

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 4.3.2.3 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 $\mathbf{p}\mathfrak{R}$ 映射 ϕ 的任意一个原像是 $[x^{p^{-m}}]_{\forall}$, 则恒成立同余式

$$\tau_e(x) \equiv [x^{p^{-m}}]_{\forall}^{p^m} \pmod{\mathbf{p}^{m+1}\mathfrak{R}}, \quad \forall 0 \leq m < \infty.$$

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 $[x^{p^{-n}}]_1$. 然后再规定 $0 \leq m \leq n$. 由于

$$\phi\left([x^{p^{-n}}]_1^{p^{n-m}}\right) = \phi\left([x^{p^{-n}}]_1\right)^{p^{n-m}} = \left(x^{p^{-n}}\right)^{p^{n-m}} = x^{p^{-m}}.$$

因此 $[x^{p^{-n}}]_1^{p^{n-m}}$ 是 $x^{p^{-m}}$ 的一个原像. 任取 $x^{p^{-m}}$ 的一个原像 $[x^{p^{-m}}]_2$, 由于

$$\phi\left([x^{p^{-m}}]_2\right) = x^{p^{-m}} = \phi\left([x^{p^{-n}}]_1^{p^{n-m}}\right),$$

因此成立同余式

$$[x^{p^{-n}}]_1^{p^{n-m}} \equiv [x^{p^{-m}}]_2 \pmod{\mathbf{p}\mathfrak{R}}.$$

再根据引理 4.3.1, 成立

$$\left([x^{p^{-n}}]_1^{p^{n-m}}\right)^{p^m} \equiv [x^{p^{-m}}]_2^{p^m} \pmod{\mathbf{p}^{m+1}\mathfrak{R}},$$

也就是

$$[x^{p^{-n}}]_1^{p^n} \equiv [x^{p^{-m}}]_2^{p^m} \pmod{\mathbf{p}^{m+1}\mathfrak{R}, \quad \forall n \geq m \geq 0. \quad (4.3.2.13)}$$

令式 (4.3.2.13) 中的 $n \rightarrow \infty$, 即可得

$$\tau_e(x) = \lim_{n \rightarrow \infty} [x^{p^{-n}}]_1^{p^n} \equiv [x^{p^{-m}}]_2^{p^m} \pmod{\mathbf{p}^{m+1}\mathfrak{R}, \quad \forall 0 \leq m < \infty.}$$

至此, 明所欲证. □

推论 4.3.2.4 任取完全环 κ 中的一个元素 x , 则恒成立同余式

$$\tau_e(x) \equiv \tau_e\left(x^{p^{-m}}\right)^{p^m} \pmod{\mathbf{p}^{m+1}\mathfrak{R}}.$$

证明 取引理 4.3.2.3 中的 $[\dots]_{\forall}$ 为 $\tau_e(\dots)$ 即可. □

依托推论 4.3.2.4, 我们可以直接得到与式 (4.3.2.12a), 式 (4.3.2.12b) 中同余号右边式子的项相关的同余式

$$\begin{aligned} \tau_e\left(x_n^{p^{-n}}\right) &\equiv \tau_e\left(\left((x_n)^{p^{-n}}\right)^{p^{-(m-n)}}\right)^{p^{m-n}} \pmod{\mathbf{p}^{m-n+1}\mathfrak{R}}. \\ \iff \tau_e\left(x_n^{p^{-n}}\right) &\equiv \tau_e\left(x_n^{p^{-m}}\right)^{p^{m-n}} \pmod{\mathbf{p}^{m-n+1}\mathfrak{R}}. \\ \iff \tau_e\left(x_n^{p^{-n}}\right)\mathbf{p}^n &\equiv \tau_e\left(x_n^{p^{-m}}\right)^{p^{m-n}}\mathbf{p}^n \pmod{\mathbf{p}^{m+1}\mathfrak{R}, \quad \forall 0 \leq n \leq m.} \end{aligned}$$