sum_{k=0}^{v} (a_k + b_k) p^k \mod p^{v+1} - \sum_{k=0}^{v-1} c_k p^k \right),\ v > 0. \end{cases}$$
$$\sum_{v=0}^{\infty} a_v p^v \times \sum_{v=0}^{\infty} b_v p^v := \sum_{v=0}^{\infty} d_v p^v,\ d_v = \begin{cases} a_0 \times b_0 \mod p,\ v = 0, \\ \dfrac{1}{p^v} \left(\displaystyle\sum_{k=0}^{v} \sum_{i+j=k} a_i b_j p^k \mod p^{v+1} - \sum_{k=0}^{v-1} d_k p^k \right),\ v > 0. \end{cases}$$

显然 $(\mathbb{Z}_p, +, \times)$ 是一个环结构. 而 $\mathbb{Z}_p$ 上的赋值 $|\bullet|_\bigstar$ 为

$$\left| \sum_{v=0}^{\infty} a_v p^v \right|_\bigstar := \lim_{n\to\infty} \left| \sum_{v=0}^{n} a_v p^v \right|_p = \left| \lim_{n\to\infty} \sum_{v=0}^{n} a_v p^v \right|_p = \left| \sum_{v=0}^{\infty} a_v p^v \right|_p,$$

即 $|\bullet|_\bigstar$ 实质上就是 $|\bullet|_p$. 后续对二者不加区分. 对任意一个 $a := \sum_{v=0}^{\infty} a_v p^v \in \mathbb{Z}_p$, 记

$$\Lambda := \{k \geq 0 :\ a_k \neq 0\},$$
$$m := \begin{cases} \min \Lambda,\ \Lambda \neq \varnothing, \\ \infty,\ \Lambda = \varnothing. \end{cases}$$

由于 $a_v \in \{0,\ 1,\ \cdots,\ p-1\}$, 因此有 $p^v \| a_v p^v$, 且由于 $|\bullet|_p$ 是非阿基米德赋值, 根据推论1.1.7, 则 a 的 p-进赋值为

$$|a|_p = p^{-m} \in [0, 1].$$

现在我们对 $\mathbb{Z}_p$ 能表示 $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ 作严格的说明. 考虑映射 f

$$f :\ \begin{array}{ccc} \mathbb{Z}_p & \to & \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \\ \displaystyle\sum_{v=0}^{\infty} a_v p^v & \to & \left(\displaystyle\sum_{v=0}^{n} a_v p^v \right)_{n\in\mathbb{N}} \end{array}.$$

命题 2.1.1 设 $n \in \mathbb{Z}_{\geq 0}$, $\sum_{v=0}^{n} a_v p^v,\ \sum_{v=0}^{n} b_v p^v \in \mathbb{Z}_p$, 则成立

$$\sum_{v=0}^{n} a_v p^v = \sum_{v=0}^{n} b_v p^v. \iff a_v = b_v,\ \forall v \in \{0,\ 1,\ \cdots,\ n\}.$$

证明 $(\Leftarrow)$ 方向的推理是显然的, 因此只需要关注 $(\Rightarrow)$ 方向的推理. 若成立 $\sum_{v=0}^{n} a_v p^v = \sum_{v=0}^{n} b_v p^v$, 则移项并合并同类项, 得到

$$\sum_{v=0}^{n} (a_v - b_v)\, p^v =: \sum_{v=0}^{n} c_v p^v = 0,\ c_v = a_v - b_v. \tag{2.1.1}$$

由于 $a_v,\ b_v \in \{0,\ 1,\ \cdots,\ p-1\}$, 因此有

$$c_v \in \{-(p-1),\ -(p-2),\ \cdots,\ 0,\ 1,\ \cdots,\ (p-2),\ (p-1)\},\ \forall v. \tag{2.1.2}$$

- 由式 *(2.1.1)*, 式 *(2.1.2)*, 有

$$c_0 = -\left(c_1 + \cdots + c_n p^{n-1}\right) p. \implies p \mid c_0. \implies c_0 = 0. \tag{2.1.3}$$

- 由式 *(2.1.1)*, 式 *(2.1.2)*, 式 *(2.1.3)*, 有

$$\begin{aligned} & c_1 p = -\left(c_2 p^2 + \cdots + c_n p^n\right) = -\left(c_2 + \cdots + c_n p^{n-2}\right) p^2. \\ \implies & c_1 = -\left(c_2 + \cdots + c_n p^{n-2}\right) p. \\ \implies & p \mid c_1. \implies c_1 = 0. \end{aligned}$$

- ……

重复以上操作, 即可得到

$$\text{式 } (2.1.1) \text{ 成立}. \implies c_0 = c_1 = \cdots = c_n = 0.$$

至此, 明所欲证. □

推论 2.1.2 任取 $\sum_{v=0}^{\infty} a_v p^v,\ \sum_{v=0}^{\infty} b_v p^v \in \mathbb{Z}_p$, 成立

$$\sum_{v=0}^{\infty} a_v p^v = \sum_{v=0}^{\infty} b_v p^v. \iff (a_n)_{n\in\mathbb{N}} = (b_n)_{n\in\mathbb{N}}.$$

证明 由于 $\sum_{v=0}^{\infty} a_v p^v,\ \sum_{v=0}^{\infty} b_v p^v \in \mathbb{Z}_p$, 于是在极限存在的前提下, 令命题*2.1.1*中的 $n \to \infty$ 即可得证. □

在此基础上, 若 $\mathbb{Z}_p$ 中

$$\sum_{v=0}^{\infty} a_v p^v \neq \sum_{v=0}^{\infty} b_v p^v.$$

由推论2.1.2, $\exists k \geq 0,\ a_k \neq b_k$, 即有 $(a_n)_{n\leq k} \neq (b_n)_{n\leq k}$. 再根据命题2.1.1, 成立 $\sum_{v=0}^{k} a_v p^v \neq \sum_{v=0}^{k} b_v p^v$, 因此也就有

$$\left(\sum_{v=0}^{n} a_v p^v\right)_{n\in\mathbb{N}} \neq \left(\sum_{v=0}^{n} b_v p^v\right)_{n\in\mathbb{N}}.$$

于是映射 f 是一个单射. 另一方面, 显然成立

$$f\left(\sum_{v=0}^{\infty}a_vp^v\right)=\left(\sum_{v=0}^{n}a_vp^v\right)_{n\in\mathbb{N}},\ \forall\left(\sum_{v=0}^{n}a_vp^v\right)_{n\in\mathbb{N}}\in\varprojlim_n\mathbb{Z}/p^n\mathbb{Z},\ \exists\sum_{v=0}^{\infty}a_vp^v\in\mathbb{Z}_p.$$

因此 f 是一个满射. 除此之外, $\forall a,\ b\in\mathbb{Z}_p$, f 显然满足

$$f(a+b)=f(a)+f(b),$$
$$f(ab)=f(a)f(b).$$

于是我们导出了以下的定理.

定理 2.1.3 $\mathbb{Z}_p$ 是 $\varprojlim_n\mathbb{Z}/p^n\mathbb{Z}$ 的环同构, 即有

$$\mathbb{Z}_p\xrightarrow{\sim}\varprojlim_n\mathbb{Z}/p^n\mathbb{Z}.$$

最后, 我们通过对 $\mathbb{Z}_p$ 进行一些补充说明来结束此小节. 首先强调 $\mathbb{Z}_p$ 中的元素 $\sum_{v=0}^{\infty}a_vp^v$ 并没有要求其部分和序列 (在 $\mathbb{Z}$ 中) 收敛. 其次, $\mathbb{Z}_p$ 的构造超越了一些常识, 比如 $\sum_{v=0}^{\infty}p^v$ 和 $\sum_{v=0}^{\infty}2p^v$, 在实数域中它们都是发散的 (或者说是不存在的), 都等于 ∞. 而在 $\mathbb{Z}_p$ 中, 根据推论2.1.2, 它们是存在且不相等的. 而对于整数环 $\mathbb{Z}$ 嵌入 $\mathbb{Z}_p$ 的问题, 一方面, $\forall a\in\mathbb{Z}_{\geq 0}$, 显然可以通过一系列取模 p 算法将 a 表为具有形式 $\sum\limits_{v=0}^{n}a_vp^v$, $a_v\in\{0,\ 1,\ \cdots,\ p-1\}$ 的有限和形式, 此时的嵌入是显然的:

$$\begin{array}{ccc}\mathbb{Z}_{\geq 0} & \hookrightarrow & \mathbb{Z}_p\\ a & \to & a\end{array}.$$

而对于 $\forall(-a)\in\mathbb{Z}_{<0}$, 我们不能将其简单地表为 $\sum_{v=0}^{\infty}(-a_v)p^v$ 的形式, 因为此时 $-a_v\leq 0$, 该形式不被 $\mathbb{Z}_p$ 接纳. 对于非正整数的形式构造比较巧妙, 可见下面的例子.

例子 2.1.4 $\mathbb{Z}\ni 0\to 0+0\times p+0\times p^2+\cdots$.

例子 2.1.5 $\mathbb{Z}\ni -1\to(p-1)+(p-1)p+(p-1)p^2+\cdots=\sum_{v=0}^{\infty}(p-1)p^v$.

注记

$$-1=(p-1)+(p-1)p+\cdots+(p-1)p^{n-1}-p^n.$$
$$\Longrightarrow\ -1\equiv(p-1)+(p-1)p+\cdots+(p-1)p^{n-1}\mod p^n.$$

例子 2.1.6 $\mathbb{Q}\ni\frac{1}{1-p}\to 1+p+p^2+\cdots=\sum_{v=0}^{\infty}p^v$.

注记

$$1=\left(1+p+\cdots+p^{n-1}\right)(1-p)+p^n.$$
$$\Longrightarrow\frac{1}{1-p}\equiv 1+p+\cdots+p^{n-1}\mod p^n.$$

由 $-a=a\times(-1)$ 有以下嵌入

$$\begin{array}{ccc}\mathbb{Z}_{\leq 0} & \hookrightarrow & \mathbb{Z}_p\\ -a & \to & a\times\sum\limits_{v=0}^{\infty}(p-1)p^v\end{array}.$$

2.2 Witt 向量的代数背景

在这一小节中, 我们先从 § 2.1 节得到的代数结构 $\mathbb{Z}_p$ 出发, 一步步分析得到 $\mathbb{Z}_p$ 的另一种表示结构的初貌. 下面以 $\mathbb{Z}_p$ 的剩余环结构研究作为开始.

命题 2.2.1 设 p 是一个素数. 存在以下环同构

$$\mathbb{Z}_p/p\mathbb{Z}_p \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} \mathbb{F}_p.$$

证明 关于后半部分的同构 $\mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} \mathbb{F}_p$ 是显然的, 详细说明可参见李文威 *[12, 例 5.2.4]*. 我们只需要说明前半部分的同构 $\mathbb{Z}_p/p\mathbb{Z}_p \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z}$ 即可.

$$\begin{aligned} p\mathbb{Z}_p &= \left\{ \sum_{v=1}^{\infty} b_v p^v :\ b_v \in \{0,\ 1,\ \cdots,\ p-1\},\ \forall v \in \mathbb{Z}_{\geq 1} \right\}. \\ &= \left\{ b \in \mathbb{Z}_p :\ |b|_p < 1 \right\} \subset \mathbb{Z}_p. \end{aligned}$$

显然是 $\mathbb{Z}_p$ 的一个理想, $\mathbb{Z}_p/p\mathbb{Z}_p$ 是一个剩余类环, 其结构可表示为

$$\begin{aligned} &\mathbb{Z}_p/p\mathbb{Z}_p \\ =&\{a + p\mathbb{Z}_p :\ a \in \mathbb{Z}_p\} \\ =&\left\{ \left\{ \begin{array}{c} a_0 + \displaystyle\sum_{v=1}^{\infty} b_v p^v : \\ b_v \in \{0,\ 1,\ \cdots,\ p-1\},\ \forall v \in \mathbb{Z}_{\geq 1} \end{array} \right\} :\ a_0 \in \{0,\ 1,\ \cdots,\ p-1\} \right\}. \end{aligned}$$

仿 $\mathbb{Z}/p\mathbb{Z} = \left\{ \widehat{0},\ \widehat{1},\ \cdots,\ \widehat{(p-1)} \right\}$, 可记 $\mathbb{Z}_p/p\mathbb{Z}_p = \left\{ \overline{0},\ \overline{1},\ \cdots,\ \overline{(p-1)} \right\}$, 其中 $\overline{k} := \{k + \sum_{v=1}^{\infty} b_v p^v\}$. 显然 $\mathbb{Z}_p/p\mathbb{Z}_p$ 与存在环同构 ϕ

$$\phi : \begin{array}{ccc} \mathbb{Z}_p/p\mathbb{Z}_p & \xrightarrow{\sim} & \mathbb{Z}/p\mathbb{Z} \\ \overline{a} & \mapsto & \widehat{a} \end{array}.$$

至此, 明所欲证. □

基于 $\mathbb{Z}_p$ 模去 $p\mathbb{Z}_p$ 的剩余类环可视为特征为 p 的有限域 $\mathbb{F}_p$, 我们可选定某一映射 $\tau : \mathbb{F}_p \to \mathbb{Z}_p$ 使得 $\forall x \in \mathbb{F}_p, \tau(x) \equiv x \pmod{p\mathbb{Z}_p}$ [11] , 称 $\tau(x)$ 为 x 的一个提升. 提升的严格数学定义如下.

定义 2.2.2 设 $\mathfrak{R}$ 是一个环, $\mathfrak{a}$ 是 $\mathfrak{R}$ 的一个（双边）理想, 称映射 τ 为剩余类环 $\mathfrak{R}/\mathfrak{a}$ 到环 $\mathfrak{R}$ 的一个**提升**, 若 τ 满足

$$\tau(x) \equiv x \mod \mathfrak{a},\ \forall x \in \mathfrak{R}/\mathfrak{a}.$$

命题 2.2.3 设 $\mathfrak{R}$ 是一个环, $\mathfrak{a}$ 是 $\mathfrak{R}$ 的一个（双边）理想, 则剩余类环 $\mathfrak{R}/\mathfrak{a}$ 到环 $\mathfrak{R}$ 的提升 τ 一定存在.

[11] $\tau(x) \equiv x \pmod{p\mathbb{Z}_p}$ 表示 $\tau(x) + p\mathbb{Z}_p = x$.

证明 由于代表模去理想的映射 $\phi:\ \Re \to \Re/\mathfrak{a}$ 是一个满射, 因此总是存在 $\Re_x$, 成立

$$\phi\left(\Re_x\right)=x,\ \varnothing \neq \Re_x \subseteq \Re,\ \forall x \in \Re/\mathfrak{a}.$$

遍历 $\Re/\mathfrak{a}$ 中的元素 x, 任取 $r_x \in \Re_x$, 令 $\tau\left(x\right):=r_x$. 成立以下推理

$$\left.\begin{aligned} r_x+\mathfrak{a}=\tau\left(x\right). &\implies \tau\left(x\right)\equiv r_x \mod \mathfrak{a}. \\ \phi\left(r_x\right)=r_x+\mathfrak{a}=x. &\implies r_x \equiv x \mod \mathfrak{a}. \end{aligned}\right\} \implies \tau\left(x\right)\equiv x \mod \mathfrak{a},\ \forall x \in \Re/\mathfrak{a}.$$

至此我们便构造得到了一个提升 τ, 其存在性得证. □

事实上, 在命题2.2.1给出的同构下, 不妨记

$$\mathbb{F}_p=\left\{\overline{0},\ \overline{1},\ \cdots,\ \overline{(p-1)}\right\},$$

提升 τ 的选取只需符合以下形式

$$\tau:\begin{array}{ccc} \mathbb{F}_p & \mapsto & \mathbb{Z}_p \\ \overline{a} & \to & \begin{array}{c}\text{任意选定的}a_0\text{满足} \\ a_0 \equiv a \mod p.\end{array} \end{array}$$

由此我们得到了以下的一个交换图

$$\mathbb{Z}_p \underset{\tau\text{: 提升}}{\overset{\phi\text{: 模去}p\mathbb{Z}_p}{\rightleftarrows}} \mathbb{F}_p$$

现任意取定一个提升 τ, 进行以下操作.

算法 2.2.4

- $\forall \widetilde{x} \in \mathbb{Z}_p$, 记 $x_0=\phi\left(\widetilde{x}\right) \in \mathbb{F}_p$, 则 $\exists \widetilde{x_1} \in \mathbb{Z}_p$ 使得 $\widetilde{x}=\tau\left(x_0\right)+p\widetilde{x_1}$.
- 记 $x_1=\phi\left(\widetilde{x_1}\right)$, 则 $\exists \widetilde{x_2} \in \mathbb{Z}_p$ 使得 $\widetilde{x_1}=\tau\left(x_1\right)+p\widetilde{x_2}$.
- ……

由此得到一个序列 $x_0,\ x_1,\ \cdots$, 使得 $\forall n \geq 0$, 成立

$$\begin{aligned} \widetilde{x} &= \tau\left(x_0\right)+p\widetilde{x_1} \\ &= \tau\left(x_0\right)+p\left(\tau\left(x_1\right)+p\widetilde{x_2}\right) \\ &= \cdots \\ &= \tau\left(x_0\right)+\tau\left(x_1\right)p+\cdots+\tau\left(x_n\right)p^n+\widetilde{x_{n+1}}p^{n+1},\ \widetilde{x_{n+1}} \in \mathbb{Z}_p. \end{aligned}$$

令 $n \to \infty$, 即可得

$$\widetilde{x}=\tau\left(x_0\right)+\tau\left(x_1\right)p+\cdots+\tau\left(x_n\right)p^n+\cdots=\sum_{n=0}^{\infty}\tau\left(x_n\right)p^n. \tag{2.2.1}$$

显然由上面操作得到的无穷级数 $\sum_{n=0}^{\infty}\tau\left(x_n\right)p^n$ 在 $\mathbb{Z}_p$ 中收敛到 $\widetilde{x}$. 针对算法2.2.4有下面的命题.

命题 2.2.5 $\forall\widetilde{x}\in\mathbb{Z}_p$, 满足式 *(2.2.1)* 的序列 $(x_0,\ x_1,\ \cdots,\ x_n,\ \cdots)$ 是存在且唯一的.

证明 任意取定一个 $\widetilde{x}\in\mathbb{Z}_p$, 首先可以确定 $x_0=\phi(\widetilde{x})$ 是存在且唯一的.

运算 ϕ 的实质就是取模运算 $x_0=\widetilde{x}+p\mathbb{Z}_p\in\mathbb{F}_p$, 即有

$$\widetilde{x}\equiv x_0\mod p\mathbb{Z}_p.$$

提升 τ 的定义*2.2.2*蕴涵

$$x_0\equiv\tau(x_0)\mod p\mathbb{Z}_p.$$

因此由同余式的传递性, 成立

$$\widetilde{x}\equiv\tau(x_0)\mod p\mathbb{Z}_p. \tag{2.2.2a}$$

$$\Longrightarrow\ \widetilde{x}-\tau(x_0)\equiv 0\mod p\mathbb{Z}_p. \tag{2.2.2b}$$

$$\Longrightarrow\ p|\,\widetilde{x}-\tau(x_0). \tag{2.2.2c}$$

因此 $\exists\widetilde{x_1}\in\mathbb{Z}_p$, 使得

$$\widetilde{x}=\tau(x_0)+p\widetilde{x_1}. \tag{2.2.3}$$

假设存在另一个 $\widetilde{x_1}'\in\mathbb{Z}_p$ 也成立 $\widetilde{x}=\tau(x_0)+p\widetilde{x_1}'$, 则有

$$p\widetilde{x_1}=p\widetilde{x_1}'.\ \Longrightarrow\ p\left(\widetilde{x_1}-\widetilde{x_1}'\right)=0.$$

由于 $\mathbb{Z}\subset\mathbb{Z}_p$, $\mathrm{char}(\mathbb{Z}_p)=\mathrm{char}(\mathbb{Z})=0$, 素数 p 非整环 $\mathbb{Z}_p$ 的零元, 因此即有

$$\widetilde{x_1}-\widetilde{x_1}'=0.\ \Longrightarrow\ \widetilde{x_1}=\widetilde{x_1}',$$

即满足式 *(2.2.3)* 的 $\widetilde{x_1}$ 是存在且唯一的. 因此 $x_1=\phi(\widetilde{x_1})$ 也是存在且唯一的. 继续推导下去可得 $x_2,x_3,\cdots$ 也是存在且唯一的. □

此外, 我们指出 $\mathbb{F}_p$ 中的任意序列 $(x_n)_{n\geq 0}$ 也能唯一确定一个 $\widetilde{x}=\sum_{n=0}^{\infty}\tau(x_n)\,p^n\in\mathbb{Z}_p$.

引理 2.2.6 设 $\Re$ 是一个环, $|\bullet|$ 是 $\Re$ 上的一个非阿基米德赋值, 且 $\Re$ 关于赋值 $|\bullet|$ 是完备的, 则无穷级数 $\sum_{i=1}^{\infty}a_i$ 在 $\Re$ 中关于赋值 $|\bullet|$ 收敛的充要条件是

$$\lim_{i\to\infty}|a_i|=0.$$

证明 记 $A_n=\sum_{i=1}^{n}a_i$.

1. 若 $\sum_{i=1}^{\infty}a_i$ 在 $\Re$ 中关于赋值 $|\bullet|$ 收敛, 设收敛到 A, 即 $\lim_{n\to\infty}|A_n-A|=0$, 则成立

$$\begin{aligned}0\leq|a_n|=|A_{n+1}-A_n|&=|(A_{n+1}-A)+(A-A_n)|\\&\leq|A_{n+1}-A|+|A_n-A|\to 0\ \ (n\to\infty),\end{aligned}$$

即成立 $\lim_{i\to\infty}|a_i|=0$.

2. 若成立 $\lim_{i\to\infty}|a_i|=0$, 则 $\forall\varepsilon>0$, $\exists N\in\mathbb{N}$, 使得

$$||a_i|-0|_\infty=|a_i|<\varepsilon,\ \forall i\geq N.$$

由于 $|\bullet|$ 具有非阿基米德性, 根据推论*1.1.5*, 成立

$$|A_j-A_i|=|a_{i+1}+a_{i+2}+\cdots+a_j|\leq\max_{i+1\leq k\leq j}\{|a_k|\}<\varepsilon,\ \forall j\geq i\geq N.$$

从而部分和序列 $(A_n)_{n\geq0}$ 是一个柯西列. 由于 $\left(\Re,|\bullet|_p\right)$ 是完备的, 因此柯西列 $(A_n)_{n\geq0}$ 在 $\Re$ 中收敛, 即无穷级数 $\sum_{i=1}^{\infty}a_i$ 在 $\Re$ 中收敛. □

命题 2.2.7 $\mathbb{F}_p$ 中的任意序列 $(x_n)_{n\geq0}$ 对应的无穷级数 $\widetilde{x}:=\sum_{n=0}^{\infty}\tau(x_n)p^n$ 在 $\left(\mathbb{Z}_p,|\bullet|_p\right)$ 中是收敛的.

证明 由于

$$0\leq|\tau(x_n)p^n|_p\leq p^{-n}\to0\ \ (n\to\infty),$$

由极限的迫敛性, 成立

$$\lim_{n\to\infty}|\tau(x_n)p^n|_p=0.$$

由于 $\mathbb{Z}_p$ 关于非阿基米德的 p-进赋值 $|\bullet|_p$ 是完备的, 根据引理*2.2.6*, 无穷级数 $\widetilde{x}$ 在 $\mathbb{Z}_p$ 中收敛. □

于是由命题2.2.5和命题2.2.7, 我们可以得到以下的一个集合双射 Γ_0

$$\Gamma_0:\begin{array}{ccc}\prod\limits_{n\geq0}\mathbb{F}_p & \xrightarrow{1:1} & \mathbb{Z}_p\\ x=(x_n)_{n\geq0} & \to & \sum\limits_{n=0}^{\infty}\tau(x_n)p^n\end{array}$$

由于 Γ_0 是双射, 因此存在同是双射的逆映射 ${\Gamma_0}^{-1}:\ \mathbb{Z}_p\to\prod_{n\geq0}\mathbb{F}_p$. 至此我们完成了将环 $(\mathbb{Z}_p,+,\bullet)$ 中的元素一一投影到 $\prod_{n\geq0}\mathbb{F}_p$ 中. 若能进一步定义 $\prod_{n\geq0}\mathbb{F}_p$ 上的运算 $\oplus$ 和 $\odot$ 使之成为一个环, 并且保证映射 Γ_0 满足

$$\begin{aligned}\Gamma_0(x\oplus y)&=\Gamma_0(x)+\Gamma_0(y),\\ \Gamma_0(x\odot y)&=\Gamma_0(x)\bullet\Gamma_0(y),\end{aligned}$$

则 Γ_0 便是一个环同构, $\mathbb{Z}_p$ 的环结构也就可以体现在 $\prod_{n\geq0}\mathbb{F}_p$ 上了, 此时 $\prod_{n\geq0}\mathbb{F}_p$ 就是 $\mathbb{Z}_p$ 的一个表示.

上面是从环 $\mathbb{Z}_p$ 开始进行分析和推导的, 最终得到了一个从 $\prod_{n\geq0}\mathbb{F}_p$ 到 $\mathbb{Z}_p$ 的双射结构 Γ_0. 事实上, 这个分析过程只是一种特殊情况, 而囊括于更为广泛的一种代数现象. 下面我们先介绍几个相关的代数概念.

定义 2.2.8 设 p 是一个素数, $(\Re,+,\bullet)$ 是一个特征为 p 的环, 称 $\Re$（**关于特征 p**）**是完全的**或者是一个**完全环**, 若 $\Re$ 上的自同态

$$\mathrm{Fr}_p:\begin{array}{ccc}\Re & \mapsto & \Re\\ x & \mapsto & x^p\end{array}$$

是 $\Re$ 上的自同构, 即 Fr_p 是一个双射, 其中 x^p 表示

$$\underbrace{x\bullet x\bullet\cdots\bullet x}_{p个}.$$

注记 Fr_p 确实是一个环同态. 一方面, 显然有 $\mathrm{Fr}_p(xy)=(xy)^p=x^py^p=\mathrm{Fr}_p(x)\,\mathrm{Fr}_p(y)$; 另一方面, 由于 $\Re$ 的特征为 p, 故成立 $\mathrm{Fr}_p(x+y)=(x+y)^p=x^p+y^p=\mathrm{Fr}_p(x)+\mathrm{Fr}_p(y)$.

例子 2.2.9 有限域 $\mathbb{F}_p$ 是完全的.

注记 推导过程涉及域上不可约多项式的一些知识, 此处略过, 详见李文威 *[12, 推论 8.4.16]*.

完全环 $\Re$ 具有以下的性质.

命题 2.2.10 设 $\Re$ 是一个特征为 p 的完全环, 则 $\forall x\in\Re$, x 的 p 次根在 $\Re$ 中是存在且唯一的, 记为 $x^{p^{-1}}$.

证明 由于环 $\Re$ 是完全的, 因此 $\Re$ 上的自同态 Fr_p 是一个双射, Fr_p 可逆且逆映射 ${\mathrm{Fr}_p}^{-1}$ 也是一个双射. 因此 $\forall x\in\Re$, $\exists!y\in\Re$ 满足 $y={\mathrm{Fr}_p}^{-1}(x)$, 也就有

$$y^p=\mathrm{Fr}_p(y)=\mathrm{Fr}_p\left({\mathrm{Fr}_p}^{-1}(x)\right)=x.$$

因此 y 是 x 在 $\Re$ 中的唯一一个 p 次根. □

推论 2.2.11 设 $\Re$ 是一个特征为 p 的完全环, 则 $\forall x\in\Re$, $\forall n\in\mathbb{Z}_{\geq 0}$, x 的 p^n 次根在 $\Re$ 中是存在且唯一的, 记为 $x^{p^{-n}}$.

证明

- $n=0$ 时, x 的 $p^n=1$ 次根就是 x, 显然是唯一的.
- $n=1$ 的情况已由命题*2.2.10*给出.
- $n>1$ 时, 由命题*2.2.10*, $\forall x_0\in\Re$, $\exists!x_1\in\Re$ 使得 ${x_1}^p=x$. 而对于 x_1, 同样地, $\exists!x_2\in\Re$ 使得 ${x_2}^p=x_1$. 重复此过程, 可以得到

$$\underbrace{(((x_n)^p)^p\cdots)^p}_{n层嵌套}=x\implies {x_n}^{p^n}=x.$$

即 x_n 是 x 在 $\Re$ 中唯一一个 p^n 次根. □

有了完全环的概念基础, 现在我们就可以引入 p-环的相关概念如下.

定义 2.2.12 设 $\Re$ 为一个含幺交换环, 给定 $\Re$ 的一个双边理想降链

$$\Re = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots,$$

并设 p 是一个素数, 记

$$\boldsymbol{p} := \underbrace{\mathbf{1} + \mathbf{1} + \cdots + \mathbf{1}}_{p\text{个}},$$

其中 $\mathbf{1}$ 是环 $\Re$ 的幺元. 称 $\Re$ 是一个p-**环**, 若满足

1. 相应的拓扑使 $\Re$ 成为一个完备的 *Hausdorff* **拓扑环** , 即 $\Re \xrightarrow{\sim} \varprojlim_n \Re/\mathfrak{a}_n$;
2. 对每个 n, m 皆有 $\mathfrak{a}_n\mathfrak{a}_m \subseteq \mathfrak{a}_{n+m}$;
3. $\boldsymbol{p} \in \mathfrak{a}_1$ 且剩余环 $\kappa := \Re/\mathfrak{a}_1$ 是完全的.

特别地, 称 p-环 $\Re$ 是一个**严格** p-**环**, 若额外满足

1. $\boldsymbol{p}$ 在 $\Re$ 中非零因子, 即不存在 $\lambda \in \Re_{\neq 0}$ 使得 $\boldsymbol{p}\lambda = 0$（蕴涵 $\operatorname{char}(\Re) \neq p$）;
2. $\mathfrak{a}_n = \boldsymbol{p}^n\Re$.

注记 p-环定义的条件 *(3)* 中的 $\boldsymbol{p} \in \mathfrak{a}_1$ 可以等价地改写为 $\operatorname{char}(\kappa) = p$. 事实上, 由于 $\mathfrak{a}_1$ 真包含于 $\Re$, 因此 $\operatorname{char}(\kappa) > 1$. 在此基础上可以成立以下的等价关系

$$\boldsymbol{p} \in \mathfrak{a}_1. \xLeftrightarrow{\mathfrak{a}_1\text{运算封闭性}} \sum_{i=1}^{p}(\mathbf{1} + \mathfrak{a}_1) = \sum_{i=1}^{p}\mathbf{1} + \sum_{i=1}^{p}\mathfrak{a}_1 = \boldsymbol{p} + \mathfrak{a}_1 = \mathfrak{a}_1. \xLeftrightarrow{\text{char 定义, } p\text{素}} \operatorname{char}(\kappa) = p.$$

例子 2.2.13 $\mathbb{Z}_p$ 是一个严格 p-环.

证明 给定 $\mathbb{Z}_p$ 的一个理想降链

$$\mathbb{Z}_p \supset p\mathbb{Z}_p \supset p^2\mathbb{Z}_p \supset \cdots.$$

1. $\mathbb{Z}_p \xrightarrow{\sim} \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\sim} \varprojlim_n \mathbb{Z}_p/p^n\mathbb{Z}_p$ 是一个完备的 *Hausdorff* 拓扑环.
2. $\forall n,\ m \geq 0,\ (p^n\mathbb{Z}_p)(p^m\mathbb{Z}_p) = (p^np^m)(\mathbb{Z}_p\mathbb{Z}_p) = p^{n+m}\mathbb{Z}_p$.
3. 剩余环 $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ 是一个特征为 p 的域, 是完全的, 且显然有 $p = p \cdot 1 \in p\mathbb{Z}_p$.

因此 $\mathbb{Z}_p$ 是一个 p-环. 此外, 由于 $\operatorname{char}(\mathbb{Z}_p) = 0 \neq p$, p 不是整环 $\mathbb{Z}_p$ 中的零元（因此也非零因子）, 因此 $\mathbb{Z}_p$ 也是一个严格 p-环. □

例子 2.2.14 $\mathbb{F}_p$-代数 $\mathbb{F}_p[\![t]\!]$ 是一个 p-环, 但不是一个严格 p-环.

证明 给定 $\mathbb{F}_p[\![t]\!]$ 的一个理想降链

$$\mathbb{F}_p[\![t]\!] = (1) \supset (t) \supset \left(t^2\right) \supset \cdots,$$

其中 (t^n) 表示由 $t^n \in \mathbb{F}_p[\![t]\!]$ 生成的主理想. 由于 $\mathbb{F}_p[\![t]\!]$ 是一个含幺交换环, 幺元同 $\mathbb{F}_p$ 的幺元 $\mathbf{1}$, 因此根据主理想表示的基本知识 *[6, P66]*, 有

$$(t^n) = t^n\mathbb{F}_p[\![t]\!].$$

1. $\mathbb{F}_p[\![t]\!] \xrightarrow{\sim} \varprojlim_n \mathbb{F}_p[\![t]\!]/t^n\mathbb{F}_p[\![t]\!]$ 是一个完备的 *Hausdorff* 拓扑环.

2. $\forall n,\ m \geq 0$, 成立

$$(t^n)(t^m) = (t^n\mathbb{F}_p[\![t]\!])(t^m\mathbb{F}_p[\![t]\!]) = (t^nt^m)(\mathbb{F}_p[\![t]\!]\mathbb{F}_p[\![t]\!]) = t^{n+m}\mathbb{F}_p[\![t]\!] = \left(t^{n+m}\right).$$

3. 剩余环 $\mathbb{F}_p[\![t]\!]/t\mathbb{F}_p[\![t]\!] \cong \mathbb{F}_p$ 是一个特征为 p 的域, 是完全的. 而由于 $\mathbb{F}_p \subset \mathbb{F}_p[\![t]\!]$, $\operatorname{char}(\mathbb{F}_p[\![t]\!]) = \operatorname{char}(\mathbb{F}_p) = p$, 因此有 $\boldsymbol{p} = \mathbf{0} = \sum_{n=1}^{\infty} \mathbf{0} \cdot t^n \in t\mathbb{F}_p[\![t]\!]$.

因此 $\mathbb{F}_p[\![t]\!]$ 是一个 p-环. 而由于 $\boldsymbol{p}$ 在 $\mathbb{F}_p[\![t]\!]$ 中是零元（自然也是一个零因子）, $(t^n) \neq \{\mathbf{0}\} = \mathbf{0}^n\mathbb{F}_p[\![t]\!] = \boldsymbol{p}^n\mathbb{F}_p[\![t]\!]$, 因此 $\mathbb{F}_p[\![t]\!]$ 不构成一个严格 p-环. □

有了 p-环结构后, 我们可以从严格 p-环 $\Re$ 出发, 仿照本小节开头部分, 进行类似的推导. 还是记 $\boldsymbol{p} := \sum_{i=1}^{p}(\mathbf{1} \in \Re)$. $\Re$ 是严格 p-环, 存在双边理想降链

$$\Re \supset \boldsymbol{p}\Re \supset \boldsymbol{p}^2\Re \supset \cdots.$$

$\Re$ 上元素投影到 $\boldsymbol{p}\Re$ 依然可以通过模去理想 $\boldsymbol{p}\Re$ 的方式得到, 我们仍可取映射 ϕ 为

$$\phi: \begin{array}{ccc} \Re & \to & \Re/\boldsymbol{p}\Re \\ x & \to & x + \boldsymbol{p}\Re \end{array}$$

而基于命题2.2.3提供的提升存在性保证, 我们便可以取某一个 $\boldsymbol{p}\Re$ 到 $\Re$ 的提升 τ, 并结合 ϕ 构成以下的交换图

$$\Re \underset{\tau:\ 提升}{\overset{\phi:\ 模去\mathfrak{a}_1}{\rightleftarrows}} \Re/\boldsymbol{p}\Re$$

接着, 仿算法2.2.4, 对任意 $\widetilde{x} \in \Re$, 我们也可以得到一个序列 $(x_n) \in \prod_{n\geq 0}\Re/\boldsymbol{p}\Re$ 满足

$$\widetilde{x} = \sum_{n=0}^{\infty} \tau(x_n)\boldsymbol{p}^n. \tag{2.2.4}$$

注意由于 $\Re$ 是严格 p-环, 蕴含 $\boldsymbol{p} \neq \mathbf{0} \in \Re$. 仿命题2.2.5的证明过程, 我们也有相似的命题.

命题 2.2.15 $\forall \widetilde{x} \in \Re$, 满足式 *(2.2.4)* 的序列 $(x_0,\ x_1,\ \cdots,\ x_n,\ \cdots)$ 是存在且唯一的.

由于严格 p-环 $\Re$ 是一个完备的 Hausdorff 环, 蕴含 $\Re$ 对定义其上的广义 p-进赋值 $|\bullet|_{\boldsymbol{p}}$ 是完备的. 并且 $\Re \xrightarrow{\sim} \varprojlim_n \Re/\boldsymbol{p}\Re$ 的环同构揭示了 $\Re$ 中元素也可表为 $\mathbb{Z}_p$ 中元素那样的级数结构. 因此基于引理2.2.6, 我们可以完全仿照命题2.2.7的证明过程, 得到下面的命题.

命题 2.2.16 $\Re/\boldsymbol{p}\Re$ 中的任意序列 $(x_n)_{n\geq 0}$ 对应的无穷级数 $\widetilde{x} := \sum_{n=0}^{\infty}\tau(x_n)\boldsymbol{p}^n$ 在 $\left(\Re, |\bullet|_{\boldsymbol{p}}\right)$ 中是收敛的.

于是由命题2.2.15和命题2.2.16, 我们也可以得到以下的一个集合双射 Γ_0

$$\Gamma_0: \begin{array}{ccc} \prod\limits_{n\geq 0}\Re/\boldsymbol{p}\Re & \xrightarrow{1:1} & \Re \\ x = (x_n)_{n\geq 0} & \to & \sum\limits_{n=0}^{\infty}\tau(x_n)\boldsymbol{p}^n \end{array}.$$

至此, 我们引出了严格 p-环的另一种表示方式的代数初貌: $\prod_{n\geq 0}\Re/\boldsymbol{p}\Re$, 也就是下一节要介绍的 Witt 向量集.

3 用 $\prod_{n\geq 0}\mathbb{F}_p$ 表示 $\mathbb{Z}_p$

在 § 2.2 节的最后我们得到了严格 p-环 $\Re$ 的剩余类环序列集 $\prod_{n\geq 0}\Re/\boldsymbol{p}\Re$ 到 $\Re$ 的一个集合双射

$$\begin{array}{rccc} & \prod\limits_{n\geq 0}\Re/\boldsymbol{p}\Re & \xrightarrow{1:1} & \Re \\ \Gamma_0: & x=(x_n)_{n\geq 0} & \to & \sum\limits_{n=0}^{\infty}\tau(x_n)\,\boldsymbol{p}^n \end{array}.$$

而若要用 $\prod_{n\geq 0}\Re/\boldsymbol{p}\Re$ 来表示 $\Re$, 即将 $(\Re,+,\bullet)$ 的环结构体现在 $\prod_{n\geq 0}\Re/\boldsymbol{p}\Re$ 上, 则额外要求我们考虑

任务一 怎么赋予 $\prod_{n\geq 0}\Re/\boldsymbol{p}\Re$ 运算 $\oplus$, $\odot$ 使之成为一个环;

任务二 双射 Γ_0 是否能够将环 $\left(\prod_{n\geq 0}\Re/\boldsymbol{p}\Re,\oplus,\odot\right)$ 的结构线性地投射到 $(\Re,+,\bullet)$ 上, 即双射 Γ_0 能否成为一个环态射, 满足

$$\begin{aligned}\Gamma_0(x\oplus y)&=\Gamma_0(x)+\Gamma_0(y),\\ \Gamma_0(x\odot y)&=\Gamma_0(x)\bullet\Gamma_0(y).\end{aligned}$$

本节就是致力于完成这两个任务. 值得一提的是, 任务一与任务二本质上并非相互孤立. 同一个双射 Γ_0 可能对 $\prod_{n\geq 0}\Re/\boldsymbol{p}\Re$ 上的一种环结构 $\mathcal{R}_1$ 构成环态射, 而对其上的另一种环结构 $\mathcal{R}_2$ 不构成环态射. 而观察 Γ_0 的映射形式, 又可以指出 Γ_0 的性质取决于提升 τ 的选取. 因此本节的核心就是同时兼容地构建 $\left(\prod_{n\geq 0}\Re/\boldsymbol{p}\Re,\oplus,\odot\right)$ 与选取提升 τ. 前者由 § 3.2 节解决, 后者由 § 3.3 节解决. 而 § 3.1 节则是为后两节的论述引入前置性的概念基础.

3.1 Witt 多项式

下面先给出 Witt 多项式以及 Witt 向量的定义.

定义 3.1.1 设 $(\kappa,+,\bullet)$ 是一个含幺环满足 $\mathrm{char}(\kappa)=p$, 记

$$\boldsymbol{\pi}=\underbrace{\mathbf{1}+\mathbf{1}+\cdots+\mathbf{1}}_{\pi\text{个}}\in\kappa,$$

其中 π 是一个素数, $\mathbf{1}$ 是 κ 的幺元. $X=(X_0,X_1,\cdots,X_n,\cdots)\in\prod_{n\geq 0}\kappa$ 是一列可数的无穷序列. 称下面的多项式组

$$\begin{aligned}W_0(X,\ \pi)&=X_0,\\ W_1(X,\ \pi)&=X_0{}^{\pi}+\boldsymbol{\pi}X_1,\\ W_2(X,\ \pi)&=X_0{}^{\pi^2}+\boldsymbol{\pi}X_1{}^{\pi}+\boldsymbol{\pi}^2X_2,\\ &\vdots\\ W_n(X,\ \pi)&=X_0{}^{\pi^n}+\boldsymbol{\pi}X_1{}^{\pi^{n-1}}+\cdots+\boldsymbol{\pi}^nX_n=\sum_{i=0}^{n}\boldsymbol{\pi}^iX_i{}^{\pi^{n-i}},\\ &\vdots\end{aligned}$$

是**由序列 X 导出的, 系数为 π 的 *Witt* 多项式组**, $W_n(X,\ \pi)$ 是**由序列 X 导出的, 系数为 π 的第 $n+1$ 级 *Witt* 多项式** , 其中

$$\boldsymbol{\pi}^i X_i^{\pi^{n-i}} = \left(\underbrace{\boldsymbol{\pi}\bullet\boldsymbol{\pi}\bullet\cdots\bullet\boldsymbol{\pi}}_{\pi\text{个}}\right)\cdot\left(\underbrace{X_i\bullet X_i\bullet\cdots\bullet X_i}_{\pi^{n-i}\text{个}}\right)\in\kappa.$$

在不会混淆的情况下, 也可以将 $W_n(X,\pi)$ 简记为 $W_n(X)$ 或者 W_n. 称序列 X 为 κ 上的一个 *Witt* **向量**. 特别地, 称 $X^{(n)}=(X_0,X_1,\cdots,X_n)$ 是**长度为 $n+1$ 的截断 *Witt* 向量**.

注记

1. 一般要求素数 $\pi\neq p$, 否则由于 $\boldsymbol{\pi}=\mathbf{0}\in\kappa$, 会出现 $W_0=W_1=W_2=\cdots=X_0$. 后文的叙述中没有给出说明的情况下, 一般都默认 $\pi\neq p$.
2. 一般也要求 κ 是交换环, 免去考虑 κ 上乘法运算顺序的麻烦. 后面没有给出指明时, 默认 κ 是一个含幺交换环.

对于含幺交换环 κ 上的任一个可数无穷序列 $X=(X_0,X_1,\cdots,X_n,\cdots)\in\prod_{n\geq 0}\kappa$, 自身的指数运算由下面的定义给出.

定义 3.1.2 $X^m:=({X_0}^m,{X_1}^m,\cdots,{X_n}^m,\cdots)$, 其中

$${X_n}^m=\begin{cases}\mathbf{1},\ m=0,\\ \prod\limits_{i=1}^{m}X_n, m\in\mathbb{Z}_{>0}.\end{cases}$$

基于定义3.1.2给出的指数运算规则, 由任一个序列 X 导出的相邻一级 Witt 多项式满足下面的关系式.

命题 3.1.3 $W_{n+1}(X,\pi)=W_n(X^\pi,\pi)+\boldsymbol{\pi}^{n+1}X_{n+1}$.

证明 成立以下推理

$$\begin{aligned}&W_n(X,\pi)=\sum_{i=0}^{n}\boldsymbol{\pi}^i{X_i}^{\pi^{n-i}}.\\ \Longrightarrow&W_n(X^\pi,\pi)=\sum_{i=0}^{n}\boldsymbol{\pi}^i(X_i^\pi)^{\pi^{n-i}}=\sum_{i=0}^{n}\boldsymbol{\pi}^i(X_i)^{\pi^{(n+1)-i}}.\\ \Longrightarrow&W_n(X^\pi,\pi)+\boldsymbol{\pi}^{n+1}X_{n+1}=\sum_{i=0}^{n+1}\boldsymbol{\pi}^i(X_i)^{\pi^{(n+1)-i}}=W_{n+1}(X,\pi).\end{aligned}$$

至此, 明所欲证. □

反过来, 导出的 Witt 多项式也可以通过逐步反解的方法来表示序列 X 的每一个分量 X_i. 更具体地, 记多项式环 $Z':=\mathbb{Z}[\boldsymbol{\pi}^{-1}]$, 显然有 $\mathbb{Z}\subset Z'$. 有如下命题.

命题 3.1.4 $\forall i \in \mathbb{Z}_{\geq 0}$, $\exists \Phi_i \in Z'[Y_0, Y_1, \cdots]$, 使得

$$X_i = \Phi_i(W_0, W_1, \cdots).$$

证明 当 $i = 0$ 时, 显然有 $X_0 = W_0 \in Z[W_0] \subset Z'[W_0, W_1, \cdots]$.
假设 X 的前 k 个分量均满足

$$X_i = \Phi_i(W_0, W_1, \cdots),\ \exists \Phi_i \in Z'[Y_0, Y_1, \cdots],\ i = 0,\ 1,\ \cdots,\ k-1.$$

则对于第 $k+1$ 个分量 X_k, 由

$$W_k = {X_0}^{\pi^k} + \pi {X_1}^{\pi^{k-1}} + \cdots + \boldsymbol{\pi}^k X_k$$

可以反解出

$$\begin{aligned} X_k &= -\boldsymbol{\pi}^{-k}\left({X_0}^{\pi^k} + \pi {X_1}^{\pi^{k-1}} + \cdots + \pi^{k-1} {X_{k-1}}^{\pi}\right) + \boldsymbol{\pi}^{-k} W_k. \\ &= -\left(\boldsymbol{\pi}^{-k} {\Phi_0}^{\pi^k} + \boldsymbol{\pi}^{-(k-1)} {\Phi_1}^{\pi^{k-1}} + \cdots + \boldsymbol{\pi}^{-1} {\Phi_{k-1}}^{\pi}\right) + \boldsymbol{\pi}^{-k} W_k. \\ &=: \Phi_k. \end{aligned}$$

由 $\boldsymbol{\pi}^{-1}$, $\boldsymbol{\pi}^{-2}$, $\cdots$, $\boldsymbol{\pi}^{-k}$; Φ_0, Φ_1, $\cdots$, Φ_{k-1}; $W_k \in Z'[W_0, W_1, \cdots]$ 和多项式环 $Z'[W_0, W_1, \cdots]$ 的环运算封闭性, 可得 $\Phi_k \in Z'[Y_0, Y_1, \cdots]$. 至此, 由第二数学归纳法, 结论得证. □

例子 3.1.5 $X_0 = W_0$.

例子 3.1.6 $X_1 = \boldsymbol{\pi}^{-1}(-{W_0}^{\pi} + W_1) = -\boldsymbol{\pi}^{-1}{W_0}^{\pi} + \boldsymbol{\pi}^{-1} W_1$.

例子 3.1.7 $X_2 = \boldsymbol{\pi}^{-2}\left(-\boldsymbol{\pi} {X_1}^{\pi} - {X_0}^{\pi^2} + W_2\right) = -\boldsymbol{\pi}^{-(\pi+1)}(-{W_0}^{\pi} + W_1)^{\pi} - \boldsymbol{\pi}^{-2}{W_0}^{\pi^2} + \boldsymbol{\pi}^{-2} W_2$.

现在考虑由两个序列 X 和 Y 分别导出的两个 Witt 多项式组 $(W_n(X))_{n\geq 0}$ 和 $(W_n(Y))_{n\geq 0}$. 基于此, 我们对上面的命题3.1.4作一个推广.

命题 3.1.8 $\forall \Phi \in \mathbb{Z}[X, Y]$, 存在 $(\varphi_0, \varphi_1, \cdots, \varphi_n, \cdots)$ 满足

$$\varphi_i \in Z'[X_0, \cdots, X_n, \cdots; Y_0, \cdots, Y_n, \cdots],\ \forall i \in \mathbb{Z}_{\geq 0},$$

成立

$$W_n(\varphi_0, \cdots, \varphi_n, \cdots) = \Phi(W_n(X_0, \cdots), W_n(Y_0, \cdots)),\ n = 0,\ 1,\ \cdots.$$

证明 当 $n = 0$ 时, 成立 $W_0(\varphi_0, \cdots, \varphi_n, \cdots) = \Phi(W_0(X_0, \cdots), W_0(Y_0, \cdots))$, 即有

$$\varphi_0 = \Phi(X_0, Y_0) \in \mathbb{Z}[X_0, Y_0] \subset Z'[X_0, \cdots, X_n, \cdots; Y_0, \cdots, Y_n, \cdots].$$

假设对 (φ_n) 的前 k 个分量都成立 $\varphi_i \in Z'[X_0,\cdots,X_n,\cdots;Y_0,\cdots,Y_n,\cdots]$, $i=0,\ 1,\ \cdots,\ k-1$. 考虑第 $k+1$ 个等式

$$\sum_{i=0}^{k} \boldsymbol{\pi}^i {\varphi_i}^{\pi^{k-i}} = W_k(\varphi_0,\cdots,\varphi_k) = \Phi\left(W_k(X_0,\cdots), W_k(Y_0,\cdots)\right).$$

$$\Longrightarrow \boldsymbol{\pi}^k \varphi_k = \Phi\left(W_k(X_0,\cdots), W_k(Y_0,\cdots)\right) - \sum_{i=0}^{k-1} \boldsymbol{\pi}^i {\varphi_i}^{\pi^{k-i}}.$$

$$\Longrightarrow \varphi_k = \boldsymbol{\pi}^{-k}\Phi\left(W_k(X_0,\cdots), W_k(Y_0,\cdots)\right) - \sum_{j=1}^{k} \boldsymbol{\pi}^{-j} {\varphi_{-j+k}}^{\pi^j}.$$

根据

$$\begin{aligned}
\boldsymbol{\pi}^{-1},\ \boldsymbol{\pi}^{-2},\ \cdots,\ \boldsymbol{\pi}^{-k};\ \varphi_0,\ \varphi_1,\ \cdots,\ \varphi_{k-1} &\in Z'[X_0,\cdots,X_n,\cdots;Y_0,\cdots,Y_n,\cdots],\\
\Phi\left(W_k(X_0,\cdots), W_k(Y_0,\cdots)\right) &= \Phi(X_0,\cdots,X_n,\cdots;Y_0,\cdots,Y_n,\cdots).\\
&\in \mathbb{Z}[X_0,\cdots,X_n,\cdots;Y_0,\cdots,Y_n,\cdots].\\
&\subset Z'[X_0,\cdots,X_n,\cdots;Y_0,\cdots,Y_n,\cdots],
\end{aligned}$$

和多项式环 $Z'[X_0,\cdots,X_n,\cdots;Y_0,\cdots,Y_n,\cdots]$ 的环运算封闭性, 得到

$$\varphi_k \in Z'[X_0,\cdots,X_n,\cdots;Y_0,\cdots,Y_n,\cdots].$$

至此, 由第二数学归纳法, 结论得证. □

例子 3.1.9 规定命题*3.1.8*中的 $\Phi \in \mathbb{Z}[X,Y]$ 的形式为 $\Phi = X+Y$, 此时计算得

$$\begin{aligned}
S_0 :&= \varphi_0 = X_0 + Y_0,\\
S_1 :&= \varphi_1 = X_1 + Y_1 + \frac{{X_0}^{\pi} + {Y_0}^{\pi} - (X_0+Y_0)^{\pi}}{\boldsymbol{\pi}}.\\
&= X_1 + Y_1 - \sum_{v=1}^{\pi-1} \frac{1}{\boldsymbol{\pi}} \binom{\pi}{v} {X_0}^v {Y_0}^{\pi-v},\\
&\cdots\cdots
\end{aligned}$$

例子 3.1.10 规定命题*3.1.8*中的 $\Phi \in \mathbb{Z}[X,Y]$ 的形式为 $\Phi = X \bullet Y$, 此时计算得

$$\begin{aligned}
P_0 :&= \varphi_0 = X_0 \bullet Y_0,\\
P_1 :&= \varphi_1 = {Y_0}^{\pi} \bullet X_1 + Y_1 \bullet {X_0}^{\pi} + \boldsymbol{\pi} X_1 \bullet Y_1,\\
&\cdots\cdots
\end{aligned}$$

此外, 在一些特殊情况下, 序列 X 和 Y 的相等关系也可以迁移到 Witt 多项式组 $(W_n(X))_{n\geq 0}$ 和 $(W_n(Y))_{n\geq 0}$ 的相等关系. 具体内容由如下命题给出.

命题 3.1.11 设 κ 是一个含幺交换环, 素数 $\pi \neq \mathrm{char}(\kappa)$. 若 $\boldsymbol{\pi}$ 在 κ 中非零因子, 则成立等价关系

$$\begin{aligned}
&X = (X_0,\cdots X_n,\cdots) = (Y_0,\cdots,Y_n,\cdots) = Y.\\
\Longleftrightarrow\ &(W_0(X),\cdots,W_n(X),\cdots) = (W_0(Y),\cdots,W_n(Y),\cdots).
\end{aligned}$$

证明 若 $X=Y$, 由 *Witt* 多项式组的构造方式, 显然成立 $(W_n(X))_{n\geq 0}=(W_n(Y))_{n\geq 0}$. 反之, 若成立 $(W_n(X))_{n\geq 0}=(W_n(Y))_{n\geq 0}$, 我们逐级地比对同级的 *Witt* 多项式.

- $$W_0(X)=W_0(Y). \iff X_0=Y_0. \tag{3.1.1}$$

- $$W_1(X)=W_1(Y). \iff {X_0}^{\pi}+\boldsymbol{\pi}X_1={Y_0}^{\pi}+\boldsymbol{\pi}Y_1. \tag{3.1.2}$$

  由式 *(3.1.1)* 和式 *(3.1.2)*, 有 $\boldsymbol{\pi}(X_1-Y_1)=0$. 由于 $\boldsymbol{\pi}$ 非环 κ 中的零因子, 因此只能是

  $$X_1-Y_1=0. \implies X_1=Y_1. \tag{3.1.3}$$

- $$W_2(X)=W_2(Y). \iff {X_0}^{\pi^2}+\boldsymbol{\pi}{X_1}^{\pi}+\boldsymbol{\pi}^2X_2={Y_0}^{\pi^2}+\boldsymbol{\pi}{Y_1}^{\pi}+\boldsymbol{\pi}^2Y_2. \tag{3.1.4}$$

  由式 *(3.1.1)*, 式 *(3.1.3)* 和式 *(3.1.4)*, 有 $\boldsymbol{\pi}^2(X_2-Y_2)=0$. 由于 $\boldsymbol{\pi}$ 非环 κ 中的零因子, 因此 $\forall\lambda\in\kappa_{\neq 0}$, $\boldsymbol{\pi}\lambda\neq 0$, 因此也就有

  $$\boldsymbol{\pi}(\boldsymbol{\pi}\lambda)\neq 0. \implies \boldsymbol{\pi}^2\lambda\neq 0,$$

  即 π^2 也非环 κ 中的零因子. 因此只能是

  $$X_2-Y_2=0. \implies X_2=Y_2.$$

- ……

重复以上操作即可证得 $X=Y$. □

3.2 Witt 向量的环结构

有了 § 3.1 节提供的 Witt 多项式和 Witt 向量的基础后, 在这一节我们来讨论由含幺交换环 κ 上 Witt 向量构成的集合 $\prod_{n\geq 0}\kappa$ 的环结构. 首先我们指出, $\prod_{n\geq 0}\kappa$ 关于平凡加法和平凡乘法运算可以构成一个环. 具体地, 有下面的命题.

命题 3.2.1 设 $(\kappa,+,\bullet)$ 是一个含幺交换环. 对 $\prod_{n\geq 0}\kappa$, $\forall X:=(X_n)_{n\geq 0}$,$Y:=(Y_n)_{n\geq 0}\in\prod_{n\geq 0}\kappa$, 定义其上的运算 $\oplus$ 和 $\odot$ 为

$$\begin{aligned}(X_n)_{n\geq 0}\oplus(Y_n)_{n\geq 0}&:=(X_n+Y_n)_{n\geq 0},\\(X_n)_{n\geq 0}\odot(Y_n)_{n\geq 0}&:=(X_n\bullet Y_n)_{n\geq 0}.\end{aligned}$$

则 $\left(\prod_{n\geq 0}\kappa,\oplus,\odot\right)$ 构成一个含幺交换环, 记为 $\mathfrak{O}(\kappa)$.

证明 此定义下 X, $Y\in\prod_{n\geq 0}\kappa$ 之间的 $\oplus$, $\odot$ 运算实质上归结到 X, Y 的同一级分量 X_n, $Y_n\in\kappa$ 之间的 $+$, $\bullet$ 运算, 因此 $\left(\prod_{n\geq 0}\kappa,\oplus,\odot\right)$ 全部的环运算性质继承于或可溯源于环 $(\kappa,+,\bullet)$. 结论是显然的. □

更重要地, $\prod_{n\geq 0}\kappa$ 上可能存在其他的环结构, 而事实也是如此. 在这方面 E. Witt [12] [5] 作出了重大贡献. 他设计了一种极为巧妙的环结构, 具体来说, $\forall X:=(X_n)_{n\geq 0}$, $Y:=(Y_n)_{n\geq 0}\in\prod_{n\geq 0}\kappa$, 他定义运算 $\oplus$ 和 $\odot$ 为

$$\begin{aligned}(X_n)_{n\geq 0}\oplus(Y_n)_{n\geq 0}&:=(S_n)_{n\geq 0},\ \text{s.t. } W_n(S_0,\cdots,S_n,\cdots)=W_n(X)+W_n(Y),\\(X_n)_{n\geq 0}\odot(Y_n)_{n\geq 0}&:=(P_n)_{n\geq 0},\ \text{s.t. } W_n(P_0,\cdots,P_n,\cdots)=W_n(X)\bullet W_n(Y).\end{aligned}\tag{3.2.1}$$

首先, 命题3.1.8揭示了

$$(S_n)_{n\geq 0},\ (P_n)_{n\geq 0}\in\prod_{n\geq 0}Z'[X_0,\cdots,X_n,\cdots;Y_0,\cdots,Y_n,\cdots].$$

即满足式 (3.2.1) 的序列 $(S_n)_{n\geq 0}$, $(P_n)_{n\geq 0}$ 是存在的. 而命题3.1.11又说明了在 Witt 多项式系数 $\boldsymbol{\pi}$ 非含幺交换环 κ 中零因子的情况下, 满足式 (3.2.1) 的序列 $(S_n)_{n\geq 0}$, $(P_n)_{n\geq 0}$ 是唯一的. 由此引出下面奠基性的命题.

命题 3.2.2 当 *Witt* 多项式系数 $\boldsymbol{\pi}$ 非含幺交换环 κ 中的零因子时, 式 *(3.2.1)* 定义的环运算是一个良定义.

本小节的主要任务就是来验证 $\prod_{n\geq 0}\kappa$ 在式 (3.2.1) 给出的运算下确实构成一个环 [13] . 为了系统地进行论述, 我们将后面的内容分成几个小块: § 3.2.1 节对讨论运算封闭性所涉及的模理想同余概念作一些必要的介绍; § 3.2.2 节对运算封闭性作正式的论述; § 3.2.3 节再对其他的环性质进行验证.

[12] Ernst Witt, 1911.6—1991.7, 德国数学家.

[13] 严格上说, 还需要加上一些限制条件, § 3.2.3 节会明确指出, 不过这无伤大雅.

3.2.1 模理想同余简述

实际上本文前面某些地方也略有涉及模理想同余的使用. 现正式引入该概念如下.

定义 3.2.1.1 设 $\Re$ 是一个环, I 是 $\Re$ 的一个双边理想, $\forall x,\ y \in \Re$, 称 $x,\ y$ **模理想 I 同余**, 若满足

$$x + I = y + I,$$

记为 $x \equiv y \mod I$.

模理想同余有一个常用的等价说法.

定理 3.2.1.2 $x \equiv y \mod I$ 的充分必要条件是 $x - y \in I$, 即 $\exists z \in I$, 使得 $x = y + z$.

证明

1. ($\Rightarrow$)
   $x \equiv y \mod I. \Rightarrow x + I = y + I$, 即 $\exists a,\ b \in I$, 成立

   $$x + a = y + b. \implies x = y + (b - a).$$

   由理想 I 是 $\Re$ 的子环, 运算具有封闭性, 得到 $b - a \in I$.

2. ($\Leftarrow$)
   若 $\exists z \in I$, 使得 $x = y + z$, 则有

   $$x + I = y + z + I = y + (z + I) = y + I.$$

   明所欲证. □

模理想同余有以下几个基本的性质.

性质 3.2.1.3 (自反性) $x \equiv x \mod I$.

证明 $x + I = x + I.$ □

性质 3.2.1.4 (交换性) 若 $x \equiv y \mod I$, 则 $y \equiv x \mod I$.

证明 $x + I = y + I. \Rightarrow y + I = x + I.$ □

性质 3.2.1.5 (传递性) 若 $x \equiv y \mod I$ 且 $y \equiv z \mod I$, 则有 $x \equiv z \mod I$.

证明

$$\left.\begin{aligned} x + I = y + I. \\ y + I = z + I. \end{aligned}\right\} \implies x + I = z + I.$$

明所欲证. □

性质 3.2.1.6 (乘法运算) 若 $x_1 \equiv y_1 \mod I$, $x_2 \equiv y_2 \mod I$, 则有 $x_1x_2 \equiv y_1y_2 \mod I$.

证明 由 $x_1 + I = y_1 + I$, $x_2 + I = y_2 + I$, 有

$$\begin{aligned} &(x_1 + I)(x_2 + I) = (y_1 + I)(y_2 + I). \\ \Longrightarrow\ & x_1x_2 + x_1I + Ix_2 + I = y_1y_2 + y_1I + Iy_2 + I. \end{aligned} \tag{3.2.1.2}$$

由双边理想 I 的乘法吸收性, 有 x_1I, y_1I, Ix_2, $Iy_2 \subseteq I$, 因此也就有

$$x_1I + Ix_2 + I = y_1I + Iy_2 + I = I. \tag{3.2.1.3}$$

结合式 *(3.2.1.2)* 和式 *(3.2.1.3)*, 即得

$$x_1x_2 + I = y_1y_2 + I.$$

明所欲证. □

特别地, 若 $\Re$ 是一个交换环, 则额外满足下面的性质.

性质 3.2.1.7 (加法运算) 若 $x_1 \equiv y_1 \mod I$, $x_2 \equiv y_2 \mod I$, 则有 $x_1+x_2 \equiv y_1+y_2 \mod I$.

证明

$$\left.\begin{aligned} x_1 + I = y_1 + I. \\ x_2 + I = y_2 + I. \end{aligned}\right\} \Longrightarrow (x_1 + I) + (x_2 + I) = (y_1 + I) + (y_2 + I).$$

$$\xrightarrow{\Re\text{的交换性.}} (x_1 + x_2) + (I + I) = (y_1 + y_2) + (I + I).$$

$$\Longrightarrow (x_1 + x_2) + I = (y_1 + y_2) + I.$$

明所欲证. □

性质 3.2.1.8 (减法运算) 若 $x + y \equiv z \mod I$, 则有 $x \equiv z - y \mod I$.

证明 由性质*3.2.1.7*, 有

$$\begin{aligned} &x + y \equiv z \mod I. \\ \Longrightarrow\ & x = (x + y) + (-y) \equiv z + (-y) = z - y \mod I. \end{aligned}$$

明所欲证. □

于是在 $\Re$ 是交换环的情况下, 我们又可以导出模理想同余的另一充要条件以及一个常用的延伸性质.

定理 3.2.1.9 若 $\Re$ 是交换环, 则 $x \equiv y \mod I$ 的充要条件是 $x - y \equiv 0 \mod I$.

性质 3.2.1.10 若 $\Re$ 是交换环, 且 $X_{0,1,\cdots,n} \equiv Y_{0,1,\cdots,n} \mod I$, 则 $\forall \Phi \in \Re[X_0, X_1, \cdots, X_n]$, 成立

$$\Phi(X_0, X_1, \cdots, X_n) \equiv \Phi(Y_0, Y_1, \cdots, Y_n) \mod I.$$

证明 基于乘法运算性质*3.2.1.6* 和加法运算性质*3.2.1.7*, 通过线性组合的方式, 结论是显然的. □

注记 在 $\Re$ 是一个含幺交换环的情况下, 通常研究

$$\Phi \in \mathbb{Z}\left[X_0, X_1, \cdots, X_n\right].$$

下面我们先给出一个引理, 然后基于此研究 § 3.2.2 节涉及到的一类特殊模理想同余.

引理 3.2.1.11 设 $\Re$ 是一个含幺交换环, 则 $\forall \lambda \in \Re$, 由 λ 生成的主理想 $\langle \lambda \rangle$ 可表示为

$$\langle \lambda \rangle = \lambda \Re.$$

证明 见冯克勤 *[6, P66].* □

引理3.2.1.11说明了当 $\Re$ 是一个含幺交换环时, $\forall \lambda \in \Re$, $\lambda\Re$ 一定是 $\Re$ 的一个理想. 又由 $\Re$ 的环运算封闭性, $\forall n \in \mathbb{Z}_{\geq 0}$, $\lambda^n \in \Re$, $\lambda^n\Re$ 也是一个 $\Re$ 的, 由 λ^n 生成的主理想. 因此我们可以考虑以下的模理想同余的关系

$$x \equiv y \mod \lambda^n \Re,\ x,\ y \in \Re.$$

这类同余关系也满足一些特殊的性质. 这里只介绍后续可能用到的一个性质.

性质 3.2.1.12 在 $\Re$ 是含幺交换环的前提下, 若 $x \equiv y \mod I$, 则成立

$$\lambda x \equiv \lambda y \mod \lambda I,\ \forall \lambda \in \Re.$$

证明

$$\begin{aligned} & x \equiv y \mod I. \\ \Longrightarrow\ & x + I = y + I. \\ \Longrightarrow\ & \lambda x + \lambda I = \lambda\left(x + I\right) = \lambda\left(y + I\right) = \lambda y + \lambda I. \end{aligned}$$

明所欲证. □

至此, 我们对模理想同余作了一个大致而必要的介绍.

3.2.2 环运算封闭性

这一小节我们正式来讨论 $\oplus$, $\odot$ 的运算封闭性. 这个性质的最终证明需要立足于两个引理. 下面我们先引入两个必要的初等数论定理, 为该两个引理的提出和证明作铺垫.

引理 3.2.2.1 设 p 是一个素数, 成立

$$p|\binom{p}{k},\ \forall k\in\{1,\ 2,\ \cdots,\ p-1\}.$$

证明 首先, 显然成立

$$\gcd(p,i)=1,\ \forall i\in\{1,\ 2,\ \cdots,\ p-1\}.$$

因此对于任一个选定的 $1\leq k\leq p-1$, 成立

$$\gcd(p,k!\,(p-k)!)=1. \tag{3.2.2.1}$$

而由定理*A.1.2*, 成立

$$(k!\,(p-k)!)|\,p!. \tag{3.2.2.2}$$

由式 *(3.2.2.1)* 和式 *(3.2.2.2)*, 成立

$$\binom{p}{k}/p=\frac{(p-1)!}{k!\,(p-k)!}\in\mathbb{Z}.\implies p|\binom{p}{k}.$$

至此, 明所欲证. □

引理 3.2.2.2 (Fermat) 设 $\Im$ 是一个含幺交换环, $p\neq\mathrm{char}(\Im)$ 是一个素数, $\boldsymbol{p}:=\sum_{i=1}^{p}\mathbf{1}\in\Im$. $\forall a\in\Im$, 成立同余式

$$a^p\equiv a\mod\boldsymbol{p}.$$

证明 若干种证法以及狭义和广义的结论可以参见王志兰 *[13]*. □

下面我们开始逐步地引入第一个目标引理3.2.2.5. 该引理的证明过程参考了 Witt [5, Lemma].

命题 3.2.2.3 设 π 是一个素数, $\Im$ 是一个特征不为 π 的含幺交换环, 并记 $\boldsymbol{\pi}:=\sum_{i=1}^{\pi}\mathbf{1}\in\Im$. 则对任意的 $x,\ y\in\Im$, 成立推理

$$x\equiv y\mod\boldsymbol{\pi}^r\Im,\ \exists r\in\mathbb{Z}_{\geq 0}.\implies x^\pi\equiv y^\pi\mod\boldsymbol{\pi}^{r+1}\Im.$$

证明 首先, $\Im$ 可以视为自己的一个理想, 而又由于 $x,\ y\in\Im$, 则一定成立

$$x\equiv y\mod\boldsymbol{\pi}^0\Im.$$

r 的存在性得以保证.

在此基础上, $x\equiv y\mod\boldsymbol{\pi}^r\Im$ 蕴涵了 $\exists z\in\Im$ 使得 $x-y=\boldsymbol{\pi}^r z$, 即有

$$x=y+\boldsymbol{\pi}^r z. \tag{3.2.2.3}$$

式 *(3.2.2.3)* 两边都取 π 次幂, 得到

$$x^{\pi}=(y+\boldsymbol{\pi}^{r}z)^{\pi}=y^{\pi}+\binom{\pi}{1}(\boldsymbol{\pi}^{r}z)\,y^{\pi-1}+\cdots+\binom{\pi}{\pi-1}(\boldsymbol{\pi}^{r}z)^{\pi-1}y+(\boldsymbol{\pi}^{r}z)^{\pi}. \tag{3.2.2.4}$$

根据引理*3.2.2.1*, 可令 $\binom{\pi}{k}=\pi\varphi_k$, 其中 $\varphi_k\in\mathbb{Z}$. 于是式 *(3.2.2.4)* 可以改写为

$$\begin{aligned}x^{\pi}=&y^{\pi}+\boldsymbol{\pi}\boldsymbol{\varphi_1}(\boldsymbol{\pi}^{r}z)\,y^{\pi-1}+\cdots+\boldsymbol{\pi}\boldsymbol{\varphi_{\pi-1}}(\boldsymbol{\pi}^{r}z)^{\pi-1}y+(\boldsymbol{\pi}^{r}z)^{\pi}.\\ =&y^{\pi}+\boldsymbol{\pi}^{r+1}\left(\boldsymbol{\pi}^{0}\boldsymbol{\varphi_1}zy^{\pi-1}+\cdots+\boldsymbol{\pi}^{(\pi-2)r}\boldsymbol{\varphi_{\pi-1}}z^{\pi-1}y+\boldsymbol{\pi}^{(\pi-1)r-1}z^{\pi}\right).\\ =&y^{\pi}+\boldsymbol{\pi}^{r+1}\left(\boldsymbol{\pi}^{(\pi-1)r-1}z^{\pi}+\sum_{v=1}^{\pi-1}\boldsymbol{\pi}^{v-1}\boldsymbol{\varphi_v}z^{v}y^{\pi-v}\right). \qquad (3.2.2.5)\\ =:&y^{\pi}+\boldsymbol{\pi}^{r+1}Q. \qquad (3.2.2.6)\end{aligned}$$

由于 $\pi\geq 2$ 是一个素数, 因此式 *(3.2.2.5)* 中的指数部分 $(\pi-1)\,r-1$, $\pi-2\geq 0$, 且显然有 $\pi-v\geq 0$, $\forall v=1,\,2,\,\cdots,\,\pi-1$. 再根据 y, z, $\boldsymbol{\pi}$; $\boldsymbol{\varphi_1}$, $\boldsymbol{\varphi_2}$, $\cdots$, $\boldsymbol{\varphi_{\pi-1}}\in\mathfrak{S}$ 和环 $\mathfrak{S}$ 的运算封闭性, 得 $Q\in\mathfrak{S}$, 由式 *(3.2.2.6)* 即可推得 $x^{\pi}\equiv y^{\pi}\mod\boldsymbol{\pi}^{r+1}\mathfrak{S}$. □

推论 3.2.2.4 设 π 是一个素数, $\mathfrak{S}$ 是一个特征不为 π 的含幺交换环, 并记 $\boldsymbol{\pi}:=\sum_{i=1}^{\pi}\mathbf{1}\in\mathfrak{S}$. 则对任意的 x, $y\in\mathfrak{S}$, 成立推理

$$x\equiv y\mod\boldsymbol{\pi}^{r}\mathfrak{S},\ \exists r\in\mathbb{Z}_{\geq 0}.\implies x^{\pi^{n}}\equiv y^{\pi^{n}}\mod\boldsymbol{\pi}^{r+n}\mathfrak{S},\ \forall n\in\mathbb{Z}_{\geq 0}.$$

证明 $n=0$ 的情况是显然的. $n=1$ 的情况已经由命题*3.2.2.3*给出. 由于 $\pi\geq 2$ 是一个素数, 由 x, $y\in\mathfrak{S}$ 和环 $\mathfrak{S}$ 的运算封闭性, 仍有 x^{π}, $y^{\pi}\in\mathfrak{S}$. 成立以下推理

$$\begin{aligned}&x\equiv y\mod\boldsymbol{\pi}^{r}\mathfrak{S}.\\ \implies&x^{\pi}\equiv y^{\pi}\mod\boldsymbol{\pi}^{r+1}\mathfrak{S}.\\ \implies&x^{\pi^{2}}=(x^{\pi})^{\pi}\equiv(y^{\pi})^{\pi}=y^{\pi^{2}}\mod\boldsymbol{\pi}^{(r+1)+1}\mathfrak{S}=\boldsymbol{\pi}^{r+2}\mathfrak{S}.\end{aligned}$$

因此 $n=2$ 的情况是成立的. 依次类推, 可证得 $\forall n\in\mathbb{Z}_{\geq 2}$ 的情况. □

引理 3.2.2.5 设 $\mathfrak{S}$ 是一个含幺交换环, $\pi\neq\operatorname{char}(\mathfrak{S})$ 是一个素数, $\boldsymbol{\pi}:=\sum_{i=1}^{\pi}\mathbf{1}\in\mathfrak{S}$. 对任意的 $X:=(X_n)_{n\geq 0}$, $Y:=(Y_n)_{n\geq 0}\in\prod_{n\geq 0}\mathfrak{S}$, 成立推理

$$X_v\equiv Y_v\mod\boldsymbol{\pi}^{r}\mathfrak{S},\ \forall v\in\{0,\,1,\,\cdots,\,n\}.\implies W_n(X)\equiv W_n(Y)\mod\boldsymbol{\pi}^{r+n}\mathfrak{S}.$$

证明 首先由推论*3.2.2.4*可得

$$\begin{aligned}&X_v\equiv Y_v\mod\boldsymbol{\pi}^{r}\mathfrak{S}.\\ \implies&{X_v}^{\pi}\equiv{Y_v}^{\pi}\mod\boldsymbol{\pi}^{r+1}\mathfrak{S}.\\ \implies&({X_v}^{\pi})^{\pi^{n-1-v}}\equiv({Y_v}^{\pi})^{\pi^{n-1-v}}\mod\boldsymbol{\pi}^{r+1+(n-1-v)}\mathfrak{S}=\boldsymbol{\pi}^{r+n-v}\mathfrak{S}.\\ \implies&\boldsymbol{\pi}^{v}({X_v}^{\pi})^{\pi^{n-v}}\equiv\boldsymbol{\pi}^{v}({Y_v}^{\pi})^{\pi^{n-v}}\mod\boldsymbol{\pi}^{r+n-v+v}\mathfrak{S}=\boldsymbol{\pi}^{r+n}\mathfrak{S},\ \forall v\in\{0,\,1,\,\cdots,\,n-1\}.\end{aligned}$$

结合定义*3.1.2*和 *Witt* 多项式的构造方式, 有

$$W_{n-1}(X^{\pi})=\sum_{v=0}^{n-1}\boldsymbol{\pi}^{v}({X_v}^{\pi})^{\pi^{n-v}}\equiv\sum_{v=0}^{n-1}\boldsymbol{\pi}^{v}({Y_v}^{\pi})^{\pi^{n-v}}=W_{n-1}(Y^{\pi})\mod\boldsymbol{\pi}^{r+n}\mathfrak{S}.$$

再根据命题*3.1.3*给出的相邻级 *Witt* 多项式关系, 可得

$$\begin{aligned}&W_{n-1}\left(X^{\pi}\right)-W_{n-1}\left(Y^{\pi}\right).\\=&\left(W_n\left(X\right)-\boldsymbol{\pi}^nX_n\right)-\left(W_n\left(Y\right)-\boldsymbol{\pi}^nY_n\right).\\=&\left(W_n\left(X\right)-W_n\left(Y\right)\right)-\boldsymbol{\pi}^n\left(X_n-Y_n\right)\equiv0\mod\boldsymbol{\pi}^{r+n}\Im.\end{aligned}\tag{3.2.2.7}$$

另一方面, 又成立

$$\begin{aligned}&X_n\equiv Y_n\mod\boldsymbol{\pi}^r\Im.\\\Longrightarrow\ &X_n-Y_n\equiv0\mod\boldsymbol{\pi}^r\Im.\\\Longrightarrow\ &\boldsymbol{\pi}^n\left(X_n-Y_n\right)\equiv0\mod\boldsymbol{\pi}^{r+n}\Im.\end{aligned}\tag{3.2.2.8}$$

由式 *(3.2.2.7)* 和式 *(3.2.2.8)*, 可得

$$W_n\left(X\right)-W_n\left(Y\right)-0\equiv0\mod\boldsymbol{\pi}^{r+n}\Im.\implies W_n\left(X\right)\equiv W_n\left(Y\right)\mod\boldsymbol{\pi}^{r+n}\Im.$$

至此, 明所欲证. □

下面我们再引入第二个目标引理3.2.2.6及其推论.

引理 3.2.2.6 设 $\Im$ 是一个含幺交换环, $\pi\neq\mathrm{char}\left(\Im\right)$ 是一个素数, $\boldsymbol{\pi}:=\sum_{i=1}^{\pi}\mathbf{1}\in\Im$. $\forall\Phi\in\mathbb{Z}\left[X,Y\right]$, 成立

$$\Phi(X,Y)^{\pi}\equiv\Phi\left(X^{\pi},Y^{\pi}\right)\mod\boldsymbol{\pi}\Im,\ \forall X,\ Y\in\Im.$$

证明 由 $\Phi\in\mathbb{Z}\left[X,Y\right]$ 是二元有限和形式, 设

$$\Phi\left(X,Y\right)=\sum_{\substack{0\leq i\leq r\\0\leq j\leq s}}\boldsymbol{k_{ij}}X^iY^j,\ k_{ij}\in\mathbb{Z}.$$

结合定义*3.1.2*给出的指数运算定义, 于是有

$$\begin{aligned}&\Phi(X,Y)^{\pi}-\Phi\left(X^{\pi},Y^{\pi}\right)\\=&\left(\sum_{\substack{0\leq i\leq r\\0\leq j\leq s}}\boldsymbol{k_{ij}}X^iY^j\right)^{\pi}-\sum_{\substack{0\leq i\leq r\\0\leq j\leq s}}\boldsymbol{k_{ij}}X^{\pi i}Y^{\pi j}.\\=&\sum_{\substack{0\leq i\leq r\\0\leq j\leq s}}\left(\boldsymbol{k}_{\boldsymbol{ij}}^{\pi}-\boldsymbol{k_{ij}}\right)X^{\pi i}Y^{\pi i}+\\&\sum_{(n_{i,j})}\binom{\pi}{n_{0,0}}\left(X^0Y^0\right)^{\pi-n_{0,0}}\prod_{0\leq u\leq r}\prod_{1\leq v\leq s}\binom{n_{u,v-1}}{n_{u,v}}\left(\boldsymbol{k_{uv}}X^uY^v\right)^{n_{u,v-1}-n_{u,v}}.\\=&:J+K.\end{aligned}$$

K 中的求和号 $\sum_{(n_{i,j})}$ 表示展布在一切满足条件

$$\begin{aligned}&\pi\geq n_{0,0}\geq n_{0,1}\geq\cdots\geq n_{0,s}\geq n_{1,0}\geq\cdots\geq n_{1,s}\geq\cdots\geq n_{r,s}\geq0,\\&\exists n_{i,j},\ \text{s.t. }n_{i,j}\neq0,\ \pi,\end{aligned}$$

的序列

$$(n_{i,j}) \in \prod_{\substack{0\leq i\leq r\\ 0\leq j\leq s}} \mathbb{Z}_{\geq 0}$$

之上. 由引理*3.2.2.2*得 $J \in \boldsymbol{\pi}\mathfrak{S}$. 由引理*3.2.2.1*得 $K \in \boldsymbol{\pi}\mathfrak{S}$. 于是有

$$\begin{aligned} &\Phi(X,Y)^{\pi} - \Phi\left(X^{\pi}, Y^{\pi}\right) \in \boldsymbol{\pi}\mathfrak{S}. \\ \Longrightarrow\ &\Phi(X,Y)^{\pi} - \Phi\left(X^{\pi}, Y^{\pi}\right) \equiv 0 \mod \boldsymbol{\pi}\mathfrak{S}. \\ \Longrightarrow\ &\Phi(X,Y)^{\pi} \equiv \Phi\left(X^{\pi}, Y^{\pi}\right) \mod \boldsymbol{\pi}\mathfrak{S}. \end{aligned}$$

至此, 明所欲证. □

推论 3.2.2.7 设 $\mathfrak{S}$ 是一个含幺交换环, $\pi \neq \operatorname{char}(\mathfrak{S})$ 是一个素数, $\boldsymbol{\pi} := \sum_{i=1}^{\pi} \mathbf{1} \in \mathfrak{S}$. 对任一个 $X := (X_n) \in \prod_{n\geq 0} \mathfrak{S}$, 成立

$$W_n(X)^{\pi} \equiv W_n\left(X^{\pi}\right) \mod \boldsymbol{\pi}\mathfrak{S},\ \forall n = 0,\ 1,\ \cdots.$$

注记 同引理*3.2.2.6*中的证明思想, 可将该引理中 $\Phi \in \mathbb{Z}[X,Y]$ 的二元情况推广到 $\Psi \in \mathbb{Z}[X_0, X_1, \cdots, X_n]$ 的任意有限多元情况, 即成立

$$\Psi(X_0, X_1, \cdots, X_n)^{\pi} \equiv \Psi\left({X_0}^{\pi}, {X_1}^{\pi}, \cdots, {X_n}^{\pi}\right) \mod \boldsymbol{\pi}\mathfrak{S},\ \forall X_0,\ \cdots,\ X_n \in \mathfrak{S}.$$

$\forall X \in \prod_{n\geq 0} \mathfrak{S}$, $\forall n \in \mathbb{Z}_{\geq 0}$, 由 *Witt* 多项式的构造方式, 第 $n+1$ 级 *Witt* 多项式 $W_n(X)$ 只涉及 X 的前 $n+1$ 个分量, 显然有 $W_n(X) \in \mathbb{Z}[X_0, X_1, \cdots, X_n]$. 于是该推论显然成立.

至此, 启迪于 Serre [4, Chapter 2, § 6, Theorem 6.], 并参考 Witt [5, Satz 1.] 的证明思路, 我们来正式说明式 (3.2.1) 所定义的运算的封闭性.

定理 3.2.2.8 设 κ 是一个含幺交换环, $\pi \neq \operatorname{char}(\kappa)$ 是一个素数, $\boldsymbol{\pi} := \sum_{i=1}^{\pi} \mathbf{1} \in \kappa$. $\forall \Phi \in \mathbb{Z}[X,Y]$, $\forall X := (X_n)_{n\geq 0}$, $Y := (Y_n)_{n\geq 0} \in \prod_{n\geq 0} \kappa$, 存在一个序列 $\varphi = (\varphi_0, \varphi_1, \cdots, \varphi_n, \cdots)$ 满足

$$\varphi_i \in \mathbb{Z}\left[X_0, \cdots, X_n, \cdots; Y_0, \cdots, Y_n, \cdots\right],\ \forall i \in \mathbb{Z}_{\geq 0},$$

成立

$$W_n\left(\varphi_0, \cdots, \varphi_n, \cdots\right) = \Phi\left(W_n\left(X_0, \cdots\right), W_n\left(Y_0, \cdots\right)\right),\ n = 0,\ 1,\ \cdots.$$

证明 记 $\mathfrak{S} := \mathbb{Z}\left[X_0, \cdots, X_n, \cdots Y_0, \cdots, Y_n, \cdots\right]$. 显然 $\mathfrak{S}$ 是一个含幺交换环. 由于 $\mathbb{Z} \subset \mathfrak{S}$, 有 $\operatorname{char}(\mathfrak{S}) = \operatorname{char}(\mathbb{Z}) = 0 \neq \pi$. 且显然对每个 X_n, Y_n 成立 X_n, $Y_n \in \mathfrak{S}$, 也就有 $W_n(X)$, $W_n(Y) \in \mathfrak{S}$.

1. 第一步, 由命题*3.1.3*给出的

$$\begin{aligned} W_n(X) &= W_{n-1}\left(X^{\pi}\right) + \boldsymbol{\pi}^n X_n, \\ W_n(Y) &= W_{n-1}\left(Y^{\pi}\right) + \boldsymbol{\pi}^n Y_n, \end{aligned}$$

成立

$$W_n(X) \equiv W_{n-1}(X^\pi) \mod \boldsymbol{\pi}^n\Im,$$
$$W_n(Y) \equiv W_{n-1}(Y^\pi) \mod \boldsymbol{\pi}^n\Im.$$

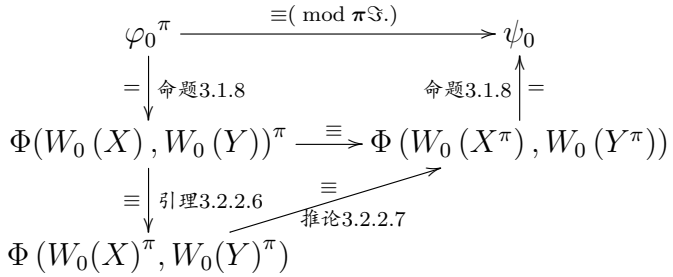
于是由性质*3.2.1.10*, 成立

$$W_n(\varphi) = \Phi(W_n(X), W_n(Y)) \equiv \Phi(W_{n-1}(X^\pi), W_{n-1}(Y^\pi)) =: W_{n-1}(\psi) \mod \boldsymbol{\pi}^n\Im,$$
$$\exists \psi \in \prod_{n\geq 0} \mathbb{Z}[X_0, \cdots, X_n, \cdots; Y_0, \cdots, Y_n, \cdots]. \tag{3.2.2.9}$$

2. 第二步, 对 φ 的第一个分量 φ_0, 显然成立

$$\varphi_0 = \Phi(W_0(X), W_0(Y)) = \Phi(X_0, Y_0) \in \Im.$$

3. 第三步, 我们指出成立 ${\varphi_0}^\pi \equiv \psi_0 \mod \boldsymbol{\pi}\Im$. 事实上, 该同余式由下面的交换图给出.



4. 第四步, 在第三步的基础上, 假设对 φ, ψ 的前 $n-1\,(n \geq 1)$ 个分量满足

$${\varphi_v}^\pi \equiv \psi_v \mod \boldsymbol{\pi}\Im,\ \forall v = 0,\ 1,\ \cdots,\ n-1.$$

则由引理*3.2.2.5*可得

$$W_{n-1}(\varphi)^\pi \equiv W_{n-1}(\psi) \mod \boldsymbol{\pi}^{1+(n-1)}\Im = \boldsymbol{\pi}^n\Im. \tag{3.2.2.10}$$

由式 *(3.2.2.9)* 和式 *(3.2.2.10)*, 成立

$$W_n(\varphi) \equiv W_{n-1}(\varphi)^\pi \mod \boldsymbol{\pi}^n\Im.$$

再由命题*3.1.3*给出的迭代式, 得到

$$\boldsymbol{\pi}^n\varphi_n = W_n(\varphi) - W_{n-1}(\varphi)^\pi \equiv 0 \mod \boldsymbol{\pi}^n\Im,$$

即有 $\varphi_n \in \Im,\ \forall n \geq 1$.

至此, 明所欲证. □

推论 3.2.2.9 式 *(3.2.1)* 中的 $(S_n)_{n\geq 0},\ (P_n)_{n\geq 0} \in \prod_{n\geq 0} \mathbb{Z}[X_0, \cdots, X_n, \cdots; Y_0, \cdots, Y_n, \cdots]$. 进而由环 κ 的线性运算封闭性, 也就有 $(S_n)_{n\geq 0},\ (P_n)_{n\geq 0} \in \prod_{n\geq 0} \kappa$.

3.2.3 其他环条件的验证

基于 § 3.2.2 节提供的运算封闭性的保证, 我们就可以放心地对其他环条件进行验证. § 3.2 节开篇中的命题3.2.2提到了式 (3.2.1) 是良定义的充分条件是 Witt 多项式系数 $\boldsymbol{\pi}$ 在含幺交换环 κ 中非零因子. 而当这个条件成立时, § 3.1 节中的命题3.1.11可以拿来使用. 事实上, 该命题将在验证其他环条件中发挥重要作用. 以下限制 Witt 多项式系数 $\boldsymbol{\pi}$ 在含幺交换环 κ 中非零因子, 并任取 $X := (X_n)_{n\geq 0}$, $Y := (Y_n)_{n\geq 0}$, $Z := (Z_n)_{n\geq 0} \in \prod_{n\geq 0} \kappa$.

首先我们指出式 (3.2.1) 满足结合律.

命题 3.2.3.1 成立以下恒等式

1. $(X \oplus Y) \oplus Z = X \oplus (Y \oplus Z)$;
2. $(X \odot Y) \odot Z = X \odot (Y \odot Z)$.

证明 由下面的交换图

$$
\begin{array}{ccc}
A := (X \oplus Y) \oplus Z & \xrightarrow{=} & X \oplus (Y \oplus Z) =: B \\
{\scriptstyle W_n(A)=}\downarrow & & \downarrow{\scriptstyle W_n(B)=} \\
W_n(X \oplus Y) + W_n(Z) & \xrightarrow{=} & W_n(X) + W_n(Y \oplus Z) \\
{\scriptstyle S(X,Y):=X\oplus Y}\downarrow & & \downarrow{\scriptstyle S(Y,Z):=Y\oplus Z} \\
W_n(S(X,Y)) + W_n(Z) & \xrightarrow{=} & W_n(X) + W_n(S(Y,Z)) \\
{\scriptstyle =}\downarrow & & \downarrow{\scriptstyle =} \\
(W_n(X) + W_n(Y)) + W_n(Z) & \underset{\kappa\text{交换}}{\overset{=}{\longleftrightarrow}} & W_n(X) + (W_n(Y) + W_n(Z))
\end{array}
$$

$$
\begin{array}{ccc}
C := (X \odot Y) \odot Z & \xrightarrow{=} & X \odot (Y \odot Z) =: D \\
{\scriptstyle W_n(C)=}\downarrow & & \downarrow{\scriptstyle W_n(D)=} \\
W_n(X \odot Y) \cdot W_n(Z) & \xrightarrow{=} & W_n(X) \cdot W_n(Y \odot Z) \\
{\scriptstyle P(X,Y):=X\odot Y}\downarrow & & \downarrow{\scriptstyle P(Y,Z):=Y\odot Z} \\
W_n(P(X,Y)) \cdot W_n(Z) & \xrightarrow{=} & W_n(X) \cdot W_n(P(Y,Z)) \\
{\scriptstyle =}\downarrow & & \downarrow{\scriptstyle =} \\
(W_n(X) \cdot W_n(Y)) \cdot W_n(Z) & \underset{\kappa\text{交换}}{\overset{=}{\longleftrightarrow}} & W_n(X) \cdot (W_n(Y) \cdot W_n(Z))
\end{array}
$$

可得到

$$W_n(A) = W_n(B),\ W_n(C) = W_n(D).$$

由于 $\boldsymbol{\pi}$ 在含幺交换环 κ 中非零因子, 根据命题*3.1.11*, 即可得到 $A = B,\ C = D$. □

然后我们指出式 (3.2.1) 满足交换律.

命题 3.2.3.2 成立以下恒等式

1. $X \oplus Y = Y \oplus X$;

2. $X \odot Y = Y \odot X$.

证明 由下面的交换图

$$\begin{array}{ccc}
S(X,Y) := X \oplus Y & \xrightarrow{=} & Y \oplus X =: S(Y,X) \\
\downarrow & & \downarrow \\
W_n(S(X,Y)) & \xrightarrow{=} & W_n(S(Y,X)) \\
= \downarrow & & \downarrow = \\
W_n(X) + W_n(Y) & \xleftrightarrow{=} & W_n(Y) + W_n(X)
\end{array}$$

$$\begin{array}{ccc}
P(X,Y) := X \odot Y & \xrightarrow{=} & Y \odot X =: P(Y,X) \\
\downarrow & & \downarrow \\
W_n(P(X,Y)) & \xrightarrow{=} & W_n(P(Y,X)) \\
= \downarrow & & \downarrow = \\
W_n(X) \cdot W_n(Y) & \xleftrightarrow{=} & W_n(Y) \cdot W_n(X)
\end{array}$$

可得到

$$W_n(S(X,Y)) = W_n(S(Y,X)),\ W_n(P(X,Y)) = W_n(P(Y,X)).$$

由于 $\boldsymbol{\pi}$ 在含幺交换环 κ 中非零因子, 根据命题*3.1.11*, 即可得证. □

其次, 我们指出式 (3.2.1) 定义的运算下, 有

- $\oplus$ 运算的单位元为 $\mathbf{0} = (0,0,0,\cdots)$;
- $\odot$ 运算的单位元为 $\mathbf{1} = (1,0,0,\cdots)$.

命题 3.2.3.3 成立

1. $(X_0,X_1,X_2,\cdots) \oplus (0,0,0,\cdots) = (X_0,X_1,X_2,\cdots)$;

2. $(Y_0,Y_1,Y_2,\cdots) \odot (1,0,0,\cdots) = (Y_0,Y_1,Y_2,\cdots)$.

证明

1. 显然成立

$$W_n(\mathbf{0}) = \sum_{v=0}^{n} \pi^v 0^{\pi^{n-v}} = 0,\ \forall n \in \mathbb{Z}_{\geq 0}.$$

记 $\varphi := (\varphi_n) = X \oplus \mathbf{0}$, 则有

$$W_n(\varphi) = W_n(X) + W_n(\mathbf{0}) = W_n(X),\ \forall n \in \mathbb{Z}_{\geq 0}.$$

由于 $\boldsymbol{\pi}$ 在含幺交换环 κ 中非零因子, 根据命题*3.1.11*, 即有 $\varphi = X$.

2. 显然成立

$$W_0(\mathbf{1}) = 1;\ W_n(\mathbf{1}) = 1 + \sum_{v=1}^{n} \pi^v 0^{\pi^{n-v}} = 1,\ \forall n \geq 1.$$

记 $\psi := (\psi_n) = Y \odot \mathbf{1}$, 则有

$$W_n(\psi) = W_n(Y) \cdot W_n(\mathbf{1}) = W_n(Y),\ \forall n \in \mathbb{Z}_{\geq 0}.$$

由于 $\boldsymbol{\pi}$ 在含幺交换环 κ 中非零因子, 根据命题*3.1.11*, 即有 $\psi = Y$. □

接着, 在 $\oplus$ 单位元已知的情况下, 我们指出在 Witt 多项式系数 $\pi \neq \mathrm{char}(\kappa)$ 的基础上再限制 $\pi \neq 2$, 可以轻松找到任意 $X = (X_n)$ 的关于 $\oplus$ 的逆元素.

命题 3.2.3.4（在 *Witt* 多项式系数 $\pi \neq \mathrm{char}(\kappa)$, 2 的情况下）$\forall X = (X_n)$, 存在 $-X = (-X_n)$, 成立

$$X \oplus (-X) = \mathbf{0}.$$

证明 由于素数 $\pi \neq 2$, 因此 π 是一个奇数, 也就有 $\forall m \in \mathbb{Z}_{\geq 0}$, π^m 是一个奇数. 记 $\varphi := X \oplus (-X)$, 则有

$$\begin{aligned}
&W_n(\varphi) = W_n(X) + W_n(-X)\\
=&\sum_{v=0}^{n} \pi^v {X_v}^{\pi^{n-v}} + \sum_{v=0}^{n} \pi^v (-X_v)^{\pi^{n-v}}\\
=&\sum_{v=0}^{n} \pi^v {X_v}^{\pi^{n-v}} - \sum_{v=0}^{n} \pi^v {X_v}^{\pi^{n-v}}\\
=&\ 0 = W_n(\mathbf{0}),\ \forall n \geq 0.
\end{aligned}$$

由于 $\boldsymbol{\pi}$ 在含幺交换环 κ 中非零因子, 根据命题*3.1.11*, 即有 $\varphi = \mathbf{0}$. □

最后我们指出式 (3.2.1) 满足两个分配律.

命题 3.2.3.5 $X \odot (Y \oplus Z) = (X \odot Y) \oplus (X \odot Z)$ 且 $(X \oplus Y) \odot Z = (X \odot Z) \oplus (Y \odot Z)$.

证明 由下面的交换图

$$\begin{array}{ccc}
A := X \odot (Y \oplus Z) & \xrightarrow{\quad = \quad} & (X \odot Y) \oplus (X \odot Z) =: B\\
{\scriptstyle W_n(A)=}\downarrow & & \downarrow{\scriptstyle W_n(B)=}\\
W_n(X) \cdot W_n(Y \oplus Z) & \xrightarrow{\quad = \quad} & W_n(X \odot Y) + W_n(X \odot Z)\\
{\scriptstyle S(Y,Z):=Y\oplus Z}\downarrow{\scriptstyle =} & & {\scriptstyle =}\downarrow{\scriptstyle P(X,Y):=X\odot Y,\ P(X,Z):=X\odot Z}\\
W_n(X) \cdot W_n(S(Y,Z)) & \xrightarrow{\quad = \quad} & W_n(P(X,Y)) + W_n(P(X,Z))\\
{\scriptstyle =}\downarrow & & \downarrow{\scriptstyle =}\\
W_n(X) \cdot (W_n(Y) + W_n(Z)) & \underset{\kappa\text{分配律}}{\overset{=}{\longleftrightarrow}} & W_n(X) \cdot W_n(Y) + W_n(X) \cdot W_n(Z)
\end{array}$$

$$
\begin{array}{ccc}
C:=(X\oplus Y)\odot Z & \xrightarrow{\quad=\quad} & (X\odot Z)\oplus(Y\odot Z)=:D \\
{\scriptstyle W_n(C)=}\downarrow & & \downarrow{\scriptstyle W_n(D)=} \\
W_n(X\oplus Y)\cdot W_n(Z) & \xrightarrow{\quad=\quad} & W_n(X\odot Z)+W_n(Y\odot Z) \\
{\scriptstyle S(X,Y):=X\oplus Y}\downarrow{\scriptstyle =} & & {\scriptstyle =}\downarrow{\scriptstyle P(X,Z):=X\odot Z,\ P(Y,Z):=Y\odot Z} \\
W_n(S(X,Y))\cdot W_n(Z) & \xrightarrow{\quad=\quad} & W_n(P(X,Z))+W_n(P(Y,Z)) \\
{\scriptstyle =}\downarrow & & \downarrow{\scriptstyle =} \\
(W_n(X)+W_n(Y))\cdot W_n(Z) & \underset{\kappa\text{分配律}}{\overset{=}{\longleftrightarrow}} & W_n(X)\cdot W_n(Z)+W_n(Y)\cdot W_n(Z)
\end{array}
$$

可得到

$$W_n(A)=W_n(B),\ W_n(C)=W_n(D).$$

由于 $\boldsymbol{\pi}$ 在含幺交换环 κ 中非零因子, 根据命题*3.1.11*, 即可得到 $A=B,\ C=D.$ □

至此, 综合 § 3.2.2 和 § 3.2.3 节的结论, 我们最终验证得到了 $\prod_{n\geq 0}\kappa$ 上的一个崭新的环结构——Witt **环结构**.

命题 3.2.3.6 设 κ 是一个含幺交换环, $\boldsymbol{\pi}$ 在 κ 中非零因子, 则 $\prod_{n\geq 0}\kappa$ 在运算

$$
\begin{aligned}
(X_n)_{n\geq 0}\oplus(Y_n)_{n\geq 0}&:=(S_n)_{n\geq 0},\ \text{s.t. } W_n(S_0,\cdots,S_n,\cdots)=W_n(X)+W_n(Y),\\
(X_n)_{n\geq 0}\odot(Y_n)_{n\geq 0}&:=(P_n)_{n\geq 0},\ \text{s.t. } W_n(P_0,\cdots,P_n,\cdots)=W_n(X)\cdot W_n(Y),
\end{aligned}
$$

下构成一个含幺交换环, 称为 *Witt* **环** , 记为 $\mathcal{W}(\kappa)$.

证明

1. 运算 $\oplus$, $\odot$ 的良定义性由命题 *3.2.2*提供支撑.
2. $\left(\prod_{n\geq 0}\kappa,\oplus\right)$ 是一个阿贝尔群, 由推论*3.2.2.9*, 命题*3.2.3.1*, 命题*3.2.3.2*, 命题*3.2.3.3*, 命题*3.2.3.4*提供支撑.
3. $\left(\prod_{n\geq 0}\kappa,\odot\right)$ 是一个阿贝尔幺半群, 由推论*3.2.2.9*, 命题*3.2.3.1*, 命题*3.2.3.2*, 命题*3.2.3.3*提供支撑.
4. 分配律直接由命题*3.2.3.5*提供支撑. □

3.3 原像集为 Witt 向量环的环态射

根据本节开头提到的 $\prod_{n\geq 0}\Re/\boldsymbol{p}\Re$ 到 $\Re$ 的双射 Γ_0 映像的构造方式, 显然 Γ_0 的态性也直接受到提升 τ 的选取. 鉴于 Γ_0 映像呈现线性组合的面貌, 我们自然地会考虑如果选取的 τ 足够经典, 具有一些良好的性质, 如 $\tau(x)\tau(y)=\tau(xy)$ 或者 $\tau(x)+\tau(y)=\tau(x+y)$ 等, 那么 Γ_0 应该比较倾向于形成一个环态射. 本节的核心工作首先就是构建一个经典的 Teichmüller 提升 τ_e, 这将是 § 3.3.1 节的工作. 然后配合之前研究的 $\prod_{n\geq 0}\Re/\boldsymbol{p}\Re$ 上的环结构, 来研究 $\prod_{n\geq 0}\Re/\boldsymbol{p}\Re$ 与 $\Re$ 环同构的问题, 这将是 § 3.3.2 节的工作. 下面先引入一个在后面两个小小节的讨论中将被经常用到的一个引理.

引理 3.3.1 设 A 是一个含幺交换环, p 是一个素数, $\boldsymbol{p}:=\sum_{i=1}^{p}\mathbf{1}\in A$. 给定 A 的一个双边理想降链 $A=\mathfrak{a}_0\supset\mathfrak{a}_1\supset\mathfrak{a}_2\supset\cdots$ 满足

$$\mathfrak{a}_n\mathfrak{a}_m\subseteq\mathfrak{a}_{n+m}\ \text{且}\ \boldsymbol{p}\in\mathfrak{a}_1.$$

$\forall a,\ b\in A$, 若 $\exists m\in\mathbb{Z}_{\geq 1}$, 满足 $a\equiv b\mod\mathfrak{a}_m$, 则成立

$$a^{p^n}\equiv b^{p^n}\mod\mathfrak{a}_{m+n},\ \forall n\in\mathbb{Z}_{\geq 0}.$$

注记 由于 A 是一个含幺交换环, 实际使用中常取 $\mathfrak{a}_n=\boldsymbol{p}^nA$.

证明

1. 当 $n=0$ 时, 显然有
$$a^{p^0}=a\equiv b=b^{p^0}\mod\mathfrak{a}_m=\mathfrak{a}_{m+0}.$$

2. 当 $n=1$ 时, 置
$$P(X,Y):=X^{p-1}+X^{p-2}Y+\cdots+XY^{p-2}+Y^{p-1}\in\mathbb{Z}[X,Y]. \tag{3.3.1}$$
且一个已知条件为
$$a\equiv b\mod\mathfrak{a}_m. \tag{3.3.2}$$
由式 *(3.3.2)*, 成立 $a-b\equiv 0\mod\mathfrak{a}_m$，即有
$$a-b\in\mathfrak{a}_m. \tag{3.3.3}$$
由式 *(3.3.1)* 和式 *(3.3.2)*, 成立
$$P(a,b)\equiv P(a,a)=a^{p-1}+a^{p-1}+\cdots+a^{p-1}=\boldsymbol{p}a^{p-1}\mod\mathfrak{a}_m.$$
即有
$$P(a,b)\in\boldsymbol{p}a^{p-1}+\mathfrak{a}_m. \tag{3.3.4}$$
由于 $\boldsymbol{p}$ 是理想 $\mathfrak{a}_1$ 中的一个元素, $a^{p-1}\in A$, 由 $\mathfrak{a}_1$ 的乘法吸收性: $\mathfrak{a}_1A\subseteq\mathfrak{a}_1$ 得到
$$\boldsymbol{p}a^{p-1}\in\mathfrak{a}_1.$$

又由于 $m \geq 1$，$\mathfrak{a}_m \subseteq \mathfrak{a}_1$, 于是有

$$\boldsymbol{p}a^{p-1} + \mathfrak{a}_m \subseteq \mathfrak{a}_1. \tag{3.3.5}$$

由式 *(3.3.3)*, 式 *(3.3.4)* 和式 *(3.3.5)*, 成立

$$a^p - b^p = (a-b)\,P(a,b) \in \mathfrak{a}_m\mathfrak{a}_1 \subseteq \mathfrak{a}_{m+1},$$

即有

$$a^p - b^p \equiv 0 \mod \mathfrak{a}_{m+1}. \implies a^p \equiv b^p \mod \mathfrak{a}_{m+1}.$$

3. 对于 $n \geq 2$ 的情况, 可将 a^{p^n}, b^{p^n} 视为

$$a^{p^n} = ((a^p)^p \cdots)^p,\ b^{p^n} = ((b^p)^p \cdots)^p,$$

从而化归到 $n = 1$ 的情况. 结论显然也是成立的. □

3.3.1 Teichmüller 提升简述

参照李文威 [12, 命题 10.9.4], 我们来构造一个特殊的提升 τ. 首先我们简略地提及一下构造过程中涉及的一个点集拓扑学概念.

定义 3.3.1.1 设 X 是一个非空集, $\mathfrak{B} \subset 2^X$ 是 X 的一个非空子集族, 称 $\mathfrak{B}$ 是 X 上的**滤子基**, 若满足

1. $\forall A,\ B \in \mathfrak{B}$, 存在 $C \in \mathfrak{B}$ 使得 $C \subseteq (A \cap B)$;

2. $\varnothing \notin \mathfrak{B}$.

特别地, 在 $(X,+)$ 是一个 *Hausdorff* 交换拓扑群的情况下, 称滤子基 $\mathfrak{B}$ 是一个**柯西滤子基**, 若对 $(X,+)$ 中单位点 0 的任何领域 $U(0;\delta)$, 存在 $E \in \mathfrak{B}$ 使得

$$E - E := \{x - y : x, y \in E\} \subseteq U.$$

现正式引入一个特殊提升 τ 的构造方法如下.

定义 3.3.1.2 设 A 是一个 p-环, $\kappa := A/\mathfrak{a}_1$. 由于 κ 是完全的, 根据推论*2.2.11*, $\forall x \in \kappa$, $\forall n \in \mathbb{Z}_{\geq 0}$, 存在唯一的 p^n-次根 $x^{p^{-n}} \in \kappa$. 记 $x^{p^{-n}}$ 在 A 中的原像集 L_n 以及相应的 U_n 为

$$\begin{aligned}
L_n(x) :&= \left\{ \left[x^{p^{-n}}\right] :\ \phi\left(\left[x^{p^{-n}}\right]\right) = x^{p^{-n}} \right\} \subseteq A,\\
U_n(x) :&= \left\{\lambda^{p^n} :\ \lambda \in L_n\right\} = \left\{ \left[x^{p^{-n}}\right]^{p^n} :\ \phi\left(\left[x^{p^{-n}}\right]\right) = x^{p^{-n}} \right\} \subseteq A,\\
&n = 0,\ 1,\ 2,\ \cdots,
\end{aligned}$$

其中 ϕ 是 A 到 κ 的, 代表模去理想 $\mathfrak{a}_1$ 的满射. 称

$$\tau_e(x) := \lim_{n\to\infty} U_n(x) = \lim_{n\to\infty} \left[x^{p^{-n}}\right]_\forall^{p^n},\ \forall \left[x^{p^{-n}}\right]_\forall \in L_n(x) \tag{3.3.1.1}$$

为 *Teichmüller* [14] **映射** .

在这里先补充说明一点, 由于 ϕ 代表模去理想 $\mathfrak{a}_1$ 的操作, 而剩余类环 κ 上的加法 $\oplus$ 和乘法 $\otimes$ 为

$$\begin{aligned}(a+I)\oplus(b+I) &:= (a+b)+I,\\ (a+I)\otimes(b+I) &:= ab+I,\ \forall a,\ b\in A.\end{aligned}$$

于是映射 ϕ 既是一个保持加性的映射又是一个保持乘性的映射, 即有

$$\begin{aligned}\phi(a+b) &= \phi(a)\oplus\phi(b),\\ \phi(ab) &= \phi(a)\otimes\phi(b).\end{aligned}$$

后面的推导过程中将不可避免地使用到这些性质, 故在此作一个提及. 言归正传, 出于严谨考虑, 我们先验证定义3.3.1.2是一个良定义.

命题 3.3.1.3 式 *(3.3.1.1)* 中的极限是存在的. *Teichmüller* 映射 τ_e 确实是一个提升, 称为 *Teichmüller* **提升**.

证明 我们只需要证明 $\{U_n(x)\}_{n\geq 0}$ 是一个柯西滤子基即可.

1. 显然 $\forall n\geq 0, \forall x^{p^{-n}}\in\kappa$, 由于模去理想映射 ϕ 是一个满射, 因此总是存在 $\left[x^{p^{-n}}\right]_{\exists}\in A$ 满足
$$\phi\left(\left[x^{p^{-n}}\right]_{\exists}\right) = x^{p^{-n}}\in\kappa.$$
因此 $L_n\neq\varnothing$, 也就有 $U_n\neq\varnothing$, 也就有 $\varnothing\notin\{U_n\}_{n\geq 0}$.

2. $\forall m,\ t\in\mathbb{Z}_{\geq 0}$, 任取 $L_{m+t}(x)$ 中的一个元素 $\left[x^{p^{-(m+t)}}\right]_{\forall}$, 成立
$$\phi\left(\left[x^{p^{-(m+t)}}\right]_{\forall}^{p^t}\right) = \phi\left(\left[x^{p^{-(m+t)}}\right]_{\forall}\right)^{p^t} = \left(x^{p^{-(m+t)}}\right)^{p^t} = x^{p^{-m}},$$
因此有
$$\begin{aligned}&\left[x^{p^{-(m+t)}}\right]_{\forall}^{p^t}\in\left\{\left[x^{p^{-m}}\right]\right\} = L_m(x).\\ \Longrightarrow&\left(\left[x^{p^{-(m+t)}}\right]_{\forall}^{p^t}\right)^{p^m} = \left[x^{p^{-(m+t)}}\right]_{\forall}^{p^{m+t}}\in U_m(x).\\ \Longrightarrow& U_{m+t}(x)\subseteq U_m(x),\ \forall m,\ t\in\mathbb{Z}_{\geq 0}.\end{aligned}$$
因此我们得到了一个关于包含关系的降链
$$U_0\supseteq U_1\supseteq U_2\supseteq\cdots. \tag{3.3.1.2}$$
因此 $\forall U_r,\ U_s\in\{U_n\}_{n\geq 0}, \forall m\geq\max\{r,\ s\}$, 成立
$$U_m\subseteq U_{\max\{r,s\}} = U_r\cap U_s.$$

[14] Oswald Teichmüller, 1913.6–1943.9, 德国数学家, 哲学家.

3. 任取 $\left[x^{p^{-m}}\right]_1,\ \left[x^{p^{-m}}\right]_2 \in L_m(x)$, 由于二者均为 $x^{p^{-m}}$ 在模去理想 $\mathfrak{a}_1$ 的映射 ϕ 下的原像, 因此显然有

$$\left[x^{p^{-m}}\right]_1 \equiv \left[x^{p^{-m}}\right]_2 \mod \mathfrak{a}_1.$$

进而根据引理*3.3.1*, 可得

$$\begin{aligned} &\left[x^{p^{-m}}\right]_1^{p^m} \equiv \left[x^{p^{-m}}\right]_2^{p^m} \mod \mathfrak{a}_{m+1}. \\ \Longrightarrow\ &\left[x^{p^{-m}}\right]_1^{p^m} - \left[x^{p^{-m}}\right]_2^{p^m} \equiv 0 \mod \mathfrak{a}_{m+1}. \\ \Longrightarrow\ &\left[x^{p^{-m}}\right]_1^{p^m} - \left[x^{p^{-m}}\right]_2^{p^m} \in \mathfrak{a}_{m+1}. \end{aligned}$$

又由于理想降链关系 $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots$, 进而成立

$$\begin{aligned} &\left[x^{p^{-m}}\right]_1^{p^m} - \left[x^{p^{-m}}\right]_2^{p^m} \in \mathfrak{a}_n \subseteq \mathfrak{a}_{m+1}. \\ \Longrightarrow\ &\left[x^{p^{-m}}\right]_1^{p^m} - \left[x^{p^{-m}}\right]_2^{p^m} \equiv 0 \mod \mathfrak{a}_n,\ \forall 0 \leq n \leq m+1. \end{aligned}$$

进而有以下的对应关系

$$\begin{aligned} U_m(x) - U_m(x) \subseteq A \quad &\xrightarrow{\sim} \quad \varprojlim_n A/\mathfrak{a}_n \\ \left[x^{p^{-m}}\right]^{p^m} \quad &\to \quad \left(\underbrace{0, 0, \cdots, 0}_{m+1\text{个}}, ?, ?, \cdots\right). \end{aligned}$$

因此任取 $(A, +)$ 单位点 0 的一个邻域 U, 当 m 足够大时, 总有

$$U_m - U_m \subseteq U.$$

综上三点, $\{U_n(x)\}_{n\geq 0}$ 是环 A 一个柯西滤子基. 又由于 p-环 A 是完备的 *Hausdorff* 环, 因此式 *(3.3.1.1)* 中的极限是存在的, 即 $\exists! y \in A$, 满足

$$\lim_{n\to\infty} U_n(x) = y.$$

结合式 *(3.3.1.2)* 提供的降链关系, 也就有

$$y = \bigcap_{n=0}^{\infty} U_n(x). \tag{3.3.1.3}$$

由于 $\forall n \geq 0$, 任取 $\left[x^{p^{-n}}\right]_\forall^{p^n} \in U_n$ 成立

$$\phi\left(\left[x^{p^{-n}}\right]_\forall^{p^n}\right) = \phi\left(\left[x^{p^{-n}}\right]_\forall\right)^{p^n} = \left(x^{p^{-n}}\right)^{p^n} = x. \implies \left[x^{p^{-n}}\right]_\forall^{p^n} \equiv x \mod \mathfrak{a}_1.$$

因此结合式 *(3.3.1.3)* 也就有

$$\tau_e(x) = y \equiv x \mod \mathfrak{a}_1.$$

从而 $\tau_e\colon \kappa \to A$ 确实是一个提升. □

对定义3.3.1.2验证完毕后, 我们指出 Teichmüller 提升 τ_e 具有若干良好的性质, 从而具备研究其的动机充分性. 且某些方面上 Teichmüller 提升 τ_e 具有的性质是其他提升不具备的, 因此也存在研究其的动机必要性. 下面我们先介绍关于式 (3.3.1.1) 中极限的一个运算法则, 然后对 Teichmüller 提升 τ_e 的若干性质进行说明.

定理 3.3.1.4 极限 $\lim_{n\to\infty} U_n(x_1)\,U_n(x_2)$, $\lim_{n\to\infty}(U_n(x_1)+U_n(x_2))$ 均存在, 且成立

$$\lim_{n\to\infty} U_n(x_1)\,U_n(x_2) = \lim_{n\to\infty} U_n(x_1) \cdot \lim_{n\to\infty} U_n(x_2),$$
$$\lim_{n\to\infty} (U_n(x_1)+U_n(x_2)) = \lim_{n\to\infty} U_n(x_1) + \lim_{n\to\infty} U_n(x_2).$$

证明 记 $y_{1,2} := \lim_{n\to\infty} U_n(x_{1,2})$. 我们只证明第一条公式, 第二条类似可证.

1. 一方面, 基于命题*3.3.1.3*中的式 *(3.3.1.2)*, 我们有

$$y_{1,2} = \bigcap_{n=1}^{\infty} U_n(x_{1,2}). \implies y_1y_2 \in \bigcap_{n=1}^{\infty} U_n(x_1)\,U_n(x_2). \tag{3.3.1.4}$$

2. 另一方面, $\{U_n(x_1)\,U_n(x_2)\}$ 也是一个柯西滤子基.

(a) 由于 $\forall n \geq 0$, $U_n(x_1)$, $U_n(x_2) \neq \varnothing$, 自然也就有 $U_n(x_1)\,U_n(x_2) \neq \varnothing$, $\varnothing \notin \{U_n(x_1)\,U_n(x_2)\}$.

(b) 由降链关系

$$U_0(x_1) \supseteq U_1(x_1) \supseteq \cdots;\quad U_0(x_2) \supseteq U_1(x_2) \supseteq \cdots,$$

可以推出新的降链关系

$$U_0(x_1)\,U_0(x_2) \supseteq U_1(x_1)\,U_1(x_2) \supseteq \cdots. \tag{3.3.1.5}$$

(c) 任取 $\left[x_1^{p^{-m}}\right]_1, \left[x_1^{p^{-m}}\right]_2 \in L_m(x_1)$, $\left[x_2^{p^{-m}}\right]_3, \left[x_2^{p^{-m}}\right]_4 \in L_m(x_2)$, 根据 *§ 3.2.1* 节介绍的模理想同余的性质, 成立

$$\left.\begin{aligned}\left[x_1^{p^{-m}}\right]_1 &\equiv \left[x_1^{p^{-m}}\right]_2 \mod \mathfrak{a}_1.\\ \left[x_2^{p^{-m}}\right]_3 &\equiv \left[x_2^{p^{-m}}\right]_4 \mod \mathfrak{a}_1.\end{aligned}\right\} \implies \left[x_1^{p^{-m}}\right]_1\left[x_2^{p^{-m}}\right]_3 \equiv \left[x_1^{p^{-m}}\right]_2\left[x_2^{p^{-m}}\right]_4 \mod \mathfrak{a}_1.$$

仿命题*3.3.1.3*的证明过程, 即得 $\{U_n(x_1)\,U_n(x_2)\}$ 是一个柯西滤子基. 由于 A 是完备的 *Hausdorff* 环, 结合式 *(3.3.1.5)* 提供的降链形式, 即得

$$\#\left(\bigcap_{n=1}^{\infty} U_n(x_1)\,U_n(x_2)\right) = 1. \tag{3.3.1.6}$$

3. 由式 *(3.3.1.4)*, 式 *(3.3.1.6)*, 即可得

$$\lim_{n\to\infty} U_n(x_1)\,U_n(x_2) = \bigcap_{n=1}^{\infty} U_n(x_1)\,U_n(x_2) = y_1y_2 = \lim_{n\to\infty} U_n(x_1) \cdot \lim_{n\to\infty} U_n(x_2).$$

至此, 明所欲证. □

命题 3.3.1.5 *Teichmüller* 提升 τ_e 具有以下的特点,

1. $\tau_e(0)=\mathbf{0}\in A$, $\tau_e(1)=\mathbf{1}\in A$;
2. $\tau_e\left(x^{p^n}\right)=\tau_e(x)^{p^n}$, $\forall n\geq 0$, 且满足这种性质的提升只有 τ_e;
3. $\tau_e(xy)=\tau_e(x)\,\tau_e(y)$, 且满足这种性质的提升只有 τ_e;
4. 当 $char(A)=p$ 时成立 $\tau_e(x+y)=\tau_e(x)+\tau_e(y)$.

证明

1. 由于 p-环 A 的剩余类环 κ 是完全的, 而 $\forall n\geq 0$, $1^{p^n}=1$, 因此 1 是 1 的唯一一个 p^n-次根. 成立

$$\phi(\mathbf{1})=1=1^{p^{-n}}.$$

因此有

$$\mathbf{1}\in L_n(1).\implies \mathbf{1}=\mathbf{1}^{p^n}=U_n(1),\ \forall n\geq 0.\implies \mathbf{1}\in\bigcap_{n=1}^{\infty}U_n(1).$$

因此只能是

$$\tau_e(1)=\bigcap_{n=1}^{\infty}U_n(1)=\mathbf{1}.$$

$\tau_e(0)=\mathbf{0}$ 仿此可证, 此处不作赘述.

2. 我们先证明 $\tau_e(x^p)=\tau_e(x)^p$.
记 $y:=x^p$, 则有

$$\begin{aligned}\tau_e(x^p)=\tau_e(y)&=\lim_{n\to\infty}\left[y^{p^{-(n+1)}}\right]_{\forall}^{p^{n+1}}.\\&=\lim_{n\to\infty}\left(\left[x^{p^{-n}}\right]_{\forall}^{p^n}\right)^p=\prod_{i=1}^{p}\lim_{n\to\infty}\left[x^{p^{-n}}\right]_{\forall}^{p^n}=\prod_{i=1}^{p}\tau_e(x)=\tau_e(x)^p.\end{aligned}$$

基于此, 有

$$\tau_e\left(x^{p^n}\right)=\tau_e\left(\underbrace{((x^p)^p\cdots)^p}_{n\text{层指数嵌套}}\right)=\tau_e\left(\underbrace{((x^p)^p\cdots)}_{n-1\text{层指数嵌套}}\right)^p=\cdots=\tau_e(x)^{p^n}.$$

最后任取一个提升 τ' 满足 $\tau'\left(x^{p^n}\right)=\tau'(x)^{p^n}$, 指定式 *(3.3.1.1)* 中的 $[\cdots]$ 为 $\tau'(\cdots)$, 则有

$$\tau_e(x)=\lim_{n\to\infty}\tau'\left(x^{p^{-n}}\right)^{p^n}=\lim_{n\to\infty}\tau'\left(\left(x^{p^{-n}}\right)^{p^n}\right)=\lim_{n\to\infty}\tau'(x)=\tau'(x).$$

唯一性得证.

3. 我们分步来进行说明.

(a) 第一步, 首先我们指出, $\forall x \in \kappa$, 取定 x 的一个原像 $[x]_0$ 后, x 关于 ϕ 的原像集 $L_0(x)$ 可以表示为

$$L_0(x) = [x]_0 + \mathfrak{a}_1. \tag{3.3.1.7}$$

一方面, $\forall t \in \mathfrak{a}_1$, 由于

$$\phi([x]_0 + t) = \phi([x]_0) + \phi(t) = x + 0 = x,$$

有 $[x]_0 + \mathfrak{a}_1 \subseteq L_0(x)$. 另一方面, $\forall y \in L_0(x)$, 有

$$\phi(y - [x]_0) = \phi(y) - \phi([x]_0) = x - x = 0. \implies y - [x]_0 \equiv 0 \mod \mathfrak{a}_1,$$

即存在 $t \in \mathfrak{a}_1$ 使得 $y - [x]_0 = t$ 即 $y = [x]_0 + t$, 有 $L_0(x) \subseteq [x]_0 + \mathfrak{a}_1$. 由此成立式 *(3.3.1.7)*.

(b) 第二步, 基于第一步的结论, $\forall x, y \in \kappa$, 任意取定 xy, x, y 的一个原像 $[xy]_0$, $[x]_0$, $[y]_0$, 有

$$\phi([xy]_0) = xy = \phi([x]_0)\phi([y]_0), \text{ 即} [xy]_0 + \mathfrak{a}_1 = ([x]_0 + \mathfrak{a}_1)([y]_0 + \mathfrak{a}_1).$$

因此对 xy 的任意一个原像 $[xy]_0 + t_0 =: [xy]_\forall$, 总是存在 x, y 的一个原像 $[x]_0 + t_1 =: [x]_1$, $[y]_0 + t_2 =: [y]_2$, 成立

$$[xy]_\forall = [xy]_0 + t_0 = ([x]_0 + t_1)([y]_0 + t_2) = [x]_1[y]_2. \tag{3.3.1.8}$$

(c) 第三步, 由于

$$xy = \left(x^{p^{-n}}\right)^{p^n}\left(y^{p^{-n}}\right)^{p^n} = \left(x^{p^{-n}}y^{p^{-n}}\right)^{p^n},$$

而 p-环 A 的剩余类环 κ 是完全的, 因此 $x^{p^{-n}}y^{p^{-n}}$ 是 xy 的唯一一个 p^n-次根, 即有

$$(xy)^{p^{-n}} = x^{p^{-n}}y^{p^{-n}}.$$

基于式 *(3.3.1.8)*, 第二步的结论, 命题*3.3.1.4*第 *(1)* 条, 我们有

$$\begin{aligned}\tau_e(xy) &= \lim_{n\to\infty}\left[(xy)^{p^{-n}}\right]_\forall^{p^n} = \lim_{n\to\infty}\left[x^{p^{-n}}y^{p^{-n}}\right]_\forall^{p^n} = \lim_{n\to\infty}\left(\left[x^{p^{-n}}\right]_1\left[y^{p^{-n}}\right]_2\right)^{p^n} \\ &= \lim_{n\to\infty}\left(\left[x^{p^{-n}}\right]_1^{p^n}\left[y^{p^{-n}}\right]_2^{p^n}\right) = \lim_{n\to\infty}\left[x^{p^{-n}}\right]_1^{p^n} \cdot \lim_{n\to\infty}\left[y^{p^{-n}}\right]_2^{p^n} = \tau_e(x)\tau_e(y).\end{aligned}$$

(d) 最后, 任取一个提升 τ' 满足 $\tau'(xy) = \tau'(x)\tau'(y)$, 指定式 *(3.3.1.1)* 中的 $[\cdots]$ 为 $\tau'(\cdots)$, 则有

$$\tau_e(x) = \lim_{n\to\infty}\prod_{i=1}^{p^n}\tau'\left(x^{p^{-n}}\right) = \lim_{n\to\infty}\tau'\left(\prod_{i=1}^{p^n}x^{p^{-n}}\right) = \lim_{n\to\infty}\tau'(x) = \tau'(x).$$

唯一性得证.

4. 我们还是分步来进行说明.

(a) 第一步, 由于 $\boldsymbol{p} \in \mathfrak{a}_1$, $\operatorname{char}(\kappa) = p$, 结合引理*3.2.2.1*可得

$$\begin{aligned}\left(x^{p^{-n}} + y^{p^{-n}}\right)^{p^n} &= \left(\left(x^{p^{-n}} + y^{p^{-n}}\right)^{p}\right)^{p^{n-1}}. \\ &= \left(x^{p^{-(n-1)}} + y^{p^{-(n-1)}} + \sum_{k=1}^{n-1} \binom{p}{k} \left(x^{p^{-n}}\right)^k \left(y^{p^{-n}}\right)^{p-k}\right)^{p^{n-1}}. \\ &= \left(x^{p^{-(n-1)}} + y^{p^{-(n-1)}}\right)^{p^{n-1}}. \\ &= \cdots = x + y.\end{aligned}$$

又由于 κ 是完全的, 因此 $x^{p^{-n}} + y^{p^{-n}}$ 是 $x + y$ 的唯一一个 p^n-次根, 即有

$$(x+y)^{p^{-n}} = x^{p^{-n}} + y^{p^{-n}}. \tag{3.3.1.9}$$

(b) 第二步, 若 $\operatorname{char}(A) = p$, 参照第一步的思想, 也能得到

$$\left(\left[x^{p^{-n}}\right]_\forall + \left[y^{p^{-n}}\right]_\forall\right)^{p^n} = \left[x^{p^{-n}}\right]_\forall^{p^n} + \left[y^{p^{-n}}\right]_\forall^{p^n}. \tag{3.3.1.10}$$

(c) 第三步, 参照 *(3)* 中的第一、二步, 也能得到 $\forall x,\ y \in \kappa$, 任取 $x + y$ 的一个原像 $[x+y]_0$, 总是存在 $x,\ y$ 的一个原像 $[x]_1,\ [y]_2$, 成立

$$[x+y]_0 = [x]_1 + [y]_2. \tag{3.3.1.11}$$

(d) 第四步, 基于式 *(3.3.1.9)*, 式 *(3.3.1.10)*, 式 *(3.3.1.11)* 和极限运算定理第 *(2)* 条, 成立

$$\begin{aligned}\tau_e(x+y) &= \lim_{n\to\infty} \left[(x+y)^{p^{-n}}\right]_\forall^{p^n} = \lim_{n\to\infty} \left[x^{p^{-n}} + y^{p^{-n}}\right]_\forall^{p^n}. \\ &= \lim_{n\to\infty} \left(\left[x^{p^{-n}}\right]_1 + \left[y^{p^{-n}}\right]_2\right)^{p^n} = \lim_{n\to\infty} \left(\left[x^{p^{-n}}\right]_1^{p^n} + \left[y^{p^{-n}}\right]_2^{p^n}\right). \\ &= \lim_{n\to\infty} \left[x^{p^{-n}}\right]_1^{p^n} + \lim_{n\to\infty} \left[y^{p^{-n}}\right]_2^{p^n} = \tau_e(x) + \tau_e(y).\end{aligned}$$

至此, 明所欲证. □

到这里, 我们就初步介绍完 Teichmüller 提升 τ_e 这一经典映射结构.

3.3.2 态射性验证

经过了 § 2.2 节, § 3.2 节和 § 3.3.1 节的讨论, 我们最终选取并整理了以下的一套条件:

$$\begin{gathered}\Re:\ \text{一个严格}p\text{-环};\\ \Re\text{的剩余类环}:\ \kappa:=\Re/\boldsymbol{p}\Re;\\ \prod_{n\geq 0}\kappa\text{上的环结构}:\ \text{Witt 环}\ \mathcal{W}(\kappa);\\ \Gamma_0\text{像中的提升}:\ \text{Teichmüller 提升}\tau_e.\end{gathered}\tag{3.3.2.1}$$

对于之前提及的双射 Γ_0 :

$$\begin{array}{ccc}\mathcal{W}(\kappa) & \xrightarrow{\Gamma_0} & \Re\\ x=(x_n)_{n\geq 0} & \to & \sum\limits_{n=0}^{\infty}\tau_e(x_n)\,\boldsymbol{p}^n\end{array}\tag{3.3.2.2}$$

根据我们自己的尝试和搜集的资料, 目前无论是验证其保持加性和乘性或者发现其不保持加性或乘性, 都没有比较理想的手段. 为此, 我们欲充分利用条件 (3.3.2.1), 从双射 Γ_0 上导出另一个便于研究的双射 Γ_c. 一方面, 我们还是将目光移到 § 2.2 节命题2.2.5中的式 (2.2.2a), 并且考虑更为一般的情况

$$\widetilde{x_n}\equiv\tau_e(x_n)\mod\boldsymbol{p}\Re,\ n=0,\ 1,\ \cdots,\ \widetilde{x_0}=\widetilde{x}.\tag{3.3.2.3}$$

另一方面, 反复运用费马小定理3.2.2.2, 不难有如下推论.

推论 3.3.2.1 (Fermat) 设 $\Im$ 是一个含幺交换环, $p\neq\operatorname{char}(\Im)$ 是一个素数, $\boldsymbol{p}:=\sum_{i=1}^{p}\mathbf{1}\in\Im$. $\forall a\in\Im$, 成立同余式

$$a^{p^n}\equiv a\mod\boldsymbol{p}.$$

由于含幺交换环 $\Re$ 是一个严格 p-环, $\operatorname{char}(\Re)\neq p$, 且 κ 是完全的, ${x_n}^{p^{-n}}$ 是存在的. 因此在 $\Re$ 中可应用推论3.3.2.1得到

$$\tau_e\left({x_n}^{p^{-n}}\right)^{p^n}\equiv\tau_e\left({x_n}^{p^{-n}}\right)\mod\boldsymbol{p}.\tag{3.3.2.4}$$

得益于 Teichmüller 提升 τ_e 的选取, 我们可以把式 (3.3.2.4) 中同余号左边的 $(\cdots)$ 外的指数 p^n 移入 $(\cdots)$ 内, 得到

$$\tau_e(x_n)\equiv\tau_e\left({x_n}^{p^{-n}}\right)\mod\boldsymbol{p}.\implies\tau_e(x_n)\equiv\tau_e\left({x_n}^{p^{-n}}\right)\mod\boldsymbol{p}\Re.\tag{3.3.2.5}$$

由式 (3.3.2.3) 和式 (3.3.2.5), 根据同余式的传递性, 即有

$$\widetilde{x_n}\equiv\tau_e\left({x_n}^{p^{-n}}\right)\mod\boldsymbol{p}\Re,\ n=0,\ 1,\ \cdots.\tag{3.3.2.6}$$

由此, 参考式 (2.2.2) 的推理过程, 仿算法2.2.4, 我们也可以得到以下一个可以正确执行的算法.

算法 3.3.2.2

- $\forall \widetilde{x} \in \Re$, 记 $x_0 = \phi\left(\widetilde{x}\right) \in \kappa$, 则 $\exists \widetilde{x_1} \in \Re$ 使得 $\widetilde{x} = \tau_e\left({x_0}^{p^{-0}}\right) + \boldsymbol{p}\widetilde{x_1}$.
- 记 $x_1 = \phi\left(\widetilde{x_1}\right)$, 则 $\exists \widetilde{x_2} \in \Re$, 使得 $\widetilde{x_1} = \tau_e\left({x_1}^{p^{-1}}\right) + \boldsymbol{p}\widetilde{x_2}$.
- ……

无穷次执行算法3.3.2.2可以得到一个收敛式

$$\widetilde{x} = \sum_{n=0}^{\infty} \tau_e\left({x_n}^{p^{-n}}\right)\boldsymbol{p}^n \tag{3.3.2.7}$$

同命题2.2.15和命题2.2.16的思想, 我们最终便在 Γ_0 的基础上导出了另一种 $\mathcal{W}(\kappa)$ 到 $\Re$ 的双射形式

$$\begin{array}{rccc} \Gamma_c: & \mathcal{W}(\kappa) & \xrightarrow{1:1} & \Re \\ & x = (x_n)_{n\geq 0} & \to & \sum\limits_{n=0}^{\infty} \tau_e\left({x_n}^{p^{-n}}\right)\boldsymbol{p}^n. \end{array} \tag{3.3.2.8}$$

至此, 我们将研究 Γ_0 是否环态射的注意力转移到研究 Γ_c 是否环态射. 而实际上双射 Γ_c 已经被证明确实是 $\mathcal{W}(\kappa)$ 到 $\Re$ 的一个环态射. 参考李文威 [12, § 10.9], 以下我们对此进行一个系统的说明.

第一步转换 首先, 明确我们的目标是证明 $\forall x := (x_n),\ y := (y_n) \in \mathcal{W}(\kappa)$, 成立

$$\Gamma_c(x \oplus y) = \Gamma_c(x) + \Gamma_c(y), \tag{3.3.2.9a}$$

$$\Gamma_c(x \odot y) = \Gamma_c(x) \odot \Gamma_c(y). \tag{3.3.2.9b}$$

由 § 3.2 节介绍的 Witt 环运算规则, 令

$$\begin{aligned} S(x,y) &:= x \oplus y \in \mathbb{Z}[x_0, \cdots, x_n, \cdots; y_0, \cdots, y_n, \cdots] \subseteq \mathcal{W}(\kappa), \\ P(x,y) &:= x \odot y \in \mathbb{Z}[x_0, \cdots, x_n, \cdots; y_0, \cdots, y_n, \cdots] \subseteq \mathcal{W}(\kappa). \end{aligned}$$

则式 (3.3.2.9) 可进一步地改写为

$$\sum_{n=0}^{\infty} \tau_e\left(S_n(x,y)^{p^{-n}}\right)\boldsymbol{p}^n = \sum_{n=0}^{\infty} \tau_e\left({x_n}^{p^{-n}}\right)\boldsymbol{p}^n + \sum_{n=0}^{\infty} \tau_e\left({y_n}^{p^{-n}}\right)\boldsymbol{p}^n, \tag{3.3.2.10a}$$

$$\sum_{n=0}^{\infty} \tau_e\left(P_n(x,y)^{p^{-n}}\right)\boldsymbol{p}^n = \sum_{n=0}^{\infty} \tau_e\left({x_n}^{p^{-n}}\right)\boldsymbol{p}^n \cdot \sum_{n=0}^{\infty} \tau_e\left({y_n}^{p^{-n}}\right)\boldsymbol{p}^n. \tag{3.3.2.10b}$$

第二步转换 由于存在环同构

$$\begin{array}{rccc} H: & \Re & \xrightarrow{1:1} & \varprojlim_n \Re/\boldsymbol{p}^n\Re \\ & x & \to & \left(x + \boldsymbol{p}^n\Re\right)_{n\geq 0} \end{array}$$

因此 $\Re$ 中 a, b 的相等关系可以等价转换为 a, b 在 $\varprojlim_n \Re/\boldsymbol{p}^n\Re$ 中的像 $H(a)$, $H(b)$ 的等价关系, 即

$$a = b \in \Re. \iff H(a) = H(b) \in \varprojlim_n \Re/\boldsymbol{p}^n\Re. \tag{3.3.2.11}$$

具体地说, 若 $a=b$, 则有

$$H(a)-H(b)=H(a-b)=H(0)=0,\ \text{即}H(a)=H(b).$$

反过来, 若 $H(a)=H(b)$, 则有

$$H(a-b)=H(a)-H(b)=0.$$

由于一定成立 $H(0)=0$, 而 H 是环同构蕴涵 H 是双射, 因此只能是 $a=b$. 因此式 (3.3.2.11) 成立. 基于此, 我们可将式 (3.3.2.10) 等价地改写为

$$H\left(\sum_{n=0}^{\infty}\tau_e\left(S_n(x,y)^{p^{-n}}\right)\boldsymbol{p}^n\right)=H\left(\sum_{n=0}^{\infty}\tau_e\left({x_n}^{p^{-n}}\right)\boldsymbol{p}^n+\sum_{n=0}^{\infty}\tau_e\left({y_n}^{p^{-n}}\right)\boldsymbol{p}^n\right),$$
$$H\left(\sum_{n=0}^{\infty}\tau_e\left(P_n(x,y)^{p^{-n}}\right)\boldsymbol{p}^n\right)=H\left(\sum_{n=0}^{\infty}\tau_e\left({x_n}^{p^{-n}}\right)\boldsymbol{p}^n\cdot\sum_{n=0}^{\infty}\tau_e\left({y_n}^{p^{-n}}\right)\boldsymbol{p}^n\right).$$

又由于 $H(a)$, $H(b)\in\varprojlim_n\Re/\boldsymbol{p}^n\Re$ 是可数无穷序列的形式, $H(a)=H(b)$ 相等, 等价于 $H(a)$, $H(b)$ 每个对应分量都相等, 即有 $\forall m\in\mathbb{Z}_{\geq 0}$, 成立

$$\sum_{n=0}^{\infty}\tau_e\left(S_n(x,y)^{p^{-n}}\right)\boldsymbol{p}^n+\boldsymbol{p}^{m+1}\Re=\left(\sum_{n=0}^{\infty}\tau_e\left({x_n}^{p^{-n}}\right)\boldsymbol{p}^n+\sum_{n=0}^{\infty}\tau_e\left({y_n}^{p^{-n}}\right)\boldsymbol{p}^n\right)+\boldsymbol{p}^{m+1}\Re,$$
$$\sum_{n=0}^{\infty}\tau_e\left(P_n(x,y)^{p^{-n}}\right)\boldsymbol{p}^n+\boldsymbol{p}^{m+1}\Re=\left(\sum_{n=0}^{\infty}\tau_e\left({x_n}^{p^{-n}}\right)\boldsymbol{p}^n\cdot\sum_{n=0}^{\infty}\tau_e\left({y_n}^{p^{-n}}\right)\boldsymbol{p}^n\right)+\boldsymbol{p}^{m+1}\Re.$$

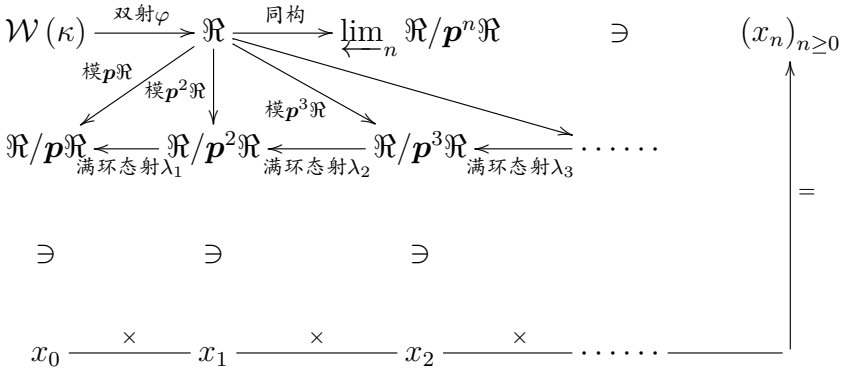
再写成便于处理的模理想 $\boldsymbol{p}^{m+1}\Re$ 同余的形式, 并且约去级数中带 $\boldsymbol{p}^{m+1}$, $\boldsymbol{p}^{m+2}$, $\cdots$ 的高阶项, 即可得到 $\forall m\in\mathbb{Z}_{\geq 0}$, 成立

$$\sum_{n=0}^{m}\tau_e\left(S_n(x,y)^{p^{-n}}\right)\boldsymbol{p}^n\overset{\bmod\boldsymbol{p}^{m+1}\Re}{=\!=\!=}\left(\sum_{n=0}^{m}\tau_e\left({x_n}^{p^{-n}}\right)\boldsymbol{p}^n+\sum_{n=0}^{m}\tau_e\left({y_n}^{p^{-n}}\right)\boldsymbol{p}^n\right)\tag{3.3.2.12a}$$
$$\sum_{n=0}^{m}\tau_e\left(P_n(x,y)^{p^{-n}}\right)\boldsymbol{p}^n\overset{\bmod\boldsymbol{p}^{m+1}\Re}{=\!=\!=}\sum_{n=0}^{m}\tau_e\left({x_n}^{p^{-n}}\right)\boldsymbol{p}^n\cdot\sum_{n=0}^{m}\tau_e\left({y_n}^{p^{-n}}\right)\boldsymbol{p}^n.\tag{3.3.2.12b}$$

注意这里对于式 (3.3.2.12b) 的形式, 我们没有采用更精细的写法

$$\sum_{n=0}^{m}\tau_e\left(P_n(x,y)^{p^{-n}}\right)\boldsymbol{p}^n\equiv\sum_{n=0}^{m}\left(\sum_{i+j=n}\tau_e\left({x_i}^{p^{-i}}\right)\tau_e\left({y_j}^{p^{-j}}\right)\right)\boldsymbol{p}^n\mod\boldsymbol{p}^{m+1}\Re.$$

后面我们会看到, 式 (3.3.2.12b) 的形式经过变形能够和 $\Re$ 上的 Witt 多项式建立联系, 方便我们进一步地思考和证明.



第三次转换 接下来我们进行最后一次等价转换. 这个过程需要依托下面的引理.

引理 3.3.2.3 任取完全环 κ 中的一个元素 x, 记 $x^{p^{-m}} \in \kappa$ 关于模去理想 $\boldsymbol{p}\Re$ 映射 ϕ 的任意一个原像是 $\left[x^{p^{-m}}\right]_{\forall}$, 则恒成立同余式

$$\tau_e\left(x\right) \equiv \left[x^{p^{-m}}\right]_{\forall}^{p^m} \mod \boldsymbol{p}^{m+1}\Re,\ \forall 0 \leq m < \infty.$$

证明 任取一个 $x \in \kappa$. $\forall n \geq 0$, 记 x 的 p^n-次根 $x^{p^{-n}}$ 关于 ϕ 的任一个原像为 $\left[x^{p^{-n}}\right]_1$. 然后再规定 $0 \leq m \leq n$. 由于

$$\phi\left(\left[x^{p^{-n}}\right]_1^{p^{n-m}}\right) = \phi\Big(\left[x^{p^{-n}}\right]_1\Big)^{p^{n-m}} = \left(x^{p^{-n}}\right)^{p^{n-m}} = x^{p^{-m}}.$$

因此 $\left[x^{p^{-n}}\right]_1^{p^{n-m}}$ 是 $x^{p^{-m}}$ 的一个原像. 任取 $x^{p^{-m}}$ 的一个原像 $\left[x^{p^{-m}}\right]_2$, 由于

$$\phi\left(\left[x^{p^{-m}}\right]_2\right) = x^{p^{-m}} = \phi\left(\left[x^{p^{-n}}\right]_1^{p^{n-m}}\right),$$

因此成立同余式

$$\left[x^{p^{-n}}\right]_1^{p^{n-m}} \equiv \left[x^{p^{-m}}\right]_2 \mod \boldsymbol{p}\Re.$$

再根据引理*3.3.1*, 成立

$$\left(\left[x^{p^{-n}}\right]_1^{p^{n-m}}\right)^{p^m} \equiv \left[x^{p^{-m}}\right]_2^{p^m} \mod \boldsymbol{p}^{m+1}\Re,$$

也就是

$$\left[x^{p^{-n}}\right]_1^{p^n} \equiv \left[x^{p^{-m}}\right]_2^{p^m} \mod \boldsymbol{p}^{m+1}\Re,\ \forall n \geq m \geq 0. \tag{3.3.2.13}$$

令式 *(3.3.2.13)* 中的 $n \to \infty$, 即可得

$$\tau_e\left(x\right) = \lim_{n\to\infty}\left[x^{p^{-n}}\right]_1^{p^n} \equiv \left[x^{p^{-m}}\right]_2^{p^m} \mod \boldsymbol{p}^{m+1}\Re,\ \forall 0 \leq m < \infty.$$

至此, 明所欲证. □

推论 3.3.2.4 任取完全环 κ 中的一个元素 x, 则恒成立同余式

$$\tau_e\left(x\right) \equiv \tau_e\Big(x^{p^{-m}}\Big)^{p^m} \mod \boldsymbol{p}^{m+1}\Re.$$

证明 取引理*3.3.2.3*中的 $\left[\cdots\right]_{\forall}$ 为 $\tau_e\left(\cdots\right)$ 即可. □

依托推论3.3.2.4, 我们可以直接得到与式 (3.3.2.12a), 式 (3.3.2.12b) 中同余号右边式子的项相关的同余式

$$\begin{aligned}
&\tau_e\left({x_n}^{p^{-n}}\right) \equiv \tau_e\left(\left((x_n)^{p^{-n}}\right)^{p^{-(m-n)}}\right)^{p^{m-n}} \mod \boldsymbol{p}^{m-n+1}\Re.\\
\Longleftrightarrow\ &\tau_e\left({x_n}^{p^{-n}}\right) \equiv \tau_e\Big({x_n}^{p^{-m}}\Big)^{p^{m-n}} \mod \boldsymbol{p}^{m-n+1}\Re.\\
\Longleftrightarrow\ &\tau_e\left({x_n}^{p^{-n}}\right)\boldsymbol{p}^n \equiv \tau_e\Big({x_n}^{p^{-m}}\Big)^{p^{m-n}}\boldsymbol{p}^n \mod \boldsymbol{p}^{m+1}\Re,\ \forall 0 \leq n \leq m.
\end{aligned}$$

同理也有

$$\tau_e\left({y_n}^{p^{-n}}\right)\equiv\tau_e\left(\left((y_n)^{p^{-n}}\right)^{p^{-(m-n)}}\right)^{p^{m-n}}\mod \boldsymbol{p}^{m-n+1}\Re.$$

$$\Longleftrightarrow\tau_e\left({y_n}^{p^{-n}}\right)\boldsymbol{p}^n\equiv\tau_e\left({y_n}^{p^{-m}}\right)^{p^{m-n}}\boldsymbol{p}^n\mod \boldsymbol{p}^{m+1}\Re,\ \forall 0\le n\le m.$$

至此, 我们可以再将式 (3.3.2.12) 等价改写为

$$\begin{array}{ccc}
W_m^{(\Re)}\left(\tau_e\left(S(x,y)^{p^{-m}}\right)\right) & \xrightarrow[\text{mod}\ \boldsymbol{p}^{m+1}\Re]{\equiv} & W_m^{(\Re)}\left(\left\{\tau_e\left({x_n}^{p^{-m}}\right)\right\}\right)+W_m^{(\Re)}\left(\left\{\tau_e\left({y_n}^{p^{-m}}\right)\right\}\right) \\
= \uparrow & & \uparrow = \\
\sum\limits_{n=0}^{m}\tau_e\left(S_n(x,y)^{p^{-m}}\right)^{p^{m-n}}\boldsymbol{p}^n & \xrightarrow{\equiv} & \sum\limits_{n=0}^{m}\tau_e\left({x_n}^{p^{-m}}\right)^{p^{m-n}}\boldsymbol{p}^n+\sum\limits_{n=0}^{m}\tau_e\left({y_n}^{p^{-m}}\right)^{p^{m-n}}\boldsymbol{p}^n \\
\tau_e\text{是乘性提升}\uparrow\text{指数运算可交换} & \nearrow_{\text{mod}\ \boldsymbol{p}^{m+1}\Re}^{\equiv} & \\
\sum\limits_{n=0}^{m}\tau_e\left(S_n(x,y)^{p^{-n}}\right)\boldsymbol{p}^n & &
\end{array}\tag{3.3.2.14}$$

$$\begin{array}{ccc}
W_m^{(\Re)}\left(\tau_e\left(P(x,y)^{p^{-m}}\right)\right) & \xrightarrow[\text{mod}\ \boldsymbol{p}^{m+1}\Re]{\equiv} & W_m^{(\Re)}\left(\left\{\tau_e\left({x_n}^{p^{-m}}\right)\right\}\right)\cdot W_m^{(\Re)}\left(\left\{\tau_e\left({y_n}^{p^{-m}}\right)\right\}\right) \\
= \uparrow & & \uparrow = \\
\sum\limits_{n=0}^{m}\tau_e\left(P_n(x,y)^{p^{-m}}\right)^{p^{m-n}}\boldsymbol{p}^n & \xrightarrow{\equiv} & \sum\limits_{n=0}^{m}\tau_e\left({x_n}^{p^{-m}}\right)^{p^{m-n}}\boldsymbol{p}^n\cdot\sum\limits_{n=0}^{m}\tau_e\left({y_n}^{p^{-m}}\right)^{p^{m-n}}\boldsymbol{p}^n \\
\tau_e\text{是乘性提升}\uparrow\text{指数运算可交换} & \nearrow_{\text{mod}\ \boldsymbol{p}^{m+1}\Re}^{\equiv} & \\
\sum\limits_{n=0}^{m}\tau_e\left(P_n(x,y)^{p^{-n}}\right)\boldsymbol{p}^n & &
\end{array}\tag{3.3.2.15}$$

其中

$$W_m^{(\Re)}\left(\left\{\tau_e\left({x_n}^{p^{-m}}\right)\right\}\right),\ W_m^{(\Re)}\left(\left\{\tau_e\left({y_n}^{p^{-m}}\right)\right\}\right),$$
$$W_m^{(\Re)}\left(\tau_e\left(S(x,y)^{p^{-m}}\right)\right),\ W_m^{(\Re)}\left(\tau_e\left(P(x,y)^{p^{-m}}\right)\right)$$

分别表示由 $\Re$ 上序列

$$\left\{\tau_e\left({x_n}^{p^{-m}}\right)\right\}_{n\ge0},\ \left\{\tau_e\left({y_n}^{p^{-m}}\right)\right\}_{n\ge0},$$
$$\left\{\tau_e\left(S_n(x,y)^{p^{-m}}\right)\right\}_{n\ge0},\ \left\{\tau_e\left(P_n(x,y)^{p^{-m}}\right)\right\}_{n\ge0}$$

导出的第 $m+1$ 个 Witt 多项式, $\forall m\ge0$.

态射性证明 至此, 参考李文威 [12, 定理 10.9.11], 我们来证明 Γ_c 确实是一个环态射.

命题 3.3.2.5 *式 (3.3.2.14), 式 (3.3.2.15) 是成立的.*

证明 我们只对式 *(3.3.2.14)* 作讨论. 式 *(3.3.2.15)* 的情况同理可证. 这里我们需要考虑 $\prod_{n\ge0}\Re$ 上的 *Witt* 环结构 $\mathcal{W}(\Re)$.

1. 第一步, 记

$$S\left(x_0,\cdots,x_n,\cdots;y_0,\cdots,y_n,\cdots\right):=x\oplus y,\ \forall x:=\left(x_n\right)_{n\geq 0},\ y:=\left(y_n\right)_{n\geq 0}\in\mathcal{W}\left(\kappa\right).$$

由于

$$\left\{\tau_e\left({x_n}^{p^{-m}}\right)\right\}_{n\geq 0},\ \left\{\tau_e\left({y_n}^{p^{-m}}\right)\right\}_{n\geq 0}\in\mathcal{W}\left(\Re\right),$$

我们记

$$S'\begin{pmatrix}\tau_e\left({x_0}^{p^{-m}}\right),\cdots,\tau_e\left({x_n}^{p^{-m}}\right),\cdots;\\ \tau_e\left({y_0}^{p^{-m}}\right),\cdots,\tau_e\left({y_n}^{p^{-m}}\right),\cdots\end{pmatrix}:=\left\{\tau_e\left({x_n}^{p^{-m}}\right)\right\}\oplus\left\{\tau_e\left({y_n}^{p^{-m}}\right)\right\}.$$

由此成立

$$W_m^{(\Re)}\left(S'\begin{pmatrix}\tau_e\left({x_0}^{p^{-m}}\right),\cdots,\tau_e\left({x_n}^{p^{-m}}\right),\cdots;\\ \tau_e\left({y_0}^{p^{-m}}\right),\cdots,\tau_e\left({y_n}^{p^{-m}}\right),\cdots\end{pmatrix}\right) \tag{3.3.2.16a}$$

$$=W_m^{(\Re)}\left(\left\{\tau_e\left({x_n}^{p^{-m}}\right)\right\}\right)+W_m^{(\Re)}\left(\left\{\tau_e\left({y_n}^{p^{-m}}\right)\right\}\right). \tag{3.3.2.16b}$$

2. 第二步, 针对式 *(3.3.2.16a)* 的出现, 我们考虑

$${S_n}'\begin{pmatrix}\tau_e\left({x_0}^{p^{-m}}\right),\cdots,\tau_e\left({x_n}^{p^{-m}}\right),\cdots;\\ \tau_e\left({y_0}^{p^{-m}}\right),\cdots,\tau_e\left({y_n}^{p^{-m}}\right),\cdots\end{pmatrix}\in\Re \tag{3.3.2.17}$$

与

$$\tau_e\left(S_n\left({x_0}^{p^{-m}},\cdots,{x_n}^{p^{-m}},\cdots;{y_0}^{p^{-m}},\cdots,{y_n}^{p^{-m}},\cdots\right)\right)\in\Re \tag{3.3.2.18}$$

的关系. 基于推论*3.2.2.9*, 我们知道式 *(3.3.2.17)*, 式 *(3.3.2.18)* 都是整系数多项式. 而由于模去理想映射 ϕ 满足

$$\phi\left(\boldsymbol{z}\in\Re\right)=\phi\left(\sum_{i=1}^{z}\mathbf{1}\in\Re\right)=\sum_{i=1}^{z}\phi\left(\mathbf{1}\in\Re\right)=\sum_{i=1}^{z}1\in\kappa=z,\ \forall z\in\mathbb{Z}.$$

因此由 ϕ 保持加法和乘法的性质, 成立

$$\begin{aligned}&\phi\left({S_n}'\left(\tau_e\left({x_0}^{p^{-m}}\right),\cdots,\tau_e\left({x_n}^{p^{-m}}\right),\cdots;\tau_e\left({y_0}^{p^{-m}}\right),\cdots,\tau_e\left({y_n}^{p^{-m}}\right),\cdots\right)\right)\\ =&S_n\begin{pmatrix}\phi\left(\tau_e\left({x_0}^{p^{-m}}\right)\right),\cdots,\phi\left(\tau_e\left({x_n}^{p^{-m}}\right)\right),\cdots;\\ \phi\left(\tau_e\left({y_0}^{p^{-m}}\right)\right),\cdots,\phi\left(\tau_e\left({y_n}^{p^{-m}}\right)\right),\cdots\end{pmatrix}\\ =&S_n\left({x_0}^{p^{-m}},\cdots,{x_n}^{p^{-m}},\cdots;{y_0}^{p^{-m}},\cdots,{y_n}^{p^{-m}},\cdots\right)\\ =&\tau_e\left(S_n\left({x_0}^{p^{-m}},\cdots,{x_n}^{p^{-m}},\cdots;{y_0}^{p^{-m}},\cdots,{y_n}^{p^{-m}},\cdots\right)\right).\end{aligned}$$

因此成立

$$\begin{aligned}&{S_n}'\left(\tau_e\left({x_0}^{p^{-m}}\right),\cdots,\tau_e\left({x_n}^{p^{-m}}\right),\cdots;\tau_e\left({y_0}^{p^{-m}}\right),\cdots,\tau_e\left({y_n}^{p^{-m}}\right),\cdots\right)\\ \equiv&\ \tau_e\left(S_n\left({x_0}^{p^{-m}},\cdots,{x_n}^{p^{-m}},\cdots;{y_0}^{p^{-m}},\cdots,{y_n}^{p^{-m}},\cdots\right)\right)\ \bmod \boldsymbol{p}\Re.\end{aligned}$$

继而由引理*3.3.1,* 成立

$$\begin{aligned}&{S_n}'\left(\tau_e\left({x_0}^{p^{-m}}\right),\cdots,\tau_e\left({x_n}^{p^{-m}}\right),\cdots;\tau_e\left({y_0}^{p^{-m}}\right),\cdots,\tau_e\left({y_n}^{p^{-m}}\right),\cdots\right)^{p^{m-n}}\\\equiv\ &\tau_e\left(S_n\left({x_0}^{p^{-m}},\cdots,{x_n}^{p^{-m}},\cdots;{y_0}^{p^{-m}},\cdots,{y_n}^{p^{-m}},\cdots\right)\right)^{p^{m-n}}\mod \boldsymbol{p}^{m-n+1}\Re.\end{aligned}$$

同余号两端再同时乘以 $\boldsymbol{p}^n$, $0\leq n\leq m$, 成立

$$\begin{aligned}&{S_n}'\left(\tau_e\left({x_0}^{p^{-m}}\right),\cdots,\tau_e\left({x_n}^{p^{-m}}\right),\cdots;\tau_e\left({y_0}^{p^{-m}}\right),\cdots,\tau_e\left({y_n}^{p^{-m}}\right),\cdots\right)^{p^{m-n}}\boldsymbol{p}^n\\\equiv\ &\tau_e\left(S_n\left({x_0}^{p^{-m}},\cdots,{x_n}^{p^{-m}},\cdots;{y_0}^{p^{-m}},\cdots,{y_n}^{p^{-m}},\cdots\right)\right)^{p^{m-n}}\boldsymbol{p}^n\mod \boldsymbol{p}^{m+1}\Re.\end{aligned}$$

因此有

$$W_m^{(\Re)}\left(S'\begin{pmatrix}\tau_e\left({x_0}^{p^{-m}}\right),\cdots,\tau_e\left({x_n}^{p^{-m}}\right),\cdots;\\\tau_e\left({y_0}^{p^{-m}}\right),\cdots,\tau_e\left({y_n}^{p^{-m}}\right),\cdots\end{pmatrix}\right)\tag{3.3.2.19a}$$

$$\equiv W_m^{(\Re)}\left(\tau_e\left(S\begin{pmatrix}{x_0}^{p^{-m}},\cdots,{x_n}^{p^{-m}},\cdots;\\{y_0}^{p^{-m}},\cdots,{y_n}^{p^{-m}},\cdots\end{pmatrix}\right)\right)\mod \boldsymbol{p}^{m+1}\Re.\tag{3.3.2.19b}$$

3. 第三步, 针对式 *(3.3.2.19b)* 的出现, 我们考虑

$$\tau_e\left(S\left({x_0}^{p^{-m}},\cdots,{x_n}^{p^{-m}},\cdots;{y_0}^{p^{-m}},\cdots,{y_n}^{p^{-m}},\cdots\right)\right)$$

与

$$\tau_e\left(S(x_0,\cdots,x_n,\cdots;y_0,\cdots,y_n,\cdots)^{p^{-m}}\right)$$

的关系. 由于 $S\left({x_0}^{p^{-m}},\cdots,{x_n}^{p^{-m}},\cdots;{y_0}^{p^{-m}},\cdots,{y_n}^{p^{-m}},\cdots\right)^{p^m}\in\kappa$, 而 $\operatorname{char}(\kappa)=p$, 基于多项式幂的展开和引理*3.2.2.1,* 我们有

$$S\begin{pmatrix}{x_0}^{p^{-m}},\cdots,{x_n}^{p^{-m}},\cdots;\\{y_0}^{p^{-m}},\cdots,{y_n}^{p^{-m}},\cdots\end{pmatrix}^{p^m}=S\left(x_0,\cdots,x_n,\cdots;y_0,\cdots,y_n,\cdots\right)\in\kappa.\tag{3.3.2.20}$$

又由于 κ 是一个完全环, κ 中任一个元素都存在唯一的一个 p^m-次根, $\forall m\geq 0$, 于是对式 *(3.3.2.20)* 左右两端取 p^m-次根, 可以得到

$$S\left({x_0}^{p^{-m}},\cdots,{x_n}^{p^{-m}},\cdots;{y_0}^{p^{-m}},\cdots,{y_n}^{p^{-m}},\cdots\right)=S(x_0,\cdots,x_n,\cdots;y_0,\cdots,y_n,\cdots)^{p^{-m}}.$$

也就有

$$\tau_e\left(S\begin{pmatrix}{x_0}^{p^{-m}},\cdots,{x_n}^{p^{-m}},\cdots;\\{y_0}^{p^{-m}},\cdots,{y_n}^{p^{-m}},\cdots\end{pmatrix}\right)=\tau_e\left(S\begin{pmatrix}x_0,\cdots,x_n,\cdots;\\y_0,\cdots,y_n,\cdots\end{pmatrix}^{p^{-m}}\right).\tag{3.3.2.21}$$

4. 第四步, 综合式 *(3.3.2.16),* 式 *(3.3.2.19),* 式 *(3.3.2.21),* 我们总结得到

$$\begin{aligned}&W_m^{(\Re)}\left(\left\{\tau_e\left({x_n}^{p^{-m}}\right)\right\}\right)+W_m^{(\Re)}\left(\left\{\tau_e\left({y_n}^{p^{-m}}\right)\right\}\right)\\\xlongequal{\text{式(3.3.2.16)}}\ &W_m^{(\Re)}\left(S'\left(\tau_e\left({x_0}^{p^{-m}}\right),\cdots,\tau_e\left({x_n}^{p^{-m}}\right),\cdots;\tau_e\left({y_0}^{p^{-m}}\right),\cdots,\tau_e\left({y_n}^{p^{-m}}\right),\cdots\right)\right)\\\xlongequal{\text{式(3.3.2.19)}}\ &W_m^{(\Re)}\left(\tau_e\left(S\left({x_0}^{p^{-m}},\cdots,{x_n}^{p^{-m}},\cdots;{y_0}^{p^{-m}},\cdots,{y_n}^{p^{-m}},\cdots\right)\right)\right)\mod \boldsymbol{p}^{m+1}\Re.\\\xlongequal{\text{式(3.3.2.21)}}\ &W_m^{(\Re)}\left(\tau_e\left(S(x_0,\cdots,x_n,\cdots;y_0,\cdots,y_n,\cdots)^{p^{-m}}\right)\right)\end{aligned}$$

至此, 明所欲证. 而对于式 *(3.3.2.15)* 的证明, 只需将上面相应的符号和运算稍加修改即可, 例如将 S, S' 换成 P, P', 将式 *(3.3.2.16b)* 中的 $+$ 换成 $\times$, 即可给出相应的证明. □

注记 上述证明过程中涉及到 *Witt* 多项式的部分, *Witt* 多项式的系数 π 可取不等于 $\mathrm{char}(\kappa)$, $\mathrm{char}(\Re)$ 的任一个素数.

至此, 我们证明了双射

$$\Gamma_c : \begin{array}{ccc} \mathcal{W}(\kappa) & \to & \Re \\ x = (x_n)_{n\geq 0} & \to & \sum_{n=0}^{\infty} \tau_e\left({x_n}^{p^{-n}}\right)\boldsymbol{p}^n \end{array}$$

是一个环态射, 即 $\mathcal{W}(\kappa)$ 与 $\Re$ 之间关于 Γ_c 形成环同构, 这也就导出了我们 § 3 节最终要探索的东西.

定理 3.3.2.6 设 $\Re$ 是一个严格 p-环, $\kappa := \Re/\boldsymbol{p}\Re$ 是其剩余类环, 则在环同构意义下成立

$$\mathcal{W}(\kappa) = \Re.$$

推论 3.3.2.7 $\mathcal{W}(\mathbb{F}_p) = \mathbb{Z}_p$.

证明 例子*2.2.13*说明了 $\mathbb{Z}_p$ 是一个严格 p-环; 命题*2.2.1*说明了剩余类环 $\mathbb{Z}_p/p\mathbb{Z}_p$ 可以视为 $\mathbb{F}_p$. 因此显然有

$$\mathcal{W}(\mathbb{F}_p) \xrightarrow{\Gamma_c} \mathbb{Z}_p.$$

明所欲证. □

A 附录

- 附录A.1服务于第 § 2.1 节;
- 附录A.2服务于第 § 2.3 节.

A.1 关于组合数是整数的一种严格证明

引理 A.1.1 设 $n \in \mathbb{Z}_{>0}$, p 是一个素数, 若 $p^i \| n!$, 则有

$$i = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right].$$

证明 显然地, i 即为 $n!$ 的标准分解式中素因子 p 的指数. 将 $n!$ 展开, 视为 n 个数的乘积

$$n! = 1 \times 2 \times \cdots \times n.$$

记

$$A := \{1,\ 2,\ \ldots,\ n\},\ B_k := \{b \in A :\ p^k \mid b\},\ k = 1,\ 2,\ \ldots.$$

注意到当 k 充分大时, 有 $p^k > n$, 此时 $B_k = \varnothing$, 即 $\exists s \in \mathbb{Z}_{>0}$, 使得 $\forall k > s$, $B_k = \varnothing$, $|B_k| = 0$.

由于 $\forall i \leq j$, $p^j \mid b. \Rightarrow p^i \mid b$, 因此成立以下包含关系

$$B_1 \supseteq B_2 \supseteq \ldots B_s \supseteq B_{s+1} = B_{s+2} = \cdots = \varnothing,$$

其中 $\forall k \in \mathbb{Z}_{>0}$, 有 $|B_k| = \left[n/p^k \right]$.

另记

$$C_k := \{c \in A :\ p^k \| c\}.$$

则有 $C_k = B_k \setminus B_{k+1}$, $|C_k| = |B_k \setminus B_{k+1}| = |B_k| - |B_{k+1}|$. $n!$ 标准分解式中 p 的指数 i 为

$$\begin{aligned} i &= \sum_{k=1}^{\infty} k \left| C_k \right|. \\ &= \sum_{k=1}^{\infty} k \left(|B_k| - |B_{k+1}| \right). \\ &= \sum_{k=1}^{s} k \left(|B_k| - |B_{k+1}| \right). \\ &= \sum_{k=1}^{s} \left| B_k \right|. \\ &= \sum_{k=1}^{s} \left[\frac{n}{p^k} \right]. \end{aligned}$$

至此, 明所欲证. □

定理 A.1.2 设 $n \in \mathbb{Z}_{>0}$, $\forall k \in \{0,\ 1,\ \ldots,\ n\}$, 贾宪数 $\binom{n}{k}$ 是正整数, 即有

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} \in \mathbb{Z}_{>0}.$$

证明 $\forall x,\ y \in \mathbb{R}$, $[x] + [y] \leq [x+y]$. 在此基础上, 令 $x = k/p^r$, $y = (n-k)/p^r$, 其中 $r \in \mathbb{Z}_{\geq 0}$, p 是一个素数, 则自然成立下式

$$\left[\frac{k}{p^r}\right] + \left[\frac{n-k}{p^r}\right] \leq \left[\frac{n}{p^r}\right]. \tag{A.1.0.1}$$

记

$$S := \{p\text{是素数}:\ p \mid k!\ \vee\ p \mid n!\ \vee\ p \mid (n-k)!\}.$$

显然地, 有 $\max S \leq \min\{k!,\ (n-k)!\}$, 因此 $|S| < \infty$, 从而可以进一步将集合 S 表示为

$$S = \{p_1,\ p_2,\ \ldots,\ p_m\},$$

其中 $p_1,\ p_2,\ \ldots,\ p_m$ 是 m 个两两不相等的素数. 而 $k!$, $(n-k)!$, $n!$ 也可以进一步表为

$$\begin{aligned} k! &= {p_1}^{\alpha_1} \ldots {p_m}^{\alpha_m}, \\ (n-k)! &= {p_1}^{\beta_1} \ldots {p_m}^{\beta_m}, \\ n! &= {p_1}^{\gamma_1} \ldots {p_m}^{\gamma_m}, \end{aligned}$$

其中 $a_i,\ \beta_i,\ \gamma_i \in \mathbb{Z}_{\geq 0}$, $\forall i \in \{1,\ 2,\ \ldots,\ m\}$. 显然地, 成立

$${p_i}^{\alpha_i} \| k!, \tag{A.1.0.2a}$$

$${p_i}^{\beta_i} \| (n-k)!, \tag{A.1.0.2b}$$

$${p_i}^{\gamma_i} \| n!. \tag{A.1.0.2c}$$

由引理*A.1.1*, 有

$$\alpha_i = \sum_{r=1}^{\infty} \left[\frac{k}{{p_i}^r}\right], \tag{A.1.0.3a}$$

$$\beta_i = \sum_{r=1}^{\infty} \left[\frac{n-k}{{p_i}^r}\right], \tag{A.1.0.3b}$$

$$\gamma_i = \sum_{r=1}^{\infty} \left[\frac{n}{{p_i}^r}\right]. \tag{A.1.0.3c}$$

式 *(A.1.0.1), (A.1.0.3)* 蕴含 $\alpha_i + \beta_i \leq \gamma_i$, $\forall i \in \{1,\ 2,\ \ldots,\ m\}$. 结合 $k!$, $(m-k)!$, $n!$ 的标准分解式 *(A.1.0.2)*, 即有

$$k!\,(n-k)! \mid n!. \implies \frac{n!}{k!\,(n-k)!} \in \mathbb{Z}_{>0}.$$

至此, 明所欲证. □

A.2 完备化的若干问题说明

设 $\mathfrak{R}$ 是一个环, $|\bullet|$ 是 $\mathfrak{R}$ 上的一个赋值, 记

$$\mathfrak{C} := \left\{ \{a_n\} : \ \{a_n\} \text{是}\mathfrak{R}\text{中的柯西列} \right\},$$
$$\mathfrak{m} := \left\{ \{a_n\} : \ \lim_{n\to\infty} |a_n| = 0 \right\}.$$

$\forall \{a_n\}, \{b_n\} \in \mathfrak{C}$, 定义 $\mathfrak{C}$ 上的加法 $+$, 乘法 $\times$ 如下:

$$\{a_n\} + \{b_n\} := \{a_n + b_n\},$$
$$\{a_n\} \times \{b_n\} := \{a_n \times b_n\}.$$

定义 $\mathfrak{C}/\mathfrak{m}$ 上的单射 $|\bullet|_\bigstar$ 如下:

$$|x|_\bigstar := \lim_{n\to\infty} |a_n| \in \mathbb{R}_{\geq 0}, \ \forall x = \{a_n\} + \mathfrak{m} \in \mathfrak{C}/\mathfrak{m}.$$

下面针对商环 $\mathfrak{C}/\mathfrak{m}$ 的由来给出两个命题.

命题 A.2.1 (商环 $\mathfrak{C}/\mathfrak{m}$ 的由来) $(\mathfrak{C}, +, \times)$ 是一个含幺交换环.

证明

1. 首先证明 $(\mathfrak{C}, +)$ 是一个阿贝尔群.

(a) 封闭性

$\{a_n\}$, $\{b_n\}$ 是 $\mathfrak{R}$ 中的柯西列, 因此 $\forall \varepsilon > 0$, $\exists N_a, \ N_b \in \mathbb{N}$, 使得

$$|a_n - a_m| < \frac{\varepsilon}{2}, \ \forall n, \ m \geq N_a, \tag{A.2.0.1a}$$
$$|b_n - b_m| < \frac{\varepsilon}{2}, \ \forall n, \ m \geq N_b. \tag{A.2.0.1b}$$

取 $N = \max\{N_a, N_b\}$, $\forall n, \ m \geq N$, 成立

$$\begin{aligned} &|(a_n + b_n) - (a_m + b_m)|. \\ =&|(a_n - a_m) + (b_n - b_m)|. \\ \leq&|a_n - a_m| + |b_n - b_m|. \\ <&\frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

因此 $\{a_n + b_n\}$ 也是 $\mathfrak{R}$ 的一个柯西列, $\{a_n + b_n\} \in \mathfrak{C}$.

(b) 结合律

$$\begin{aligned} &(\{a_n\} + \{b_n\}) + \{c_n\}. \\ =&\{a_n + b_n\} + \{c_n\}. \\ =&\{a_n + b_n + c_n\}. \\ =&\{a_n + (b_n + c_n)\}. \\ =&\{a_n\} + \{b_n + c_n\}. \\ =&\{a_n\} + (\{b_n\} + \{c_n\}). \end{aligned}$$

(c) 交换律

$$\{a_n\}+\{b_n\}=\{a_n+b_n\}=\{b_n+a_n\}=\{b_n\}+\{a_n\}.$$

(d) 单位元

显然常数列 $\{0\}\in\mathfrak{C}$, 且满足

$$\{a_n\}+\{0\}=\{a_n+0\}=\{a_n\}.$$

(e) 可逆性

对 $\{a_n\}\in\mathfrak{C}$, 存在 $\{-a_n\}\in\mathfrak{C}$, 使得

$$\{a_n\}+\{-a_n\}=\{a_n-a_n\}=\{0\}.$$

2. 其次证明 $(C,\times)$ 是一个阿贝尔幺半群.

(a) 封闭性

式 *(A.2.0.1a)* 中令 $m=N_a$, 得到

$$|a_n-a_{N_a}|<\frac{\varepsilon}{2},\ \forall n\geq N_a.$$

利用赋值的三角不等式性, 有

$$|a_n|<\frac{\varepsilon}{2}+|a_{N_a}|,\ \forall n\geq N_a.$$

式 *(A.2.0.1b)* 中令 $n=N_b$, 同理得到

$$|b_m|<\frac{\varepsilon}{2}+|b_{N_b}|,\ \forall m\geq N_b.$$

对新序列 $\{a_n\times b_n\}$, 由于

$$\begin{aligned}
&|a_n\times b_n-a_m\times b_m|.\\
=&|a_n(b_n-b_m)+b_m(a_n-a_m)|.\\
\leq&|a_n||b_n-b_m|+|b_m||a_n-a_m|.\\
<&\left(\frac{\varepsilon}{2}+|a_{N_a}|\right)\times\frac{\varepsilon}{2}+\left(\frac{\varepsilon}{2}+|b_{N_b}|\right)\times\frac{\varepsilon}{2}.\\
=&\left(\frac{1}{2}\varepsilon+\frac{|a_{N_a}+b_{N_b}|}{2}\right)\varepsilon,
\end{aligned}$$

其中

$$\left(\frac{1}{2}\varepsilon+\frac{|a_{N_a}+b_{N_b}|}{2}\right)\varepsilon\in(0,\infty),\ \varepsilon\in(0,\infty).$$

因此 $\{a_n\times b_n\}$ 也是一个柯西列, $\{a_n\times b_n\}\in\mathfrak{C}$.

(b) 结合律

$$\begin{aligned}&(\{a_n\}\times\{b_n\})\times\{c_n\}.\\=&\{a_n\times b_n\}\times\{c_n\}.\\=&\{a_n\times b_n\times c_n\}.\\=&\{a_n\times(b_n\times c_n)\}.\\=&\{a_n\}\times\{b_n\times c_n\}.\\=&\{a_n\}\times(\{b_n\}\times\{c_n\}).\end{aligned}$$

(c) 交换律

$$\{a_n\}\times\{b_n\}=\{a_n\times b_n\}=\{b_n\times a_n\}=\{b_n\}\times\{a_n\}.$$

(d) 单位元

显然常数列 $\{1\}\in\mathfrak{C}$, 且满足

$$\{a_n\}\times\{1\}=\{a_n\times 1\}=\{a_n\}.$$

3. 最后证明 $\mathfrak{C}$ 关于 $+$, $\times$ 满足两个分配律.

(a) 分配律一

$$\begin{aligned}&(\{a_n\}+\{b_n\})\times\{c_n\}.\\=&\{a_n+b_n\}\times\{c_n\}.\\=&\{(a_n+b_n)\times c_n\}.\\=&\{a_n\times c_n+b_n\times c_n\}.\\=&\{a_n\}\times\{c_n\}+\{b_n\}\times\{c_n\}.\end{aligned}$$

(b) 分配律二

$$\begin{aligned}&\{a_n\}\times(\{b_n\}+\{c_n\}).\\=&\{a_n\}\times\{b_n+c_n\}.\\=&\{a_n\times(b_n+c_n)\}.\\=&\{a_n\times b_n+a_n\times c_n\}.\\=&\{a_n\}\times\{b_n\}+\{a_n\}\times\{c_n\}.\end{aligned}$$

至此, 明所欲证. □

命题 A.2.2 (商环 $\mathfrak{C}/\mathfrak{m}$ 的由来) $\mathfrak{m}$ 是 $\mathfrak{C}$ 的一个双边理想.

证明

1. 首先证明 $\mathfrak{m} \subseteq \mathfrak{C}$.

对 $\{a_n\} \in \mathfrak{m}$, 由定义, $\forall \varepsilon > 0$, $\exists N \in \mathbb{N}$ 使得

$$|a_n| < \frac{\varepsilon}{2},\ \forall n \geq \mathbb{N}.$$

也就有

$$|a_n - a_m| \leq |a_n| + |a_m| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,\ \forall m,\ n \geq \mathbb{N}.$$

于是 $\{a_n\}$ 也是一个柯西列, $\{a_n\} \in \mathfrak{C}$, $\mathfrak{m} \subseteq \mathfrak{C}$.

2. 然后证明 $(\mathfrak{m}, +)$ 是一个群.

(a) 封闭性：

对于 $\{a_n\}$, $\{b_n\} \in \mathfrak{m}$, 由于

$$\lim_{n\to\infty} (a_n + b_n) = \lim_{n\to\infty} a_n + \lim_{n\to\infty} b_n = 0 + 0 = 0.$$

于是有 $\{a_n + b_n\} \in \mathfrak{m}$.

(b) 结合律：继承于 $(\mathfrak{C}, +)$.

(c) 单位元：常数列 $\{0\}$.

(d) 可逆性：

对 $\{a_n\} \in \mathfrak{m}$, $\exists \{-a_n\} \in \mathfrak{m}$, 使得

$$\{a_n\} + \{-a_n\} = \{a_n - a_n\} = \{0\}.$$

3. 最后证明 $\mathfrak{mC} \subseteq \mathfrak{m}$.

$\forall \{a_n\} \in \mathfrak{m}$, $\{b_n\} \in \mathfrak{C}$, $\forall \varepsilon > 0$, $\exists N_a,\ N_b \in \mathbb{N}$, 成立

$$|a_n| < \varepsilon,\ \forall n \geq N_a, \tag{A.2.0.2a}$$

$$|b_n - b_m| < \varepsilon,\ \forall n \geq m \geq N_b. \tag{A.2.0.2b}$$

式 *(A.2.0.2b)* 中令 $m = N_b$, 并利用赋值的三角不等式性, 得到

$$|b_n| < \varepsilon + |b_{N_b}|,\ \forall n \geq N_b.$$

取 $N = \max\{N_a,\ N_b\}$, 即得

$$|a_n \times b_n| = |a_n| \times |b_n| < (\varepsilon + |b_{N_b}|)\,\varepsilon \in (0, \infty),\ \varepsilon \in (0, \infty).$$

即有 $\lim\limits_{n\to\infty} |a_n b_n| = 0$, $\{a_n b_n\} \in \mathfrak{m}$, $\mathfrak{mC} \subseteq \mathfrak{m}$. 同理也有 $\mathfrak{Cm} \subseteq \mathfrak{m}$. □

由此, 我们得到一个商环结构:

$$\mathfrak{C}/\mathfrak{m} = \{\{a_n\} + \mathfrak{m} :\ \{a_n\} \in \mathfrak{C}\}.$$

其上的加法 $+$, 乘法 $\times$ 定义为:

$$(\{a_n\}+\mathfrak{m})+(\{b_n\}+\mathfrak{m}):=\{a_n+b_n\}+\mathfrak{m},$$
$$(\{a_n\}+\mathfrak{m})\times(\{b_n\}+\mathfrak{m}):=\{a_n\times b_n\}+\mathfrak{m}.$$

下面依次对 $\mathfrak{C}/\mathfrak{m}$ 上定义的 $|\cdot|_\bigstar$ 的存在性, 良定义问题, 赋值结构性分析如下.

命题 A.2.3 (关于 $|\cdot|_\bigstar$ 的存在性问题) $\mathfrak{C}/\mathfrak{m}$ 上的函数 $|\cdot|_\bigstar$:

$$|x|_\bigstar:=\lim_{n\to\infty}|a_n|\in\mathbb{R}_{\geq 0},\ \forall x=\{a_n\}+\mathfrak{m}\in\mathfrak{C}/\mathfrak{m},$$

其值是一定存在的.

证明 事实上, $\{a_n\}\in\mathfrak{C}$ 是 $\mathfrak{R}$ 上的柯西列, 有 $\forall\varepsilon>0$, $\exists N\in\mathbb{N}$, 使得

$$|a_n-a_m|<\varepsilon,\ \forall n,\ m\geq N. \tag{A.2.0.3}$$

由赋值的三角不等式性, 得到

$$||a_n|-|a_m||_\infty<|a_n-a_m|. \tag{A.2.0.4}$$

式 *(A.2.0.3)* 和式 *(A.2.0.3)* 蕴含了

$$||a_n|-|a_m||_\infty<\varepsilon,\ \forall n,\ m\geq N.$$

说明了 $\{|a_n|\}$ 是 $\mathbb{R}$ 上的柯西列. 由于 $\mathbb{R}$ 关于普通赋值 $|\cdot|_\infty$ 是完备的, 根据 *[7, 定理 2.11]*, $\{|a_n|\}$ 收敛, $|x|_\bigstar=\lim\limits_{n\to\infty}|a_n|$ 存在. □

命题 A.2.4 (关于 $|\cdot|_\bigstar$ 的良定义问题) $\forall x\in\mathfrak{C}/\mathfrak{m}$, 若存在柯西列 $\{a_n\}$, $\{b_n\}\in\mathfrak{C}$, 满足

$$\{a_n\}+\mathfrak{m}=\{b_n\}+\mathfrak{m}=x. \tag{A.2.0.5}$$

则一定成立

$$\lim_{n\to\infty}|a_n|=\lim_{n\to\infty}|b_n|. \tag{A.2.0.6}$$

证明 事实上, 由式 *(A.2.0.5)*, 存在收敛到 0 的柯西列 $\{c_n\}$, $\{d_n\}\in\mathfrak{m}$, 使得

$$\begin{aligned}&\{a_n\}+\{c_n\}=\{b_n\}+\{d_n\}.\\ \Longrightarrow&\{a_n\}=\{b_n\}+\{d_n\}-\{c_n\}.\\ \Longrightarrow&\{a_n\}=\{b_n+d_n-c_n\}.\end{aligned}$$

于是有

$$\begin{aligned}|a_n|=|b_n+d_n-c_n|\leq|b_n|+|d_n-c_n|\to|b_n|+0=|b_n|\ \ (n\to\infty),\\ |a_n|=|b_n+d_n-c_n|\geq||b_n|-|d_n-c_n||_\infty\to||b_n|-0|_\infty=|b_n|\ \ (n\to\infty).\end{aligned}$$

于是成立式 *(A.2.0.6)*. □

命题 A.2.5 $\mathfrak{C}$ 上的单射 $|\cdot|_\star$ 是 $\mathfrak{C}$ 上的一个赋值结构.

证明 对于 $x = \{a_n\} + \mathfrak{m}$, $y = \{b_n\} + \mathfrak{m}$, $\{a_n\}$, $\{b_n\} \in \mathfrak{C}$,

1. $\{0\} + \mathfrak{m}$ 是商环 $\mathfrak{C}/\mathfrak{m}$ 的加法单位元,

   (a) 一方面, 显然有

   $$x = \{0\} + \mathfrak{m}. \implies |x|_\star = \lim_{n\to\infty} |0| = 0. \tag{A.2.0.7}$$

   (b) 另一方面,

   $$|x|_\star = \lim_{n\to\infty} |a_n| = 0. \implies \{a_n\} \in \mathfrak{m}. \tag{A.2.0.8}$$

   由双边理想 $\mathfrak{m}$ 关于 $+$ 的运算封闭性, 以及 $\mathfrak{m} + \mathfrak{m} = \mathfrak{m}$, 有

   $$\mathfrak{m} = \{0\} + \mathfrak{m} \subseteq \{a_n\} + \mathfrak{m} + \mathfrak{m} = \{a_n\} + \mathfrak{m} \subseteq \mathfrak{m}.$$

   即得

   $$\{a_n\} + \mathfrak{m} = \mathfrak{m} = \{0\} + \mathfrak{m}. \tag{A.2.0.9}$$

   由式 *(A.2.0.8)* 和式 *(A.2.0.9)*, 即有

   $$|x|_\star = \lim_{n\to\infty} |a_n| = 0. \implies x = \{0\} + \mathfrak{m}. \tag{A.2.0.10}$$

   (c) 由式 *(A.2.0.7)* 和式 *(A.2.0.10)*, 即有

   $$|x|_\star = \lim_{n\to\infty} |a_n| = 0. \iff x = \{0\} + \mathfrak{m}, \tag{A.2.0.11}$$

   满足定义*1.1.1*的条件 *(1)*.

2. 成立

   $$|xy|_\star = \lim_{n\to\infty} |a_n b_n| = \lim_{n\to\infty} |a_n| \cdot \lim_{n\to\infty} |b_n| = |x|_\star |y|_\star,$$

   满足定义*1.1.1*的条件 *(2)*.

3. 成立

   $$|x+y|_\star = \lim_{n\to\infty} |a_n + b_n| \le \lim_{n\to\infty} (|a_n| + |b_n|) = \lim_{n\to\infty} |a_n| + \lim_{n\to\infty} |b_n| = |x|_\star + |y|_\star,$$

   满足定义*1.1.1*的条件 *(3)*. □

索引

参考文献

[1] E.E. Enochs and O.M.G. Jenda. Relative Homological Algebra [M]. Berlin: Walter de Gruyer, 1 edition, 2000.

[2] I.B. Fesenko and S.V. Vostokov. Local Fields and Their Extensions [M]. American Mathematical Society, 2 edition, 2002.

[3] J. Neukirch. Algebraic Number Theory [M], volume 322 of Grundlehren der mathematischen Wissenschaften. Berlin Heidelberg: Springer-Verlag, 1 edition, 1999.

[4] J.-P. Serre. Local Fields [M], volume 67 of Graduate Texts in Mathematics. New York: Springer-Verlag, 1 edition, 1979.

[5] E. Witt. Zyklische Körper und Algebren der Charakteristik p vom Grade p^n [J]. J. Reine Ang. Math., 176:126–140, 1936.

[6] 冯克勤，李尚志和章璞. 近世代数引论 [M]. 合肥：中国科学技术大学出版社，第 3 版, 2009.

[7] 华东师范大学数学系. 数学分析 (上册)[M]. 北京：高等教育出版社，第 4 版, 2010.

[8] 夏道行，吴卓人和严绍宗等. 实变函数论与泛函分析 [M]. 北京：高等教育出版社，第 2 版, 1985.

[9] 尤承业. 基础拓扑学讲义 [M]. 北京：北京大学出版社，第 1 版, 2004.

[10] 屈婉玲，耿素云和张立昂. 离散数学 [M]. 北京：清华大学出版社，第 3 版, 2014.

[11] 易大义，沈云宝和李有法. 计算方法 [M]. 杭州：浙江大学出版社，第 2 版, 2002.

[12] 李文威. 代数学方法（卷一：基础架构）[M]. 北京：高等教育出版社，第 1 版, 2018.

[13] 王志兰. 费马小定理的几种证法及应用 [J]. 廊坊师范学院学报（自然科学版）, 9:11 – 13, 2009.

[14] 程其襄，张奠宙和胡善文等. 实变函数与泛函分析基础 [M]. 北京：高等教育出版社，第 4 版, 2019.

[15] 闵嗣鹤和严士健. 初等数论 [M]. 北京：高等教育出版社，第 4 版, 2020.

致谢

本学位论文是在我的导师：**陈哲**老师的亲切关怀和悉心指导下完成的。从课题的选择，文献的阅读，课题难点的突破到论文的完稿，陈哲老师不光给了我很大的支持力度，也给了我比较自由的发挥空间，让我得以在本科学习生涯的末尾真正做到自主、自发地研究一项课题。故在此向陈哲老师致以崇高的敬意。

其次，感谢我大学四年来理学院数学系里的，以**娄增建教授、林福荣教授、乌兰哈斯教授、叶瑞松教授**等为代表的，所有给我授过课的老师，是他们帮助我在本科阶段接触高等数学的各个分支，并打下比较合格的数学基础。在此向这些老师的辛勤劳动表以深切的感激和肯定。此外，也感谢为人和善而负责的数学系教务员**陈莉**老师在四年里帮助我们管理各项学习内外的杂务。

最后，特别感谢**我的母亲**。在我独自攻克难点并不断受挫和崩溃的过程中，是她一直给予我陪伴、支持和鼓励。也感谢包括**罗铮帆**同学在内的我的舍友、包括**黄非凡**同学在内的我的挚友，在学习、生活、做人等方面对我的帮助。