有限生成Abel群(二)

张起帆

四川大学数学学院

email: qifanzhang@scu.edu.cn

2020 年 3 月 30 日

内容提要

唯一性部分

我们需要证明对任意有限生成abel群M，当它满足定理的形式

$$M \cong \mathbb{Z}^r \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z} \qquad (1),$$

各个量$r, d_1, ..., d_m$都是M的(同构)不变量.

唯一性部分

首先将(1)写成内直和形式

$$M = M_1 \oplus M_2,$$

其中$M_1 \cong \mathbb{Z}^r$, $M_2 \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z}$.

注意:

- M_1中的非0元全是无限阶的，而M_2中的元全是有限阶的
- 有限阶元+无限阶元=无限阶元

因此M_2正好是M的有限阶元之集合，我们记它为M_{tor}.

唯一性部分

首先将(1)写成内直和形式

$$M = M_1 \oplus M_2,$$

其中$M_1 \cong \mathbb{Z}^r$, $M_2 \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z}$.

注意:

- M_1中的非0元全是无限阶的，而M_2中的元全是有限阶的
- 有限阶元+无限阶元=无限阶元

因此M_2正好是M的有限阶元之集合，我们记它为M_{tor}.

唯一性部分

以下按步骤进行.

1、将问题简化到有限群的情形.

前面的观察知(1)式意味着

$$M_{tor} \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z}$$

$$M/M_{tor} \cong \mathbb{Z}^r.$$

(显然, M的同构类决定M_{tor}和M/M_{tor}的同构类) 两式中后一个意味着r的确是M的(同构)不变量. 前一个则意味着剩下只需证定理对有限群成立.

唯一性部分

2、将问题简化到有限p-群的情形.

若M有限，设M的阶为n. 再设

$$M \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z} \qquad (2).$$

由孙子定理，我们知道每个$\mathbb{Z}/d_i\mathbb{Z}$同构于若干个阶为素数幂(d_i的素数幂因子)的循环群的直和，这样M也同构于阶为素数幂(所有d_i的所有素数幂因子)的循环群的直和，而且$d_i, i = 1, ..., m$的素数幂因子的全体(称为$d_i, i = 1, ..., m$的初等因子)与d_i的全体可以互相决定，因此我们只需说明M和(2)式能决定d_i的全体初等因子即可.

唯一性部分

2、将问题简化到有限p-群的情形.

若M有限，设M的阶为n. 再设

$$M \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z} \qquad (2).$$

由孙子定理，我们知道每个$\mathbb{Z}/d_i\mathbb{Z}$同构于若干个阶为素数幂(d_i的素数幂因子)的循环群的直和，这样M也同构于阶为素数幂(所有d_i的所有素数幂因子)的循环群的直和，而且$d_i, i = 1, ..., m$的素数幂因子的全体(称为$d_i, i = 1, ..., m$的初等因子)与d_i的全体可以互相决定，因此我们只需说明M和(2)式能决定d_i的全体初等因子即可.

唯一性部分

设全体初等因子为$p^{a_{1,p}}, ..., p^{a_{r_p,p}}$,$p$跑遍$n$的素因子. 则有

$$M \cong \oplus_{p|n}(\mathbb{Z}/p^{a_{1,p}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{a_{r_p,p}}\mathbb{Z})$$

写成内直和有

$$M = \oplus_{p|n} M_p \quad (3)$$

$$M_p \cong \mathbb{Z}/p^{a_{1,p}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{a_{r_p,p}}\mathbb{Z} \quad (4).$$

但上两式意味着:

$M_p = M$的阶为p的幂的元形成的子群.

唯一性部分

具体说，任意$x \in M$可唯一表为$\sum_p x_p, x_p \in M_p$，而x的阶是所有x_p的阶之积.

注意：M_p是不依赖于分解方法的. 如果能证明M_p和(4)式能决定所有$p^{a_{i,p}}$，就能说明M 和(2)式能决定所有d_i. 这样我们就将定理归结为了有限p-群的情形.

唯一性部分

具体说，任意$x \in M$可唯一表为$\sum_p x_p, x_p \in M_p$，而x的阶是所有x_p的阶之积.

注意：M_p是不依赖于分解方法的. 如果能证明M_p和(4)式能决定所有$p^{a_{i,p}}$，就能说明M 和(2)式能决定所有d_i. 这样我们就将定理归结为了有限p-群的情形.

唯一性部分

3、对有限p-群M证明定理.

需证明由有限p-群M和同构

$$M \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{a_m}\mathbb{Z}, 0 < a_1 \leq \cdots \leq a_m$$

能完全决定每个a_i.

首先说明M能完全决定m, 反复用同态基本定理可得

$$M/pM \cong \mathbb{Z}/p\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p\mathbb{Z}(m\text{个})$$

我们暂时引进术语：称上述同构决定的m为M的长度.

唯一性部分

现将M重新表示为$M \cong M_1 \oplus \cdots \oplus M_n$，而每个$M_i$是$n_i$个$\mathbb{Z}/p^{b_i}\mathbb{Z}$的直和，$b_1 > \cdots > b_n$. 现在把每个量$b_i, n_i$都用$M$内在地描述，从而完成最后证明.

唯一性部分

考察模p^rM，让r从充分大开始递减地变化，那么我们有：

(a) b_1-1是第一个使p^rM非零的r，而n_1正是这个p^rM的长度；

(b) b_2-1是继b_1-1之后第一次使p^rM的长度发生变化的r，而n_2正是这个p^rM的长度增加的数目．以此类推可知每个量b_i,n_i都是M的不变量．证毕．

我们可以将r称为M的秩，$d_1,\ldots,d_m$称为M的不变因子，那些素数幂因子称为M的初等因子．而将M_p称为M的p分支．

例子

例1、$(\mathbb{Z}/n\mathbb{Z})^\times$是一类典型的有限生成abel群.

$$(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{m-2}\mathbb{Z}, m \geq 2,$$

$$(\mathbb{Z}/5^2\times 13\mathbb{Z})^\times \cong (\mathbb{Z}/5^2\mathbb{Z})^\times \oplus (\mathbb{Z}/13\mathbb{Z})^\times \cong \mathbb{Z}/(5\times 4)\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z},$$

重新整理为

$$(\mathbb{Z}/5^2\times 13\mathbb{Z})^\times \cong \mathbb{Z}/5\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/(3\times 4\times 5)$$

$(\mathbb{Z}/65\mathbb{Z})^\times$**的不变因子是4和60；初等因子是4，4，3，5.**

例子

例2、考察曲线

$$E:\{(x,y)\in\mathbb{C}^2|y^2=x^3+ax+b\}\bigcup\{O\}, a,b\in\mathbb{Q}, 4a^3+27b^2\neq 0.$$

点O称为无穷远点(可以看作人为添加的点，实际上有含义)，条件$4a^3+27b^2\neq 0$保证多项式x^3+ax+b无重根，即曲线上没有奇点．这样的E称为定义在$\mathbb{Q}$上的椭圆曲线.

对$\mathbb{C}$的任何子域F，可以有F点集合

$$E(F):=\{(x,y)\in F^2|y^2=x^3+ax+b\}\bigcup\{O\}.$$

例子

在$E(F)$上可以定义如下加法运算使之成为abel群：

1) $P+O=O+P=P$

2) 若P和Q关于X轴对称，则$P+Q=O$

3)若非上述情形，连接PQ($P=Q$时，引切线)交E于另一点R，作R关于X轴的对称点S，则$P+Q=S$.

可以检查(不显然)这样的加法有结合律，进一步，这些点构成一个加法群(显然)，群的单位元就是那个无穷远点，一个点的逆元则是它关于X轴的对称点．所有有理点的集合也构成群.

例子

在$E(F)$上可以定义如下加法运算使之成为abel群：

1) $P+O=O+P=P$

2) 若P和Q关于X轴对称，则$P+Q=O$

3)若非上述情形，连接PQ($P=Q$时，引切线)交E于另一点R，作R关于X轴的对称点S，则$P+Q=S$.

可以检查(不显然)这样的加法有结合律，进一步，这些点构成一个加法群(显然)，群的单位元就是那个无穷远点，一个点的逆元则是它关于X轴的对称点. 所有有理点的集合也构成群.

例子

我们最关心群$E(\mathbb{Q})$，要完全弄清楚它是很难的，已知

Mordell定理

$E(\mathbb{Q})$是有限生成的abel群.

还有一个定理说$E(\mathbb{Q})_{tor}$的结构只有有限种可能.

Mazur定理

$E(\mathbb{Q})_{tor}$同构于下列群之一：

$$\mathbb{Z}/m\mathbb{Z}, m = 1, 2, 3, ..., 10, 12.$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}, m = 2, 4, 6, 8$$

例子

我们最关心群$E(\mathbb{Q})$，要完全弄清楚它是很难的，已知

Mordell定理

$E(\mathbb{Q})$是有限生成的abel群.

还有一个定理说$E(\mathbb{Q})_{tor}$的结构只有有限种可能.

Mazur定理

$E(\mathbb{Q})_{tor}$同构于下列群之一：

$$\mathbb{Z}/m\mathbb{Z}, m = 1, 2, 3, ..., 10, 12.$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}, m = 2, 4, 6, 8$$

例子

困难的是$E(\mathbb{Q})$的秩r. 著名的**BSD**猜想(美国**Clay**研究所悬赏**100**万美元的七个千禧年难题之一)说r应等于某一个由E定义的复解析函数$L_E(s)$在特殊点$s=1$处的阶.

$L_E(s)$现在无法给出定义, 但需要说明的是它是一个定义复杂却可以计算的对象; 反过来r 是定义简单却难以计算的量.

BSD猜想在古老的(至少千岁)同余数问题上有简单应用. 称正整数n 是同余数, 如果n是三边都是有理数的直角三角形的面积(等价地可描述为n是三个成等差数列的平方数的公差).

例子

对奇数n，BSD猜想预言下列两条等价：

1) 奇数n是同余数；

2) 方程$x^2+2y^2+8z^2=n$的整数解中z为奇、偶的各占一半.

一个Coates-Wiles定理回答了BSD猜想中的小部分，但足以保证上述两条的$1) \Rightarrow 2)$.

对称群S_n

定义

n个数$1, 2, ..., n$的所有置换按映射的合成形成的群称为n元对称群，记为S_n.

显然任何n元集合X的对称群$S(X)$也与它同构，由Cayley定理知任何有限群都同构于某一S_n的子群.

- 轮换即S_n中元素$(i_1...i_s)$：将i_1映到i_2，i_2映到i_3，以此类推，最后i_s映到i_1，保持其它的元不变.
- 对换即两个元组成的轮换(ij)
- 不动点 $\sigma \in S_n$的不动点指的是满足$\sigma(x) = x$的x.

对称群S_n

定义

n个数$1, 2, ..., n$的所有置换按映射的合成形成的群称为n元对称群，记为S_n.

显然任何n元集合X的对称群$S(X)$也与它同构，由**Cayley**定理知任何有限群都同构于某一S_n的子群.

- 轮换即S_n中元素$(i_1 ... i_s)$：将i_1映到i_2，i_2映到i_3，以此类推，最后i_s映到i_1，保持其它的元不变.
- 对换即两个元组成的轮换(ij)
- 不动点 $\sigma \in S_n$的不动点指的是满足$\sigma(x) = x$的x.

基本性质

1. 任何置换都可表为有限个对换之积.
2. 对任何$\sigma \in S_n$，有

$$\sigma(i_1 \dots i_s)\sigma^{-1} = (j_1 \dots j_s), j_1 = \sigma(i_1), \dots, j_s = \sigma(i_s).$$

3. 任意置换都可唯一地(不计顺序)表为不交的轮换之积.

基本性质

1.是平凡的. 2容易证明, 但需理解清楚：对一个n元集合X, 如何给出S_n到$S(X)$的同构?

自然的想法是先给集合X一个编号, 即给一个双射$\phi : \{1, 2, ..., n\} \longrightarrow X$, 然后通过下列交换图给出同构$\widehat{\phi} : S_n \longrightarrow S(X)$

$$\begin{tikzcd}
\{1,2,...,n\} \arrow[r, "\phi"] \arrow[d, "\tau"'] & X \arrow[d, "\widehat{\phi}(\tau)"'] \\
\{1,2,...,n\} \arrow[r, "\phi"] & X
\end{tikzcd}$$

基本性质

1.是平凡的. 2容易证明, 但需理解清楚：对一个n元集合X, 如何给出S_n到$S(X)$的同构?

自然的想法是先给集合X一个编号, 即给一个双射$\phi : \{1, 2, ..., n\} \longrightarrow X$, 然后通过下列交换图给出同构$\widehat{\phi} : S_n \longrightarrow S(X)$

$$\begin{array}{ccc} \{1, 2, ..., n\} & \xrightarrow{\phi} & X \\ \tau \big\downarrow & & \big\downarrow \widehat{\phi}(\tau) \\ \{1, 2, ..., n\} & \xrightarrow{\phi} & X \end{array}$$

基本性质

但编号的方法并非唯一，甚至没有一个最好的，即对任意的$\sigma \in S_n$，可以用$\phi \circ \sigma$重新编号，即有下图

$$\begin{tikzcd}
\{1,2,...,n\} \arrow[r, "\sigma"] \arrow[d, "\tau"'] & \{1,2,...,n\} \arrow[r, "\phi"] \arrow[d, "\tau'"'] & X \arrow[d, "\widehat{\phi}(\tau')"'] \\
\{1,2,...,n\} \arrow[r, "\sigma"] & \{1,2,...,n\} \arrow[r, "\phi"] & X
\end{tikzcd}$$

此时中间的箭头τ'就是$\sigma\tau\sigma^{-1}$. 所以$\sigma\tau\sigma^{-1}$与τ只差一个编号，具有完全相同的形状.

基本性质

现在简单证明3. 任取$\tau \in S_n$, 可在集合$\{1, 2, ..., n\}$上定义等价关系$\sim$如下:

$$x \sim y \Longleftrightarrow \text{存在正整数} r \text{满足} y = \tau^r(x).$$

(自己验证它是等价关系, 注意τ是有限阶的.)得到$\{1, 2, ..., n\}$的一个划分$A_1 \cup A_2 \cup \cdots \cup A_s$. 任取$a_i \in A_i$, 记$r_i$为满足$\tau^r(a_i) = a_i$的最小$r$, 那么$r_i$正好是$A_i$的元素个数, 且$A_i = \{\tau^i(a_i) | i = 0, 1, ..., r_i - 1\}$. 那么$\tau|_{A_i}$正好是这$r_i$个元的轮换. 从而$\tau$是所有这些由划分决定的轮换之积.

基本性质

现在简单证明3. 任取$\tau \in S_n$, 可在集合$\{1, 2, ..., n\}$上定义等价关系$\sim$如下:

$$x \sim y \Longleftrightarrow \text{存在正整数} r \text{满足} y = \tau^r(x).$$

(自己验证它是等价关系, 注意τ是有限阶的.)得到$\{1, 2, ..., n\}$的一个划分$A_1 \cup A_2 \cup \cdots \cup A_s$. 任取$a_i \in A_i$, 记$r_i$为满足$\tau^r(a_i) = a_i$的最小$r$, 那么$r_i$正好是$A_i$的元素个数, 且$A_i = \{\tau^i(a_i) | i = 0, 1, ..., r_i - 1\}$. 那么$\tau|_{A_i}$正好是这$r_i$个元的轮换. 从而$\tau$是所有这些由划分决定的轮换之积.

基本性质

4. $(i_1 \cdots i_{s+t}) = (i_1 \cdots i_s)(i_s i_{s+1} \cdots i_{s+t})$.

因此有

$$
\begin{aligned}
(12 \cdots n) &= (n12 \cdots, (n-1)) = (1n)(12 \cdots (n-1)) \\
&= (1n)(1, n-1) \cdots (12).
\end{aligned}
$$

5. 对任意$x \in \{1, 2, ..., n\}$, 以x为不定点的τ的全体形成子群.

6. 奇数个对换之积一定非平凡.

基本性质

4. $(i_1 \cdots i_{s+t}) = (i_1 \cdots i_s)(i_s i_{s+1} \cdots i_{s+t})$.

因此有

$$
\begin{aligned}
(12\cdots n) &= (n12\cdots, (n-1)) = (1n)(12\cdots(n-1)) \\
&= (1n)(1, n-1)\cdots(12).
\end{aligned}
$$

5. 对任意$x \in \{1, 2, ..., n\}$, 以x为不定点的τ的全体形成子群.

6. 奇数个对换之积一定非平凡.

基本性质

4. $(i_1\cdots i_{s+t})=(i_1\cdots i_s)(i_s i_{s+1}\cdots i_{s+t})$**.**

因此有

$$\begin{aligned}(12\cdots n)&=(n12\cdots,(n-1))=(1n)(12\cdots(n-1))\\&=(1n)(1,n-1)\cdots(12).\end{aligned}$$

5. 对任意$x\in\{1,2,...,n\}$, 以x为不定点的τ的全体形成子群.

6. 奇数个对换之积一定非平凡.

基本性质

性质6虽然是熟知的，但并非天经地义，而是一条需证明的性质.

性质6的证明：对乘积中对换个数做归纳. 假设个数小于奇数m的对换之积非平凡，现有m个对换之积τ，不妨设有一个对换含1，通过适当顺序调整，使得含1的对换全部在前面，即

$$\tau = \tau_1\tau_2, \tau_1 = (1i_1)\cdots(1i_s)\sigma_1\cdots\sigma_t,$$

其中$s+t=m$, 每个σ_i是不含2的对换. 这样的调整能实现是因为等式$(23)(12)=(13)(23)$.

基本性质

先分两种情形：

1) $i_1, ..., i_s$中有重复. 由性质2知τ_1可写成$s-2$个元之积, 用归纳假设知τ非平凡.

2) $i_1, ..., i_s$中无重复. 则$\tau_1(1) = i_s$, 于是1是τ_2的不动点而非τ_1的不动点, 当然非τ的不动点, 故τ非平凡.

于是我们有奇置换和偶置换的概念. 所有偶置换形成S_n的子群, 称为交错群, 记为A_n. 它是指标为2的正规子群.

定理1

对任何$n \geq 5$, A_n是单群.

基本性质

先分两种情形：

1) $i_1, ..., i_s$中有重复. 由性质2知τ_1可写成$s-2$个元之积，用归纳假设知τ非平凡.

2) $i_1, ..., i_s$中无重复. 则$\tau_1(1) = i_s$，于是1是τ_2的不动点而非τ_1的不动点，当然非τ的不动点，故τ非平凡.

于是我们有奇置换和偶置换的概念. 所有偶置换形成S_n的子群，称为交错群，记为A_n. 它是指标为2的正规子群.

定理1

对任何$n \geq 5$，A_n是单群.

基本性质

在证明定理1之前，先给两个引理：

引理1

A_n由全体3轮换生成.

依定义，A_n有一组生成元：全体形如$(ab)(cd)$的元．这个引理是说生成元还可减少到全体(abc)，只需说明$(ab)(cd)$能有3轮换表出即可．这是显然的：

$(12)(23) = (123), (12)(34) = (123)(234)$.

基本性质

引理2

对$n \geq 5$，任一3轮换(ijk)可表为$(ijk) = \sigma(123)\sigma^{-1}$，$\sigma \in A_n$。

Proof.

由性质2知(ijk)可表为$(ijk) = \sigma(123)\sigma^{-1}$，$\sigma \in S_n$，只要$\sigma(1) = i, \sigma(2) = j, \sigma(3) = k$，但$\sigma$和$\sigma(45)$都具有此性质，且必有一在$A_n$中. □

基本性质

引理2

对$n \geq 5$，任一3轮换(ijk)可表为$(ijk) = \sigma(123)\sigma^{-1}$，$\sigma \in A_n$.

Proof.

由性质2知(ijk)可表为$(ijk) = \sigma(123)\sigma^{-1}$，$\sigma \in S_n$，只要$\sigma(1) = i, \sigma(2) = j, \sigma(3) = k$，但$\sigma$和$\sigma(45)$都具有此性质，且必有一在$A_n$中. □

定理1的证明思路

设H是A_n的阶>1的正规子群，需证明$H=A_n$，由引理1知只需证明H 含有全体3轮换，再由引理2知只需证明H含有某一3轮换.

注意：对非平凡置换τ，有

$$\tau\text{的不动点数} < n-1$$

$$\tau\text{是对换} \Longleftrightarrow \tau\text{的不动点数是}n-2$$

$$\tau\text{是3轮换} \Longleftrightarrow \tau\text{的不动点数是}n-3.$$

定理1的证明思路

因此我们的任务变为说明H中含有不动点数是$n-3$的元，即A_n中不动点数最多的非平凡元. 因而化为证明如下断言：

任给H中不动点数$< n-3$的τ，就可找到非平凡$\tau' \in H$，使得τ'的不动点更多.