# Möbius 反演的若干应用

| | |
|---|---|
| Creat time | @September 27, 2022 |
| Type | Topic discussion |
| Topic | Combinatorics |
| Port time | @September 27, 2022 |
| P.S. | |



## 偏序集

**Definition 1.1 Poset** is defined as the pair of set $P$ and **binary partially ordered relation** $\leq$ such that

1. $a \leq a$ for all $a \in P$;

2. $(a \leq b) \wedge (b \leq a)$ implies $a = b$;
3. $(a \leq b) \wedge (b \leq c)$ implies $a = c$.

**Example 1.2** $(\mathbb{Z}, \leq)$ is a well-defined poset, but it has neither maximal element nor minimal element.

**Definition 1.3** An interval is defined as $[x, z] := \{y \in P \mid x \leq y \leq z\}$.

> 💡 **Remark** Interval can be empty.

**Definition 1.4** Let $A$ be a ring with identity (e.g., $\mathbb{R}$). We call $I : P \times P \to A$ an **incidence algebra** if $f(x, y) = 0$ unless $x \leq y$. In other words, $I$ maps the set of intervals in $P$ to $A$.

**Example 1.5** For instance, we have the following incidence algebra:

- $e(x, y) := \mathrm{value}(x = y)$;
- $\zeta(x, y) := \mathrm{value}(x \leq y)$.

Here the value is $1$ (or resp. $0$) whenever the statement is true (or resp. false).

**Definition 1.6** $I(P)$ is a $\mathbb{Z}$**-algebra**, the binary operation is defined as

1. $(f + g)(x, z) := f(x, z) + g(x, z)$;
2. $(f * g)(x, z) := \sum_{y \in [x,z]} f(x, y)g(y, z)$.

> 💡 **Remark** $e$ is the identity of $I(P)$.
>
> $*$ is associative, since
>
> $$\begin{aligned} & f * (g * h)(x, y), \\ = & \sum_{w \in [x,z]} \sum_{z \in [w,y]} f(x, w)g(w, z)h(z, y), \\ = & \sum_{x \leq w \leq z \leq y} f(x, w)g(w, z)h(z, y), \\ = & (f * g) * h(x, y). \end{aligned}$$

**Definiton 1.7** We call $(P, \leq)$ locally finite whenever all intervals are finite.

**Theorem 1.8** For any locally finite $(P, \leq)$, take $\forall \in f \in I(P)$, the following statements are equivalent:

1. $f$ has a left inversion;
2. $f$ has a right inversion;
3. $f(x, x) \neq 0$ for all $x \in P$.

▼ **Proof of the theorem**

1️⃣ implies 3️⃣, since $f_l^{-1}(x, x) f(x, x) = 1$.

3️⃣ implies 1️⃣, since $f_l^{-1}$ is uniquely defined by

$$\begin{cases} f_l^{-1}(x, x) f(x, x) = 1, \\ f_l^{-1}(x, y) f(y, y) = -\sum_{z \in [x, y)} f_l^{-1}(x, z) f(z, y). \end{cases}$$

💡 **Remark** As $f_l^{-1} * f(x, y) = 0$ for distinct pair $x, y$,

$$\sum_{z \in [x, y]} f_l^{-1}(x, z) f(z, y) = 0.$$

Therefore,

$$f_l^{-1}(x, y) f(y, y) = -\sum_{z \in [x, y)} f_l^{-1}(x, z) f(z, y).$$

2️⃣ is equivalent to 3️⃣ since $(P, \leq) \cong (P, \geq)^{\mathrm{op}}$.

**Theorem 1.9** The set of invertible incidence mappings forms a **multiplicative group**.

▼ **Proof of the theorem**

It is clear that the set of invertible incidence mappings forms a multiplicative semigroup with identity. Since each elements has a left inversion, we shall prove that $f_l^{-1}$ is also the right inversion. This is due to

$$
\begin{aligned}
ff_l^{-1} &= [(f_l^{-1})_l^{-1} f_l^{-1}][ff_l^{-1}] \\
&= (f_l^{-1})_l^{-1}[f_l^{-1}f]f_l^{-1} \\
&= [(f_l^{-1})_l^{-1} f_l^{-1}] \\
&= e.
\end{aligned}
$$

**Definition 1.9 Möbius function** $\mu$ is defined as the inversion of $\zeta$.

**Theorem 1.10** $\mu(x,x) = 1$, $\mu(x,z) = -\sum_{x \le y < z} \mu(x,y)$ if $x < z$.

▼ **Proof of the theorem**

See **Theorem 1.8**.

💡 **Remark** $\mu : P \times P \to \mathbb{Z}$.

**Theorem 1.11** (**Möbius inversion formula**) Let $(A,+)$ be an Abelian group, $(P,\le)$ be locally finite. Moreover, $\{z \in P \mid z \le x\}$ is finite for all $x \in P$. Taking $f, g : P \to A$, we have the following equivalent statements.

1. $g(x) = \sum_{y \le x} f(y)$ for all $x \in P$;
2. $f(x) = \sum_{y \le x} g(y)\mu(y,x)$ for all $x \in P$.

▼ **Proof of the theorem**

1️⃣ implies 2️⃣, since

$$
\begin{aligned}
\sum_{y \le x} g(y)\mu(y,x) &= \sum_{z \le y \le x} f(z)\mu(y,x) \\
(\text{fix } z, \text{sum } y) &= \sum_{z \le x} f(z)\delta(z,x) \\
&= f(x).
\end{aligned}
$$

Here $x$ is given.

2️⃣ implies 1️⃣, since

$$\begin{aligned}\sum_{y\le x} f(y) &= \sum_{z\le y\le x} g(z)\mu(z,y)\\ (\text{fix } z, \text{ sum } y) &= \sum_{z\le x} g(z)\delta(z,x)\\ &= g(x).\end{aligned}$$

Here $x$ is given.

# 数论中的 Möbius 反演公式

## 基本公式

**Definition 2.1.1** 正整数数关于整除构成偏序 $(\mathbb{Z}_{\ge 1}, |)$, $a \mid b$ 若且仅若 $b \in a\mathbb{Z}_{\ge 1}$.

**Theorem 2.1.2** 记 $\mathbb{P}$ 为素数集, 即 $\mathbb{Z}_{\ge 1}$ 中非 $1$ 的极小元之集. 则存在双射 $\mathbb{Z}_{\ge 1} \to \oplus_{\mathbb{Z}_{\ge 1}} \mathbb{Z}_{\ge 1}$.

▼ **Proof of the theorem**

记 $p_k$ 为第 $k$ 个素数, 则

$$(n_i)_{i\in\mathbb{Z}_i} \to \bigoplus_{i\ge 1} p_i^{n_i-1},$$

为良定义的双射 ($\mathbb{Z}_{\ge 1}$ 为唯一因子分解环).

**Theorem 2.1.3** $(\mathbb{Z}_{\ge 1}, |)$ 在 **Theorem 2.1.2** 的双射下同构于以下偏序 $(P, \leqq)$, 其中

- $P = \oplus_{\mathbb{Z}_{\ge 1}} \mathbb{Z}_{\ge 1}$;
- $(a_i)_{i\ge 1} \leqq (b_i)_{i\ge 1}$ 若且仅若 $a_i \leqq b_i$ 对一切 $i \in \mathbb{N}$ 成立.

▼ **Proof of the theorem**

显然.

**Theorem 2.1.4** 对一族局部有限偏序集 $(P_i, \le_i)_{i\in I}$, 定义其直和上的偏序 $(x_i)_{i\in I} \le (y_i)_{i\in I}$ 若且仅若 $x_i \le_i y_i$ 对一切 $i \in I$ 成立. 则直和上的 Möbius 函数为

$$\mu(x,y) = (\mu_i(x_i, y_i))_{i\in I}.$$

其中, 直和 $\oplus_{i\in I} P_i$ 中的元素除有限项外均为 $\min(P_i)$.

▼ **Proof of the theorem**

若 $I$ 为有限集, 则直和与直积无异. 注意到

$$\sum_{(z_i)_{i\in I}\in[(x_i)_{i\in I},(y_i)_{i\in I}]} = \sum_{z_1\in[x_1,y_1]}\cdots\sum_{z_n\in[x_n,y_n]}$$

即可.

若 $I$ 为无限集, 记 $(\mathscr{P},\subset)$ 为 $I$ 中有限子集依包含关系所称之偏序. 对 $\mathscr{P}$ 上任意给定的链 $\mathscr{C}$, 不妨设 $\mathscr{C}$ 中元素两两不同, 则 $|\{J\in\mathscr{C}\mid J\subset I\}|<\infty$ 对一切 $I\in\mathscr{C}$ 均成立.

对任意 $I_1,I_2\in\mathscr{P}$, 显然 Möbius 函数可自然延拓到 $I_1\cup I_2$ 上. 兹有断言, 上述 Möbius 函数可在 $\cup\mathscr{C}$ 上定义. 若不然, 则存在 $I_0\in\mathscr{C}$ 使得上述 Möbius 函数无法在 $\cup\{I\in\mathscr{C}\mid I\subset I_0\}$ 上定义; 而 $\cup\{I\in\mathscr{C}\mid I\subset I_0\}$ 为有限并, 从而矛盾.

根据 Zorn 引理, 即得在直和上可定义的 Möbius 函数.

**Example 2.1.5** 求解 $(\mathbb{Z}_{\geq 1},|)$ 上的 Möbius 函数.

▼ **Solution**

**Theorem 2.1.2-4** 给出同构 $(\mathbb{Z}_{\geq 1},|)\cong(\oplus_{\mathbb{Z}_{\geq 1}}\mathbb{Z}_{\geq 1},\leqq)$. 上的 Möbius 函数. 后者的导出代数可同构于其分量形式, 因此

$$\begin{aligned}&\mu_{\mathbb{Z}\geq 1}\left(\prod_{p_i\in\mathbb{P}}p_i^{m_i},\prod_{p_i\in\mathbb{P}}p_i^{n_i}\right)\\=&\mu_P\left(\bigoplus_{p_i\in\mathbb{P}}m_i,\bigoplus_{p_i\in\mathbb{P}}n_i\right)\\=&\prod_{i\geq 1}\mu_{P_i}(m_i,n_i)\\=&\prod_{i\geq 1}\mu_{\mathbb{Z}_{\geq 1}}(p_i^{m_i},p_i^{n_i}).\end{aligned}$$

注意到偏序集 $(\mathbb{Z}_{\geq 1},\leq)$ 上的 Möbius 函数为

$$\mu(i,j)=\begin{cases}1 & i=j,\\ -1 & i=j-1,\\ 0 & \text{else.}\end{cases}$$

As a result, $\mu(i,j)=\mu(i+k,j+k)$ for any $k\in\mathbb{Z}_{\geq 0}$. It yields that

$$\mu_{\mathbb{Z}_{\geq 1}}(x,y)=\mu_{\mathbb{Z}_{\geq 1}}\left(\frac{x}{\gcd(x,y)},\frac{y}{\gcd(x,y)}\right).$$

**Definition 2.1.6** For simplicity, we define $\mu(n):=\mu_{\mathbb{Z}_{\geq 1}}(1,n)$ in **Example 2.1.5**. It yields that

- $\mu(n)=+1$ if $n$ is a square-free positive integer with an even number of prime factors,
- $\mu(n)=-1$ if $n$ is a square-free positive integer with an odd number of prime factors,
- $\mu(n)=0$ if $n$ has a squared prime factor.

## 应用: Wedderburn 小定理

**Theorem 2.2.1** (**Wedderburn 小定理**) 有限整环必为域.

▼ **Proof of the theorem**

**Part** 1️⃣ 显然, 有限整环中的任意非零非单位元 $a$ 一定有逆元 $a^{o(a)-1}$, 其中 $o(a)$ 为乘法阶, 从而为体 (即除环). 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 $n=1$.

**Part** 2️⃣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 $n(x) \mid n$. 将 $K^*$ 中元素划分为共轭类, $x$ 共轭元之数量为 $\frac{|K^*|}{|N(x)^*|} = \frac{q^n-1}{q^{n(x)}-1}$. 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 $R$ 为分别选定的代表元系之集合.

**Part** 3️⃣ 若 $n \neq 1$, 下引入分圆多项式

$$\begin{aligned}
\Phi_r(x) := & \prod_{1 \leq d \leq r, \gcd(d,r)=1} (x - e^{2\pi i d/r}) \\
= & (x^r - 1) \prod_{k \geq 1} \left[ \prod_{\text{限定}^\star} (x^{r/(p_1 \cdots p_k)} - 1) \right]^{-1} \\
= & \prod_{d \mid r} (x^d - 1)^{\mu(r/d)},
\end{aligned}$$

限定$^\star$ : $p_1 \cdots p_k \mid r, p_1, \ldots, p_k$ 为互不相同之素数 (若存在).

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.

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 $\Phi_n(q) \mid \frac{q^n-1}{q^{n(x)}-1}$. 从而 $\Phi_n(q) \mid q - 1$. 注意到

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

因此矛盾, 故 $n = 1$.

# 不可约首 1 多项式计数

**Definition 3.1** We denote $\mathbb{F}_q$ as a **finte field** with $q$ elements.

**Theorem 3.2** $q = p^n$ is a always a prime power. Moreover, $\mathbb{F}_q$ is unique under isomorphism.

▼ **Proof of the theorem**

**Part** 1️⃣ Let $\mathrm{char}(\mathbb{F}_q)$ be the minimal positive integer $n$ such that $nq = 0$ for each $x \in \mathbb{F}_q$. Here $nq$ is the summation of $n$ $q$'s. If $\mathrm{char}(\mathbb{F}_q)$ is not prime, i.e., $p_1 \cdot p_2 \cdot m$, then there exists $y \in \mathbb{F}_q$ such that $p_2 \cdot my \in \mathbb{F}_q \setminus \{0\}$. Hence, for each $z \in \mathbb{F}_q$ we have

$$p_1 z = p_1(p_2 \cdot my)(p_2 \cdot my)^{-1} z = 0.$$

It yields that $\mathrm{char}(\mathbb{F}_q) = p_1$. As a result, $\mathrm{char}$ of a finite field is always a prime. Note $\mathrm{char}(\mathbb{F}_q) = p$.

**Part** 2️⃣ Take $\{v_1, \ldots, v_n\}$ as a basis of $\mathbb{F}_q$, then $|\mathbb{F}_q| = p^n$.

**Part** 3️⃣ We claim that $(\mathbb{F}_q \setminus \{0\}, \cdot)$ is also cyclic. Since $X^d - 1$ has at most $d$ roots, there is at most $1$ cyclic group in order $d$. When $(\mathbb{F}_q \setminus \{0\}, \cdot)$ is cyclic, there is exactly one subgroup in order $d$ for every $d \mid X$. Since each element belongs to a cyclic group, $(\mathbb{F}_q \setminus \{0\}, \cdot)$ has at most unique cyclic group in any given order if and only if it is cyclic.

**Part** 4️⃣ It is clear that $\mathbb{F}_{p^n}$ is generated by roots of $X^{p^n} - x$. Since $X^{p^n} - X$ has atmost $p^n$ roots, $\mathbb{F}_{p^n}$ is the splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$. Hence finite fields are unique under isomorphisms.

**Theorem 3.3** Let $f(x)$ be an irreducible polynomial in $\mathbb{F}_q[x]$, $\mathbb{F}_q[x]/\langle f(x)\rangle \cong \mathbb{F}_{q^{\deg f}}$.

▼ **Proof of the theorem**

Trivial.

**Theorem 3.4** $x^{q^n} - x$ is the product of monic polynomials in $\mathbb{F}_q[x]$ whose degree is a factor of $n$.

▼ **Proof of the theorem**

Let $E$ be splitting field of $x^{q^n} - x$ on $\mathbb{F}_q$. Then $\mathbb{F}_q$ consists of roots of $x^{q^n} - x$. Take $g(x)$ as a irreducible monic in $\mathbb{F}_q[x]$ and denote $u$ as one of its roots. It is clear that $g(x)$ is the minimal polynomial of $u$.

As a result, $g(x) \mid (x^{q^n} - x)$ whenever $u^{q^n} = u$, whenever $F_q(u) \subseteq R$, whenever $\deg g \mid n$.

We define the equivalent classes in $\mathbb{F}_{q^n}$, $x \sim y$ whenever $x$ and $y$ has the same minimal polynomial. By definition of irreducible polynomial, such equivalent relation is well-defined.

**Example 3.5** Let $M(q,n)$ be number of irreducible polynomials of degree $n$ in $\mathbb{F}_q[x]$. Then

$$q^n = \sum_{d|n} d \cdot M(q,d).$$

The Möbius inversion formula shows that

$$M(q,n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

For instance, if $n = p^m$ is a prime power, then $M(q,n) = \frac{q^{p^m} - q^{p^{m-1}}}{p^m}$.

## 图论应用 (未完待续)