# 大作业: Wedderburn 小定理之证明

张陈成 519071910019

## 定理简述

Wedderburn小定理可叙述如是: 有限整环必为域.

以循环群之角度视之, 有限整环必为除环. 有限整环之交换性可通过Jacobson定理直接导出. Jacobson定理表明一切满足

$$\forall x \in R, \exists n(x) \in \mathbb{N} \text{ s.t. } x^{n(x)+2} = x$$

之环为交换环. 倘若$n(x)$与$x$无关, 可通过Birkhoff完备性理论证明Jacobson定理(见此处论文). 本文大体转录E. Witt之经典方法乏善可陈, 是故笔者对证明所涉及的Möbius反演定理加以深入.

## 证明

不妨设$K$为有限体, 记$C(K) := \{x : xy = yx (\forall y \in K)\}$为其中心, $q = |C(K)|$. 由于

$$\pi : K \to K/C(K), x \mapsto x + C(K)$$

诱导出商环上的同态, 故可视$K$为$C(K)$上之向量空间. 记$n := \dim_{C(K)} K$为其维数, 下证明$n = 1$.

记$N(x) := \{y \in K : xy = yx\}$. 易见$N(x)$为体, 从而为$C(K)$上之向量空间, 记$n(x) := \dim_{C(K)} N(x)$. 视诸乘法群角度有$N(x)^* \leq K^*$, 故$(q^{n(x)} - 1) \mid (q^n - 1)$. 由关系

$$q^l - 1 \equiv q^{l+p} - 1 \mod (q^p - 1)$$

可知$n(x) \mid n$.

讲$K^*$中元素划分为共轭类, $x$共轭元之数量为$\dfrac{|K^*|}{|N(x)^*|} = \dfrac{q^n - 1}{q^{n(x)} - 1}$. 据中心公式有

$$q^n - 1 = q - 1 + \sum_{x \in R} \frac{q^n - 1}{q^{n(x)} - 1}.$$

其中$R$为某一代表元系之集.

若$n \neq 1$, 下引入分圆多项式

$$
\begin{aligned}
\Phi_r(x) :=& \prod_{1 \le d \le r, \gcd(d,r)=1} (x - e^{2\pi i d/r}) \\
=& (x^r - 1) \prod_{k \ge 1} \left[ \prod_{\substack{p_1 \cdots p_k | r \\ p_1, \cdots, p_k \\ \text{为互不相同之素数(若存在)}}} (x^{r/(p_1 \cdots p_k)} - 1) \right]^{-1} \\
=& \prod_{d|r} (x^d - 1)^{\mu(r/d)}.
\end{aligned}
$$

其中$\mu(m) = 0$若且仅若$m$有素数平方因子, $\mu(m) = (-1)^{k(m)}$若且仅若$m$无素数平方因子且素因数个数为$k(m)$. 最末二行变换可通过容斥原理证明: 其实质乃Möbius反演定理(证明见文末).

注意到对任意$d \mid n$, $\Phi_n(x)$之零点为$x^n - 1 = 0$之根, 同时并非$x^d - 1 = 0$之根. 因此$\Phi_n(q) \mid \dfrac{q^n - 1}{q^{n(x)} - 1}$. 从而$\Phi_n(q) \mid q - 1$. 注意到

$$
|\Phi_n(q)| = \prod_{1 \le d \le r, \gcd(d,r)=1} |q - e^{2\pi i d/r}| \ge |q - 1|^{\varphi(q)} > q - 1
$$

矛盾, 从而$n = 1$.

## Möbius反演公式

Möbius变换建立在局部有限的偏序集$(P, \le)$上. 其中, 局部有限是谓

$$
\forall x, y \in P, |\{z : x \le z \le y\}| < \infty.
$$

今考虑$I(\mathbb{Q})$为一切映射$f : \{(x, y) : x \le y\} \to \mathbb{Q}, (x, y) \mapsto f(x, y)$之集合, 构造环$(I, +, *)$如下

1. 对于加法, $(f + g)(x, y) := f(x, y) + g(x, y)$恒成立.
2. 不妨设$x \le y$, 则对于乘法(卷积)有$(f * g)(x, y) := \sum_{x \le z \le y} f(x, z) g(z, y)$.
3. 单位元即Kronecker映射$\delta(x, y) := \delta_{x,y} = \begin{cases} 1 & x = y, \\ 0 & x < y. \end{cases}$.

定义Möbius逆函数$\mu^{-1}(x, y) \equiv 1, \forall x \le y$. 下先说明映射$\mu^{-1}$之可逆性.

一般地, 有结论$U(I)=\{f:f(x,x)\neq 0,\forall x\in P\}$. 由于$\{f:f(x,x)\neq 0,\forall x\in P\}$构成半群, 下仅需证明对任意$x\in P$, $f(x,x)$恒非零与$f$左可逆等价(考虑乘法群之单边定义).

若存在$g=f_l^{-1}$, 则$g(x,x)*f(x,x)=\delta(x,x)\implies g(x,x)=[f(x,x)]^{-1}$. 对任意$x\leq y$且$x\neq y$之序对$(x,y)$有

$$0=\delta(x,y)=g(x,y)*f(x,y)=\sum_{x\leq z\leq y}g(x,z)f(z,y).$$

从而$g(x,y)f(y,y)=-\sum_{x\leq z<y}g(x,z)f(z,y)$. 由此可得唯一确定的$g$. 职是之故, 可作$I$之单位集$\{f:f(x,x)\neq 0,\forall x\in P\}$. Möbius函数及其逆函数存在. 特别地, 展开
$\mu^{-1}*\mu=\mu*\mu^{-1}=\delta$有

$$\delta(x,y)=\sum_{x\leq z\leq y}\mu(x,z)=\sum_{x\leq z\leq y}\mu(z,y).$$

下给出Möbius反演定理: 对任意$x\in P$ s.t. $|\{y\in P:y\leq x\}|$有限, 则对$f,g\in I(A)$,

$$g(x)\equiv\sum_{y\leq x}f(y)\iff f(x)\equiv\sum_{y\leq x}g(y)\mu(y,x).$$

其中$(A,\cdot)$为任意乘法Abel群.

**证明:** 注意到左式导出

$$\begin{aligned}\sum_{y\leq x}g(y)\mu(y,x)\equiv&\sum_{z\leq y\leq x}f(z)\mu(y,x)\\ \equiv&\sum_{z\leq x}\left(\sum_{z\leq y\leq x}\mu(y,x)\right)f(z)\\ \equiv&\sum_{z\leq x}\delta(z,x)f(z)\\ \equiv&f(x).\end{aligned}$$

右式导出

$$\begin{aligned}\sum_{y\leq x}f(y)\equiv&\sum_{z\leq y\leq x}g(z)\mu(z,y)\\ \equiv&\sum_{z\leq x}\left(\sum_{z\leq y\leq x}\mu(z,y)\right)g(z)\\ \equiv&\sum_{z\leq x}\delta(z,x)g(z)\\ \equiv&g(x).\end{aligned}$$

从而等价.

考虑局部有限的偏序集$(\mathbb{N}_+,|)$, 其中$|$为整除偏序. 由唯一分解定理知存在偏序同构使得下图可交换

$$\begin{array}{rccc} \pi: & \prod_{p\in\mathbb{P}}(\mathbb{N})_p & \longrightarrow & \mathbb{N}_+ \\ & \prod_{p\in\mathbb{P}}(n_p)_p & \overset{1:1}{\longmapsto} & \prod_{p\in\mathbb{P}} p^{n_p} \end{array}$$

$$\begin{tikzcd} ((n_p)_p,(m_p)_p) \arrow[dr, mapsto, "\mu'"] & \\ (\prod_{p\in\mathbb{P}} p^{n_p},\prod_{p\in\mathbb{P}} p^{m_p}) \arrow[u, mapsto, "\pi,\sim"] \arrow[r, mapsto, "\mu"] & \mu(\prod_{p\in\mathbb{P}} p^{n_p},\prod_{p\in\mathbb{P}} p^{m_p}) \end{tikzcd}$$

由同态关系知

$$\mu\left(\prod_{p\in\mathbb{P}} p^{n_p},\prod_{p\in\mathbb{P}} p^{m_p}\right)=\prod_{p\in\mathbb{P}}\mu(p^{n_p},p^{m_p}).$$

其中诸$n_p \mid m_p$为必然要求, 从而偏序集$(\prod \mathbb{N},\leqq)$上的偏序关系为
$\{a_n\}\leqq\{b_n\}\Leftrightarrow a_n\le b_n,\forall n$. 下构造相应之Möbius函数.

对于以大小关系为序关系的全序集$(\mathbb{N},\le)$, 取$\delta(m,n)=\delta_{m,n}$. 从而不待计算即可构造Möbius函数

$$\mu_0(m,n):=\begin{cases}1 & n=m,\\ -1 & m+1=n,\\ 0 & \text{else.}\end{cases}.$$

从而在指数同构下有

$$\mu(p^{m_p},p^{n_p}):=\begin{cases}1 & n_p=m_p,\\ -1 & m_p+1=n_p,\\ 0 & \text{else.}\end{cases}.$$

易见对满足偏序$a\mid b$之序对$(a,b)$, $\mu(a,b)=\mu(1,b/a)$. 下记$\mu(d)$为一切$\mu(n,dn)$之值, $n\in\mathbb{N}_+$.

端详上式即得

$$\mu(x)=\begin{cases}(-1)^{n\text{的素因子个数}} & n\text{无素平方因子}\\ 0 & \text{else.}\end{cases}$$

## 分圆多项式等价形式之补充说明

对$\mathbb{C}$上某一适当的全纯区域, 对一切$d \mid n$, 诸分圆多项式$\Phi_d(z)$于某一区域$D$内全纯且诸$\log \Phi_d(z)$无branch cuts. 置$g_n(z) = z^n - 1$, 则$g_n(z) = \prod_{d|n} \Phi_d(z)$, 亦即$\log g_n(z) = \sum_{d|n} \log \Phi_d(z)$. 由Möbius反演定理知

$$\log \Phi_n(z) = \sum_{d|n} \mu(n/d) \log g_d(z).$$

从而

$$\prod_{d|n} (z^d - 1)^{\mu(n/d)} = \Phi_n(z).$$

由全纯函数之极大模原理知$\dfrac{\prod_{d|n} (z^d - 1)^{\mu(n/d)}}{\Phi_n(z)} \equiv 1, z \in \mathbb{C}.$