arXiv:2301.12655v1 [math.AC] 30 Jan 2023

某个有理函数环的自同态

作者：Milo
Moses，2023年1月
31日

目录

1 引言 1 2 一般方法 2 3 $\mathcal{M}_{\mathbb{Q}}$ 8
的自同态 4 $\mathcal{M}_K$、 $K/\mathbb{Q}$ 代数的自同态 14

1 引言

对于任意域 K，定义环 $\mathcal{M}_K$ 如下：

$$\begin{pmatrix} \text{elements: ratios of monic polynomials in } K(x) \\ \text{addition: multiplication of rational functions} \\ \text{multiplication: } [\prod_i (x-\alpha_i)] \cdot \left[\prod_j (x-\beta_j)\right] = \left[\prod_{i,j}(x-\alpha_i\beta_j)\right] \end{pmatrix}$$

这类环自然会出现在向量空间的研究中。向量空间的自同态有相应的特征多项式，而自同态的直和/张量积对应于 $\mathcal{M}_K$中的加法/乘法。我们将在 $\mathcal{M}_K$ 上赋予一种拓扑，其中柯西序列是指首项系数收敛的序列。稍后我们将证明，这使 $\mathcal{M}_K$ 成为一个拓扑环。本文证明的主要定理如下：

定理 1.1. 设 $K/\mathbb{Q}$ 为代数扩张，且 $\phi : \mathcal{M}_K \to \mathcal{M}_K$ 是一个连续环自同态。那么，以下两者之一成立：

1. 存在整数 k、 $s \geq 0$ 和 $\sigma \in$ 伽罗瓦群$(K/\mathbb{Q})$，使得

$$\phi\left(\prod_i (x-\alpha_i)\right) = x^{\sum_i \alpha_i^s - 1} \cdot \prod_i \left(x - \sigma(\alpha_i)^k\right)$$

2. ϕ 的像中的所有有理函数的根都是单位根。如果 $K/\mathbb{Q}$是有限的，那么存在 N，使得所有根都是 N次单位根。

定理 1.1 第 (2) 部分中出现的常数 N 仅在 $K = \mathbb{Q}$ 时有效。在这种情况下，使用证明中的方法，给定（例如） $\phi([x-2])$，便可轻松计算 N。这可以转化为精确的结果，例如 $N <$ （ $\phi([x-2])$ 的根数）$^{1.8}$。 [1]

2 一般方法

本节将建立一些关于 $\mathcal{M}_K$ 的一般结果，其中 K 是任意域。在方便时，我们将专门讨论 $K \subseteq \mathbb{C}$。我们的主要工具将是环同态 $t_k : \mathcal{M}_K \to K$，它们在形如 $[x-\alpha]$ 的元素上定义如下

$$t_k([x-\alpha]) = \alpha^k,$$

并通过线性性扩展到一般元素。注意，我们采用约定 $0^0 = 1$，因此 t_0 是次数映射。这些映射的一个基本性质是，它们可用于计算多项式系数：

定理 2.1（牛顿公式）。对于任意次数为 d 的多项式 $f \in K[x]$ 和 $k \le d$，有

$$ke_k(f) = \sum_{n=1}^{k} (-1)^{n+1} e_{k-n}(f) t_n([f]).$$

这里， $e_n(f)$ 是隐式定义的初等对称多项式系数

$$f(x) = \sum_{n=0}^{d} (-1)^{d-n} e_{d-n}(f) x^n.$$

证明。这些都是经典结果。 □

推论 2.1。如果 K 的特征为零，那么对于任意首一多项式 $f, g \in K[x]$，对于所有 $k < N$， $e_k(f) = e_k(g)$ 当且仅当对于所有 $k < N$， $t_k([f]) = t_k([g])$。

证明。这直接由该定理得出。 □

特别地，我们有 t_k 定义了一个单射

$$\mathcal{M}_K \xhookrightarrow{\prod_{k=0}^{\infty} t_k} \prod_{k=0}^{\infty} K.$$

[1] 这里的结果并未明确证明，但它是我们方法的一个简单推论。常数 1.8 并非最优，而且可以轻易改进为 $1/\ln(2) + \epsilon$

这使我们能够将拓扑定义在 $\mathcal{M}_K$ 上，采用子空间拓扑；$\prod_{k=1}^{\infty} K$ 采用乘积拓扑，而 K 始终采用离散拓扑。显然，在 $\mathcal{M}_K$ 中收敛等价于 t_k 收敛，而这又等价于 e_k 收敛；它们是多项式的首项系数。现在我们将说明 t_k 在何种程度上是仅有的连续环同态 $\mathcal{M}_K \to K$。

引理 2.1. 若 S 是 K^N 的子环，其中 N为某个自然数，则 Hom(S, K)中的非零同态都是先将 S 投影到单个指标，再与某个环同态 $K \to K$复合所得。

证明。我们对 N进行归纳。若 $N = 1$，则 S 是 K的子环。因此，映射 $S \to K$ 必然是先将 S 投影到单个指标，再与某个同态复合所得。此外，根据佐恩引理，每个映射 $S \to K$ 都可以提升为映射 $K \to K$，这是一个标准结论。

在归纳步骤中，假设结论对 $N - 1$成立。固定映射 ϕ : $S \to \mathbb{Z}$。显然，ϕ 不能通过遗忘第一个指标的投影 $L \to L'$分解，当且仅当存在两个元素，它们在第一个指标以外的部分相等，但在经过 ϕ映射后得到不同元素。等价地，这意味着存在一个非零元素 (a_1, 0, 0...)，使得 ϕ 作用于它时不为 0。

如果 ϕ 可通过忘掉第 1 个或第 2 个指标的投影分解，那么归纳假设便给出结论。假设它无法通过忘掉任一指标来分解。这意味着存在元素 (a_1, 0, 0...) 和 (0, a_2, 0...)，在它们作用下 ϕ 不为 0。然而，这些元素相乘为 0。这说明 K 中存在非零元素相乘为 0，这与假设矛盾。证明完毕。

□

命题 2.1. 唯一的连续环同态 ϕ: $\mathcal{M}_K \to K$ 具有 $\sigma \circ t_k$ 的形式，其中 σ : $K \to K$ 是一个环同态。

证明。由于 K 是离散的， ϕ 的核包含 0 的一个开邻域。这些理想

$$I_N = \{r \text{ st } t_k(r) = 0 \ \forall \ k \geq N\}$$

构成 $\mathcal{M}_K$ 在该拓扑下 0 的开邻域基。因此，对于某个 N，有 $I_N \in \ker \phi$。于是，任意连续映射 $\mathcal{M}_K \to K$ 都可通过投影到 $\mathcal{M}_K / I_N$ 分解。这是 K^N 的一个子环，因此由引理 2.1 可得所需结论。

□

这非常强大，因为它使我们能够定义如下内容：

定义 2.1. 对于任意连续自同态 ϕ : $\mathcal{M}_K \to \mathcal{M}_K$，我们将函数 ϕ^* : $\mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ 和 σ^ϕ : $\mathbb{Z}_{\geq 0} \to$ （态射 $K \to K$）定义为满足以下条件的唯一值

$$t_n(\phi(r)) = \sigma_n^\phi(t_{\phi^*(n)}(r))$$

对所有 $r \in \mathcal{M}_K$。

现在我们定义 $\mathcal{M}_K$ 的最重要的自同态:

命题 2.2。对于每个 $n \geq 1$，映射

$$\lambda_n : \mathcal{M}_K \to \mathcal{M}_K$$

将 $\prod_i (x - \alpha_i)$ 映射为 $\prod_i (x - \alpha_i^n)$ 是 $\mathcal{M}_K$ 的连续端同态。对于所有 k、n 和 $\sigma_n^{\lambda_k} = 1$，都有 $\lambda_k^*(n) = kn$。

证明。这是一个直接的计算。 □

下述公式将为我们在整个证明中使用分圆方法奠定基础。

推论 2.2. 若 K 的特征为零，则对任意 $f \in \overline{K}[x]$,

$$x^d f(1/x) = \prod_{n \geq 1} (1 - x^n)^{c_n}$$

其中

$$c_n = \frac{1}{n} \sum_{d|n} \mu(n/d) t_d([f]).$$

这些量 $(1 + x)^z$ 是用牛顿广义二项式定理定义的。

证明。这就是所谓的分圆恒等式，在许多参考文献中都可以找到。

□

令 $\mathcal{M}_{\mathbb{Z}}$ 为由整数系数有理函数构成的 $\mathcal{M}_{\mathbb{Q}}$ 子环。

命题 2.3。对于任意 $r \in \mathcal{M}_{\mathbb{Z}}$ 和 $n \in \mathbb{Z}_{\geq 1}$,

$$\frac{1}{n} \sum_{d|n} \mu(n/d) t_d(r) \in \mathbb{Z}.$$

证明。我们先证明 $r = [f]$、$f \in \mathbb{Z}[x]$ 为首一时的结论，再利用线性性将其推广到一般元素。令 N 为使得 $c_N = \frac{1}{N} \sum_{d|N} \mu(n/d) t_d(r)$不属于 $\mathbb{Z}$的最小数。现在，我们考察等式两边 x^N 的系数

$$x^d f(1/x) = \prod_{n \geq 1} (1 - x^n)^{c_n}.$$

根据假设，左侧的系数是 $\mathbb{Z}$ 的一个元素。右侧的项中，含有 $n > N$ 的项过大，因此没有贡献。根据假设，所有含有 $n < N$ 的项都贡献 $\mathbb{Z}$的一个元素。因此，当且仅当 $\left(1 - x^N\right)^{c_N}$ 中 x^N 的系数属于 $\mathbb{Z}$时，最终结果才是 R 的一个元素。该系数恰好是 $-c_N$，因此 $c_N \in \mathbb{Z}$，这就产生了矛盾。由此得证。

□

继续进行所必需的引理如下：

命题 2.4。设 s_k 是一个复数序列，其具体定义如下：

$$s_k = \sum_j c_j \theta_j^k$$

其中， j 遍历一个有限值集， c_j 为复数， θ_j 位于单位圆上。存在无穷多个 $q \geq 1$ 使得

$$|s_k - s_{k+q}| \leq \frac{4\pi}{q^{1/J}} \sum_i |c_i|$$

对于每个 $k \geq 0$均成立，其中 J 是 j 所遍历的值的数量。对于每个 k_0, s_{k_0} 都是 s_k的极限点。特别地，如果 s_k 收敛，那么它必为常数。要使 s_k 为常数，唯一的可能是除 1 以外的所有根的系数均为零。

证明。首先，不妨设所有 θ_j 均不相同。令 $\theta_j = e^{2\pi i x_j}$。根据狄利克雷同时逼近定理，我们可以找到无穷多个值 q ，使得存在 p_j 满足

$$\left| x_j - \frac{p_j}{q} \right| \leq \frac{1}{q^{1+1/J}}.$$

利用关于 $|x| < 1$的估计 $|e^x - 1| \leq 2x$ ，我们得到

$$|\exp(2\pi i q x_j) - 1| \leq \frac{4\pi}{q^{1/J}}.$$

任取 $k \geq 1$ 并对 j求和，立即得到

$$|s_k - s_{k+q}| \leq \frac{4\pi}{q^{1/J}} \sum_i |c_i| .$$

由于当 q 变大时，它趋于 0，因此显然 s_k 的每个值都必须是极限点。

现在，假设 s_k 是常数。减去常数项的系数后，我们可以假设 $s_k = 0$ 一致。$|s_k|^2$ 的平均值是 $\sum_j |c_j|^2$，因此我们必须对所有 j 都有 $c_j = 0$ ，如所求。 □

有时，下面的结论也很有用：

命题 2.5。若 $r \in \mathcal{M}_{\mathbb{C}}$ 使得 $t_k(r)$ 只取有限多个值，则 r 的所有根都是单位根。

证明。若 r 有任何大于 1 的根，则由命题 2.4 可知， $t_k(r)$ 趋于无穷。因此， r 的所有根的绝对值都必须小于或等于 1。于是我们有

$$r = \prod_i (x - \theta_i)_i^c \cdot r',$$

其中 θ_i 是绝对值为 1 的互不相同的复数，且 r' 的所有根都小于 1。令 $E < 1$ 为 r' 的最大根，我们得到

$$t_k(r) = S_k + O(E^n)$$

其中 $S_k = \sum_i c_i \cdot \theta_i^k$，而 O 表示大 O 记号。选取足够大的 q，使得 $|S_{k+q} - S_k|$ 一致地足够小；根据命题 2.4，这是可行的。于是，我们有

$$t_{k+q}(r) - t_k(r)$$

当 q 变大时，它一致地趋于零，只要 k 足够大。然而，由于 $t_k(r)$ 只取有限多个值，这必然意味着，对于所有足够大的 k， $t_k(r) = t_{k+q}(r)$。特别地， $S_{k+q} - S_k$ 必须以指数级快的速度趋于零。命题 2.4 表明，这意味着 S_k 恒为零。因此，对于所有 q，我们得到 $\theta_i^q = 1$ 。

现在，考虑 r 中小于 1 的根。由于 S_k 是周期的，我们必然有：较小根的 t_k 只能取有限多个值。然而，较小根的 t_k 也趋于零。若要只取有限多个值且趋于零，唯一的可能是对于所有足够大的根， t_k 为零。对于足够大的根而言，要使其为零，唯一的可能就是不存在绝对值小于 1 的根；理由与上文相同。 □

上述工作促使我们给出以下定义：

命题 2.6。元素 $r \in \mathcal{M}_{\mathbb{Z}}$ 满足以下条件且彼此等价：

1. $r = [f/g]$，其中 f 和 g 的根的绝对值均为 1 或 0 2. $r = [f/g]$，其中 f 和 g 的根的绝对值均为 ≤ 1 3. 对所有 $\epsilon > 0$， $\lim_{k\to\infty} t_k(r)/(1+\epsilon)^k = 0$ 4. $r = c_0[x] + \sum_{n\geq 1} c_n [1 - x^{-n}]$，其中 $c_n \in \mathbb{Z}$ 是常数，且其中仅有限多个非零

具有这些等价性质中任意（或全部）一项的元素构成的子环 $r \in \mathcal{M}_{\mathbb{Z}}$ $\mathcal{M}_{\mathbb{Z},\Phi}$。

证明。我们首先证明 $2 \implies 1$。为此，我们注意到 f 的最小非零系数等于它的非零根之积。这个乘积必定是一个非零整数；由于所有根都不大于 1，因此它们的绝对值必定都等于 1。

现在我们证明 $3 \implies 2$。令 C 为 r 最大根的绝对值。若 $C \leq 1$，则证毕。若 $C > 1$，写作

$$t_n(r) = S_n \cdot C^n + O(E^n)$$

，其中 $S_n = \sum_i c_i \cdot \theta_i^n$、$|\theta_i| = 1$ 和 $E < C$。于是，

$$S_n = \frac{t_n(r)}{C^n} + O((E/C)^n),$$

因此 $S_n \to 0$。故 S_n 满足引理 2.4 的条件，因此是零常数。这与至少有一个根的绝对值为 C 这一事实矛盾，因为否则该和就不是非零的。

现在我们证明 $4 \implies 3$。为此，我们注意到

$$t_k\left(c_0[x] + \sum_{n \geq 1} c_n \left[1 - x^{-n}\right]\right)$$

是周期的，因此除以任意大的数后趋于零。

最后我们证明 $1 \implies 4$。我们对 $\deg(f) + \deg(g)$ 作归纳。若 $\deg(f) \geq 1$ 的根为 ζ，则 ζ 是一个代数数，其所有伽罗瓦共轭的绝对值也都为 1，因此根据克罗内克经典定理，它必定是次数为 n 的本原单位根，$\zeta = \zeta_n$。因此，$\Phi_n(x) | \deg(f)$，其中 Φ_n 是第 n 个分圆多项式，因此

$$[f/g] = [(f/\Phi_n(x))/g] + \sum_{d|n} \mu(n/d)\left[x^d - 1\right].$$

继续进行，直到 f 和 g 的所有根都为零，即可得证。 □

我们将 $\mathcal{M}_K$ 定义为 $\mathcal{M}_K$的拓扑完备化。

命题 2.7。子环$\mathcal{M}_{\mathbb{Z},\Phi}$ 在 $\mathcal{M}_{\mathbb{Z}}$中稠密。每个元素 $r \in \mathcal{M}_{\mathbb{Z},\Phi} = \mathcal{M}_{\mathbb{Z}}$ 都可以唯一地写成如下形式

$$r = c_0[x] + \sum_{n \geq 1} c_n \left[1 - x^{-n}\right],$$

对于任意 c_n。此外，对于 $k \in \mathbb{Z}_{\geq 1}$

$$t_k(r) = \sum_{d|k} c_d$$

以及 $t_0(r) = c_0$。

证明。首先，我们证明每个形如 $r = c_0[x]+\sum_{n\geq 1} c_n \widehat{[1-x^{-n}]}$ 的元素都属于 $\mathcal{M}_{\mathbb{Z},\ \Phi}$。这由以下事实可知

$$r = \lim_{N\to\infty} \left(c_0[x] + \sum_{n=1}^{N} c_n \left[1 - x^{-n}\right] \right),$$

根据命题 2.6 第 3 部分，极限中的每一项都属于 $\mathcal{M}_{\mathbb{Z},\Phi}$。接下来，我们证明这些和满足所述 t_k 公式。具体来说，我们先验证

$$\begin{aligned} t_k\left([x^n - 1]\right) &= \sum_{j=0}^{n-1} e^{2\pi ji/k} \\ &= \begin{cases} n & n|k \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

因此，两边除以 x^n 后，我们得到 $t_k\left([1-x^{-n}]\right)$ 的相同公式，只是其中在 0 处没有贡献。利用线性性扩展，即得该公式。根据莫比乌斯反演，唯一性得证。

对于命题的最后一部分，我们验证每个元素 $\widehat{\mathcal{M}_{\mathbb{Z}}}$ 确实都能写成这种形式。设 r_N 是 $\mathcal{M}_{\mathbb{Z}}$ 中的一个序列，且 r 是其一个极限点。令

$$c_n = \lim_{N\to\infty} \frac{1}{n} \sum_{d|n} \mu(n/d) t_d(r_N),$$

由于 t_k 连续，该式收敛。此外， $c_n \in \mathbb{Z}$，因为根据命题 2.3，它们在极限的每一步都成立。现在显然，由莫比乌斯反演可得 $r = c_0[x] + \sum_{n\geq 1} c_n[1-x^{-n}]$。 □

现在我们证明 $\mathcal{M}_{\mathbb{Z},\Phi}$ 上一个重要的乘法公式：

命题 2.8. 对任意 n、m，均有

$$[x^n - 1]\,[x^m - 1] = \gcd(n,m)\left[x^{\mathrm{lcm}(n,m)} - 1\right]$$

证明. 这是一个简单的计算，可直接由 $\mathcal{M}_{\mathbb{Z}}$ 中乘法的定义得出。 □

3 $\mathcal{M}_{\mathbb{Q}}$ 的端同态

本节中，我们研究自同态环 $(\mathcal{M}_{\mathbb{Q}})$。一个自然的起点是研究较小定义域 $\mathcal{M}_{\mathbb{Z},\ \Phi}$ 上的映射：

命题 3.1. 如果 $\phi \in \mathcal{M}_{\mathbb{Z},\ \Phi} \to \mathcal{M}_{\mathbb{C}}$ 连续，那么对于所有有理素数幂 p^α，我们有

$$\phi\left(\left[x^{p^\alpha}-1\right]\right) = s_{-\infty}[x] + \sum_{\beta=0}^{\alpha} s_\beta \cdot p^{\alpha-\beta} \cdot \left[x^{p^\beta}-1\right],$$

其中 $s_\beta \in \{-1,0,1\}$。

证明。由于 $t_k(\phi(r))$ 必须取有限个值，命题 2.5 告诉我们，$\phi(r)$ 属于 $\mathcal{M}_{\mathbb{Z},\ \Phi}$。设 $r = \phi\left(\left[x^{p^\alpha}-1\right]\right)$，并令 $c_n = \frac{1}{n}\sum_{d|n}\mu(n/d)t_d(r)$。取 N使得 $c_N \neq 0$。写作 $N = p^\gamma N'$，其中 p不能整除 N'。我们首先证明 $\gamma \leq \alpha$。具体来说，我们计算

$$\begin{aligned} p^\gamma N' \leq p^\gamma N'|c_N| &= \left|\sum_{d|p^\gamma N'} \mu(p^\gamma N'/d)t_d(r)\right| \\ &= \left|\sum_{d|N'} \mu(N'/d)\left(t_{p^\gamma d}(r) - t_{p^{\gamma-1}d}(r)\right)\right| \\ &\leq \sum_{d|N'} p^\alpha \leq p^\alpha N'. \end{aligned}$$

因此，$\gamma \leq \alpha$，如所求。注意，在 $\gamma = 0$ 的情形下，所写的公式并不完全正确（也就是说，不存在 $p^{\gamma-1}d$ 修正项），但由于 $\alpha \geq 1$，我们的命题在这种情形下事后仍然成立。现在，Nc_N 是 p^α 的倍数。特别地，c_N 必须是 $p^{\alpha-\gamma}$ 的倍数。我们用这一点来界定 N'。具体来说，根据前面的结果，我们有不等式

$$p^\gamma N'|c_N| \leq \sum_{d|N'} p^\alpha.$$

鉴于 $|c_N| \geq p^{\alpha-\gamma}$，当且仅当 $c_N = \pm p^{\alpha-\gamma}$ 且$N' = \sum_{d|N'} 1$时等号成立。这意味着 $N' = 1$或 $N' = 2$。

现在证明 $N' = 2$ 是不可能的。设 γ为满足 $c_{2p^\gamma} \neq 0$的最小值（如果存在）。那么，

$$\begin{aligned} t_{2p^\gamma} &= \sum_{d|2p^\gamma} dc_d \\ &= \sum_{d|p^\gamma} dc_d + 2p^\gamma c_{2p^\gamma} \\ &= t_{p^\gamma} \pm 2p^\alpha. \end{aligned}$$

由于 t_{p^γ} 和 t_{2p^γ} 均等于 0 或 p^α，这是不可能的。因此，对于所有 γ，$c_{2p^\gamma} = 0$。这就是所需的结果。 □

研究端同态时，一个重要的元素是 $[x]$。我们将它可能到达的位置分类如下：

命题 3.2. 对所有 $\phi \in$ 自同态环 $(\mathcal{M}_{\mathbb{Q}})$，$\phi([x])$ 必为以下之一：$[x]$、0、$[x-1]$ 或 $[(x-1)/x]$。

证明. 与之前一样，$t_k([x])$ 只取 0 或 1。如果 $\phi([x]) = c_0[x] + \sum_{n=1}^{\infty} c_n [x^n - 1]$，那么

$$|nc_n| = \left| \sum_{d|n} \mu(n/d) t_d(\phi([x])) \right| \leq \sum_{d|n} 1$$

因此，如果 $c_n \neq 0$，那么 $n \in \{0, 1, 2\}$。此外，在这些情况下，我们必有$c_n = 1$ 在这些情况下。考察有限种可能性，即可得到所需结果 □

情形 $\phi([x]) = [x-1]$ 或 $\phi([x]) = [(x-1)/x]$ 很容易处理：

命题 3.3. 自同态环 $(\mathcal{M}_{\mathbb{Q}})$ 中一个自同态的以下性质彼此等价：

1. $\forall\ k \geq 1,\ \phi^*(k) = 0$
2. $\exists\ k \geq 1\ s.t\ \phi^*(k) = 0$
3. $\phi([x]) = [x-1]\ or\ [(x-1)/x]$
4. $\exists\ k\ s.t\ \phi(r) = t_0(r)[x-1] + (t_k(r) - t_0(r))[x]\ \forall\ r \in \mathcal{M}_{\mathbb{Q}}$

证明。

(1) $\Longrightarrow$ (2)。显然。(2) $\Longrightarrow$ (3)。令 $k \geq 1$ 为满足 $\phi^*(k) = 0$的值。那么，$t_k(\phi([x])) = t_{\phi^*(k)}([x]) = 1$。因此，$\phi([x])$不可能为 0 或 $[x]$，故由命题 3.2 可得结论。

(3) $\Longrightarrow$ (4)。若 $\phi([x]) = [(x-1)/x]$，则

$$\begin{aligned} \phi([x]r) &= \phi(t_0(r)[x]) \\ &= t_0(r)[(x-1)/x] = t_0(r)[x-1] - t_0(r)[x] \\ &= \phi(r)[(x-1)/x] = \phi(r) - t_0(\phi(r))[x] \end{aligned}$$

因此整理可得

$$\phi(r) = t_0(r)[x-1] + \left(t_{\phi^*(0)}(r) - t_0(r)\right)[x].$$

当 $\phi([x]) = [x-1]$时，我们也可类似地进行。

(4) $\Longrightarrow$ (1)。通过繁琐但缺乏启发性的计算可知，任何具有 (4) 中形式的 $\phi \in$ 自同态环 $(\mathcal{M}_{\mathbb{Q}})$ 都是一个自同态。对于任意 $j \geq 1$,

$$t_j\left(t_0(r)[x-1]+\left(t_{\phi^*(0)}(r)-t_0(r)\right)[x]\right)=t_0(r)$$

因此 $\phi^*(j)=0$，从而可推出 (1)。综合这些推论，即得所需结果。

□

现在我们来分析剩下的情形，$\phi^*(1)\neq 0$。首先要更仔细地研究 ϕ^* 的行为。

引理 3.1. 如果 $\phi\in$ 自同态环$(\mathcal{M}_{\mathbb{Q}})$满足 $\phi^*(1)\neq 0$，那么 $v_p(\phi^*(k))$仅取决于$v_p(k)$。

证明。由命题 3.3，$\phi^*(1)\neq 0$ 蕴含 $\phi^*(k)\neq 0$ 对所有 k 都成立，因此$v_p(\phi^*(k))$都定义良好。由引理 3.1 给出的分类可知，$t_k(\phi([x^{p^\alpha}-1]))$仅取决于 $v_p(k)$。反过来，随着 α变化，$t_k(\phi([x^{p^\alpha}-1]))$决定了 $v_p(\phi^*(k))$，因此结论得证。

□

命题 3.4. 如果 $\phi^*(1)\neq 0$，则 $\phi^*(n)/\phi^*(1)$是乘法的，并且将 p 的幂映为 p的幂。

证明。若 n 是 p的幂，则对所有 $q\neq 0$，$v_q(n)=v_q(n)$，因此对所有 $q\neq p$，$v_q(\phi^*(n))=v_q(\phi^*(1))$，从而 $\phi^*(n)/\phi^*(1)$ 是 p的幂。因此，一般而言，

$$\begin{aligned}\phi^*(n)&=\prod_p p^{v_p(\phi^*(n))}\\&=\prod_{p^\alpha||n} p^{v_p(\phi^*(p^\alpha))}\cdot\prod_{\substack{p^\alpha||\phi^*(1)\\ p\nmid n}} p^\alpha\\&=\phi^*(1)\cdot\prod_{p^\alpha||n} p^{v_p(\phi^*(p^\alpha))-v_p(\phi^*(1))}\end{aligned}$$

因此，$\phi^*(n)/\phi^*(1)$ 是乘法的。

□

引理 3.2。设 $\phi^*(1)\neq 0$，且对某个 $k\geq 2$，$\phi([x-k])$ 有一个绝对值大于 1 的根。那么，

$$\limsup_{N\to\infty}\frac{\phi^*(n)}{n}$$

是一个非零有理数。

证明。设 C 为 $r=\phi([x-k])$ 的最大根的绝对值。根据假设，$C>1$。令 $E<C$ 为 $\phi([x-k])$ 的第二大根的绝对值，我们得到

$$\begin{aligned}k^{\phi^*(n)}&=t_{\phi^*(n)}\left([x-k]\right)\\&=t_n\left(r\right)\\&=S_n\cdot C^n+O\left(E^n\right),\end{aligned}$$

其中 $S_n = \sum_j c_j \theta_j^n$、 $c_j \in \mathbb{Z} \neq 0$ 和 $|\theta_j| = 1$ 互不相同。如果对于某个 N， S_N 为负数或复数，那么根据引理 2.4， S_N 将是 S_n 的一个极限点。这与事实矛盾，因为那样一来，对于某个 n， $k^{\phi^*(n)}$ 就会是负数或复数。因此我们可以取对数，得到

$$\phi^*(n) = \log(C)n + \log(S_n + O((E/C)^n)).$$

这里，log 表示以 k 为底的对数。众所周知，

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n<N} |S_n|^2 = \sum_j |c_j|^2.$$

因此，对于正比例的 n ，有 $S_n \geq 1$ ，因为 S_n 有上界。特别地，我们得到

$$\limsup_{n\to\infty} \frac{\phi^*(n)}{n} = \log(C) > 0.$$

选取 $N \geq 1$ 使得 $S_N \neq 0$。选取足够大的 q ，使得

$$|S_n - S_{n+q}| \ll \frac{1}{q^{1/J}},$$

其中 $J \geq 1$ 是一个固定整数。根据引理 2.4，这样的 q 有无穷多个。对 $m \ll q^{1/J}$ 一致地，我们得到

$$\begin{aligned}
&|\phi^*(N+mq) - \log(C)\cdot mq| \\
\ll_N &|\phi^*(N+mq) - \log(C)\cdot(N+mq) + \log(S_{N+mq})| \\
&+ |\log(S_{N+mq}) - \log(S_N)| \\
\ll_N &1.
\end{aligned}$$

现在我们进行变形，得到当 $N^2 m < q^{1/J}$ 时，

$$\begin{aligned}
&\frac{1}{\phi^*(N)} \left|\phi^*(N + (N^2m)q) - \log(C)\cdot(N^2m)q\right| \\
&= \left|\frac{\phi^*(1+m(Nq))}{\phi^*(1)} - \frac{N\log(C)}{\phi^*(N)}\cdot m(Nq)\right| \\
&\ll_N 1.
\end{aligned}$$

现在，我们观察到如下事实。根据命题 3.4， $\phi^*(p^a)/\phi^*(1)$ 对每个素数 p 和 $a \geq 1$ 都是 p 的幂。若 $\phi^*(p^a)/\phi^*(1) \geq p^{a+1}$，则 $\phi^*(p^a)/p^a \geq \phi^*(1)p$。由于 $\phi^*(n) \leq \log(C)n + O(1)$，这只可能对有限多个 p 成立。特别地，令 m 为所有满足对某个 $a \geq 1$ 有 $\phi^*(p^a)/\phi^*(1) \geq p^{a+1}$ 的素数之积。于是， $1 + m(Nq)$ 与这些素数都互素，因此

$$\frac{\phi^*(1+m(Nq))}{\phi^*(1)(1+m(Nq))}$$

将是一个整数的倒数。因此，由于

$$\left|\frac{\phi^*(1+m(Nq))}{\phi^*(1)(1+m(Nq))} - \frac{N\log(C)}{\phi^*(N)}\right| \ll_N \frac{1}{q}$$

当 q 足够大时， ${}^{N_{\log(C)\,\phi^*(N)}}$ 可以任意精确地用整数的倒数逼近。鉴于整数倒数组成的集合是离散的，这意味着 ${}^{N_{\log(C)\ \phi^*(N)}}$ 本身就是一个整数的倒数。特别地，log(~~(C) 是有~~理数，因此我们得到了所需结果。

□

引理 3.3. 用引理 3.2 的表述来说， $S_n = 1$ 对所有 n 均成立。

证明。根据引理 3.2 的讨论， $S_n \geq \sqrt{\sum_j |c_j|^2}$ 对比例为正的 n 成立。假设 $\sum_j |c_j|^2 = 1$。那么显然， $S_n = \theta^n$ 仅对单个值 θ 成立。为了使 S_n 对每个 n 都是正实数，我们必须有 $\theta = 1$。这就得到了所需结果。

另一种情况是 $\sum_j |c_j|^2 \neq 1$。此时我们得到，$S_n \geq \sqrt{2}$ 对比例为正的 n 成立。对于这些值，我们有

$$\phi^*(n) = \log(C)n + \log(S_n) + O((E/C)^n).$$

令 D 为 log(C) 的分母，根据引理 3.2，该分母存在。我们有

$$D\phi^*(n) = D\log(C)n + D\log(S_n) + O((E/C)^n).$$

由于 $S_n \geq \sqrt{2}$, Dlog(S_n) 与零之间有正的距离。因此，

$$D\phi^*(n) = D\log(C)n + O(1),$$

其中 O(1) 是一个大小有界的非零整数。根据命题 3.4，任何整除 $\phi^*(n)$ 的素数，要么整除 ϕ^*(1)，要么整除 n。如果一个素数同时整除 $\phi^*(n)$ 和 n，它也必定整除 O(1)，因此其大小有界。由此可知，存在 $B > 0$，使得对于所有 n， $\phi^*(n)$ 都是 B-光滑数。 B-光滑数在自然数中的比例为零。特别地， $n/\log(C)$ 总是与某个 B-光滑数相距有界，因此它只能遍历自然数中比例为零的集合。然而，我们假设 n 遍历的是一个具有正密度的集合。这就产生了矛盾。因此，对于所有 n， $S_n = 1$，证毕。

□

命题 3.5. 若对于某个 $k \geq 2$， $\phi([x-k])$ 有一个绝对值大于 1 的根，且 $\phi^*(1) \neq 0$ and $\phi = \lambda_{\phi^*(1)} + (t_{\phi^*(0)} - t_0)[x]$。

证明. 用引理 3.2 和 3.3 的表述来说，我们有

$$\phi^*(n) = \log(C)n + O((E/C)^n).$$

鉴于 $\phi^*(n)$ 和 $\log(C)n$ 是有理数，这意味着当 n足够大时， $\phi^*(n) = \log(C)n$。根据 $\phi^*(n)/\phi^*(1)$ 的乘法性，这意味着 $\log(C) = \phi^*(1)$，因此当 n足够大时， $\phi^*(n) = \phi^*(1)n$。再次根据 $\phi^*(n)/\phi^*(1)$ 的乘法性，这意味着对所有 $n \geq 1$， $\phi^*(n) = \phi^*(1)n$。引入 $\phi^*(0) = 0$，从而对所有 $n \geq 1$， $\phi^*(n) = \phi^*(1)n$。

显然，对所有 $n \geq 0$， $\lambda^*_{\phi^*(1)}(n) = \phi^*(1)n$。引入 $t_{\phi^*(0)} - t_0$以获得 $\phi^*(0)$ 的正确值，由此完成证明。 □

引理 3.4. 若 $\phi^*(1) \neq 0$，且对于某个 $k \geq 2$， $\phi([x-k])$ 的所有根的绝对值都小于或等于 1，则对于除有限多个 n 之外的所有 n，都有 $\phi([1-x^{-n}]) = 0$。

证明。我们发现 $t_k(\phi([x-k]))$ 有界。由于它是整数，因此它只取有限多个值。由此， $\phi^*(k)$ 也只取有限多个值。因此，根据命题 3.3，对于除有限多个N之外的所有 $k \geq 1$，都有 $N \nmid \phi^*(k)$。对于这些 N，我们发现对所有$k \geq 1$， $t_k(\phi([x^N - 1]))$ 都为零。因此，必有对于除有限多个 N 之外的所有 N， $\phi([x^N - 1]) = N[x]$，从而得证。 □

定理 3.1. 若 $\phi \in$ 自同态环$(\mathcal{M}_{\mathbb{Q}})$，则要么对某些 k、 j， $\phi = \lambda_k + (t_j - t_0)$，要么对于除有限多个 n 外的所有 n， $\phi([1-x^{-n}]) = 0$。

证明。若 $\phi^*(1) = 0$，则根据命题 2.7 中 (2) $\iff$ (3) 的等价性， $\phi([1-x^{-n}]) = 0$ 对除有限多个 n 外的所有 n 都成立。由于每个 $r \in \mathcal{M}_{\mathbb{Q}}$ 都可以根据命题 [ref], 写成形如 $[1-x^{-n}]$ 的元素之无限和，这意味着 $\phi(r)$ 将是一个 N次单位根，其中 N 是满足 $\phi([1-x^{-n}])$ 非零的那些 n 的最小公倍数。

或者，假设 $\phi^*(1) \neq 0$。若 $\phi([x-2]) \in \mathcal{M}_{\mathbb{Z},\,\Phi}$，则根据引理 3.4， $\phi([1-x^{-n}]) = 0$ 对除有限多个 n 外的所有 n 都成立，因此我们可以通过上述论证得出结论。否则，根据引理 3.5， ϕ 具有所需的形式。 □

4 $\mathcal{M}_K$、 $K/\mathbb{Q}$ 代数上的自同态

设 ϕ： $\mathcal{M}_K \to \mathcal{M}_K$ 是一个连续环自同态。根据命题 2.1，对于每个 n，都存在 $\sigma_n^\phi \in$ 伽罗瓦群$(K/\mathbb{Q})$ 和 $\phi^*(n) \in \mathbb{Z}_{\geq 0}$，使得 $t_n \circ \phi = \sigma_n^\phi \circ t_{\phi^*(n)}$。特别地，对每个 n， t_n 为有理数这一性质在 ϕ 下保持不变，因此根据牛顿公式，具有有理系数这一性质也随之保持不变。

因此， ϕ 限制为映射 $\mathcal{M}_{\mathbb{Q}} \to \mathcal{M}_{\mathbb{Q}}$。定理 3.1 表明，$\phi^*(k)$要么关于 k一致有界，要么对于 $k \geq 1$，它是形如 $\phi^*(1)k$的线性函数。现在我们分别讨论这两种情况：

命题 4.1。设 ϕ： $\mathcal{M}_K \to \mathcal{M}_K$ 是一个连续环自同态，并且 $\phi^*(k)$有界。那么， ϕ 的像中所有元素的根都是单位根。如果 $K/\mathbb{Q}$ 是有限的，那么所有根都是对于某个固定的 N 而言的 N次根。

证明。首先，选择 $r \in \mathcal{M}_K$。然后， $t_k(\phi(r)) = \sigma_k(t_{\phi^*(k)}(r))$ 只取有限多个值，因为 $t_{\phi^*(k)}(r)$ 只取有限多个值，而伽罗瓦群 $\mathrm{Gal}(K/\mathbb{Q})$ 可以将这些值映射到它们的伽罗瓦共轭（有限多个）中的某个子集。由命题 2.5 可知， $\phi(r)$ 的所有根都是单位根。

假设 $K/\mathbb{Q}$ 是有限的。那么， $t_k(\phi(r))$ 只取有限多个值；当 r 变化时，这个有限数量现在是统一有界的。假设不存在这样的 N，使得每个 $\phi(r)$ 都模 N 周期的。那么，通过对这些值取加权线性组合，我们可以构造出一些元素 r，使得 $\phi(r)$ 取任意多个值。这就产生了矛盾，因此，对于某个统一的周期 N， $\phi(r)$ 模 N 是周期的。

现在我们证明， r 模 N 周期意味着它的所有非零根都是 N 次单位根，由此便可推出我们的结论。写作 $t_k(r) = \sum_i c_i \alpha_i^k$。由于它模 N 是周期的，我们得到

$$\sum_i c_i \alpha_i^{k_0} \left(\alpha_i^N\right)^k$$

对于每个 k_0，它关于 k 都是常数。因此，我们得到

$$\sum_{\alpha_i^N = \alpha} c_i \alpha_i^{k_0} = 0$$

对所有 $\alpha \neq 1$都成立。因此，再由命题 2.5 可得，当$\alpha_i^N \neq 1$时， $c_i = 0$。特别地，所有 α_i 都是 N次单位根，因此结论得证。 □

引理 4.1. 设 $\alpha \in \overline{\mathbb{Q}}$ 为一个代数数。对于所有充分大的整数N， $\alpha' = N\alpha + 1$ 的任意两个伽罗瓦共轭之比都不是单位根。

证明. 假设存在无穷多个 N，使得对于某个自同构 σ， $N\alpha+1$ 与 $N\sigma(\alpha)+1$之比是单位根。于是存在一个无穷序列 $\frac{\alpha+1/N}{\sigma(\alpha)+1/N}$，其元素均为单位根。这些元素在 $\mathbb{Q}$上的代数次数都有界，因此它们必定全是某个J次单位根。 J次单位根的集合是离散的，因此不可能存在由 J次单位根构成的非恒定收敛序列。由此得到矛盾，所需结论得证。

□

命题 4.2。设 ϕ： $\mathcal{M}_K \to \mathcal{M}_{\mathbb{C}}$ 是一个连续环自同态，满足对所有 $n \geq 1$， $\phi^*(n) = \phi^*(1)n$。那么，对所有 $n \geq 1$， $\sigma_n^\phi = \sigma_1^\phi$。

证明。取 $\alpha \in K$。我们希望证明 $\sigma_n^\phi(\alpha) = \sigma_1^\phi(\alpha)$。由命题 4.1，不失一般性，可以假设 α 的伽罗瓦共轭之间的比值都不是单位根。考察 $\phi([x-\alpha])$ 的像，可得

$$\sigma_n^\phi(\alpha)^{\phi^*(1)n} = t_n(\phi([x-\alpha])) = S_n \cdot C^n + O(E^n),$$

其中 C 是实数， $E < C$，而 $S_n = \sum_i c_i \cdot \theta_i^n$ 是单位圆上复数的加权和。取绝对值并取对数，可得对满足 $|S_n| \geq 6/5$ 的所有 n，均有

$$\log|\sigma_n^\phi(\alpha)| \cdot \phi^*(1)n = \log(C) \cdot n + \log|S_n| + O((E/C)^n).$$

取比值，得到

$$\log|\sigma_n^\phi(\alpha)| = \frac{\log(C)}{\phi^*(1)} + \frac{\log|S_n|}{\phi^*(1)n} + O((E/C)^n).$$

鉴于当 n 变化时， $\sigma_n^\phi(\alpha)$只取有限多个值，若要使其能被$\log(C)/\phi^*(1)$任意精确地逼近，唯一的可能就是当 n足够大时，$\log|\sigma_n^\phi(\alpha)| = \cancel{\log(C)}\,\phi^*(1)$。因此，对于足够大的 n 且满足 $|S_n| \geq 6/5$，我们有

$$\frac{\log|S_n|}{\phi^*(1)n} = O((E/C)^n).$$

鉴于$\log|S_n|$ 与0保持一定距离，这种情况只会在有限多个 n时发生。因此，只有有限多个 n满足 $|S_n| \geq 6/5$。因此，

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} |S_n|^2 = \sum_i |c_i|^2 \leq (6/5)^2 < 2.$$

鉴于 $|c_i|$ 是整数，要使 $\sum_i |c_i|^2$ 小于2，就必须存在某个 i使得$c_i = 1$ 成立，并且对所有其他 i， $c_i = 0$ 成立。因此，存在某个 $|\theta| = 1$使得 $S_n = \theta^n$ 成立。特别地，我们得到

$$\sigma_n^\phi(\alpha)^{\phi^*(1)n} = (\theta C)^n + O(E^n)$$

对于所有足够大的 n都成立。因此，

$$\sigma_n^\phi(\alpha)^{\phi^*(1)n} = (\theta C)^n$$

对于所有 $n \geq 1$都成立。因此，

$$\left(\frac{\sigma_n^\phi(\alpha)}{\sigma_1^\phi(\alpha)}\right)^{\phi^*(1)n} = 1$$

对所有 $n \geq 1$ 均成立。根据我们对 α 的假设，因此可得 $\sigma_n^\phi(\alpha) = \sigma_1^\phi(\alpha)$。由此得到所需的结论。 □

综合这两种情况，即得所需结果。