练习选讲三

张起帆

四川大学数学学院

email: qifanzhang@scu.edu.cn

2019年10月30日

内容提要

练习1

1．设群G**是abel群，运算记加法，阶为**mn**，**$(m, n) = 1$**，证明：**

(1) $G = G[m] \oplus G[n]$

(2) $G[m] = \oplus_{p|m} G_p$

(3) $G[m] = nG$

(4) $G[m]$**是唯一的**m**阶子群。**

练习1

(5) 对$\alpha \in G$，记$\alpha = \alpha_1 + \alpha_2$，$\alpha_1 \in G[m], \alpha_2 \in G[n]$，则存在不依赖于$\alpha$的整数$k$使得$\alpha_1 = k\alpha$.

(6) α生成G当且仅当α_1生成$G[m]$且α_2生成$G[n]$.

(7) 若有G到另一个群K的满同态ϕ，则K也是abel的，且$\phi(G[m]) = K[m]$.

(8) 接上一问，若K是m阶，则$G \cong K \times \textbf{Ker } \phi$.

分析

都是直接验证，只是注意观察以下事实:

若$p^k|||G|$，则$G_p = G[p^k]$

对**(5)**题中的量，$\mathbb{Z}\alpha = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2$

分析

若G,K都是有限**abel**群，则给一个同态$\phi: G \longrightarrow K$等价于对每个$p$都给出一个$\phi_p: G_p \longrightarrow K_p$

（$\phi_p = \phi|_{G_p}$）

且ϕ满等价于所有ϕ_p都满，ϕ单等价于所有ϕ_p都单。

第**(8)**中，ϕ的限制给出$G[m]$到K的同构，而**Ker** $\phi = G[n]$

练习2

2. 若G是有限**abel**的p-群，$|G| = p^n$，$n > 1$，证明

(1) 以下几条等价

a) G是循环群

b) $|G[p^{n-1}]| = p^{n-1}$

c) $|G[p^{n-1}]| \leq p^{n-1}$

d) $|G[p^{n-1}]| < p^n$

(2) 若有G到p阶群K的同态ϕ，则

G是循环群等价于$G[p^{n-1}] =$ **Ker** ϕ，也等价于$G[p^{n-1}] \supset$ **Ker** ϕ.

分析

(1) 简单验证

(2) **Ker** ϕ是G的一个（现成的）p^{n-1}阶子群，当然 $G[p^{n-1}] \supset$ **Ker** ϕ，于是

$$G[p^{n-1}] = \textbf{Ker } \phi \Longleftrightarrow |G[p^{n-1}]| \leq p^{n-1}$$

练习3

3. 记$G=(\mathbb{Z}/p^n\mathbb{Z})^\times$，$p>2$，$n>1$，$|G|=(p-1)p^{n-1}$. 于是有标准分解：

$$G=G[p-1]\oplus G_p$$

(1) 证明以下对$G[p-1]$和G_p的描述：

$G[p-1]=\{\overline{x}|x^{p-1}\equiv 1 \pmod{p^n}\}=\{\overline{a^{p^{n-1}}}|a=1,...,p-1\}\cong(\mathbb{Z}/p\mathbb{Z})^\times$

$G_p=\{\overline{x}|x^{p^{n-1}}\equiv 1 \pmod{p^n}\}=\{\overline{x}|x\equiv 1 \pmod{p}\}$

(2) 对任意$\overline{a}\in G$，a在$G=G[p-1]$和G_p中的分量分别是什么？

(参考建议：可以考虑G到$(\mathbb{Z}/p\mathbb{Z})^\times$的自然同态。)

练习3

(3) 现在承认$\mathbb{Z}/p\mathbb{Z})^\times$是循环群（即模$p$的原根存在），证明$H := (\mathbb{Z}/p^2\mathbb{Z})^\times$是循环群。

练习3

(4) 对$n>2$，考察G到H的自然同态ϕ，证明ϕ的限制映射分别给出$G[p-1]$到$H[p-1]$的同构和G_p到H_p的满同态。

(5) 利用第2题结论证明G是循环群的充分必要条件是

$$x^{p^{n-2}} \equiv 1 \pmod{p^n} \Longrightarrow x \equiv 1 \pmod{p^2}$$

(6) 讨论p为奇和偶时，G是否是循环群，以及如何找群的生成元（即原根）。

分析

(1),(2),(3)只需对这个具体的群对号入座，且利用G到$(\mathbb{Z}/p\mathbb{Z})^\times$的自然同态和1题的最后一问。

分析

后面几问则是根据G到$\mathbb{Z}/p^2\mathbb{Z})^\times$的自然同态，用2题的结论和分析。

练习4

4. 设G是n阶abel群，证明关于循环群有以下等价描述并用条件5)考察3题中关于$\mathbb{Z}/p^n\mathbb{Z})^\times$是循环群的讨论：

1) G是循环群
2) 对任意$d|n$，G有唯一的d阶群。
3) 对任意$d|n$，$|G[d]| = d$.
4) 对任意$d|n$，$|G[d]| \leq d$.
5) 对任意$p|n$，$|G[d]| \leq d$.
6) 对任意$ds = n$，有$G[d] = sG$

分析

此题可以考虑有限abel群结构定理（也可以不用）。

练习5

5. 若G同构于m个有限循环的p-群的直和，请问$G[p]$的结构是什么？G有多少个p阶子群？

分析

直接计算，请记住第一问的结论。注意第二个问时，可以在$G[p]$中数。

练习6

设p为奇，证明：

(1) $x^2 \equiv a \pmod p$的解数为$1 + (\frac{a}{p})$.

(2) 记$\zeta_p = e^{2\pi i/p}$，$g_d = \sum\limits_{a=0}^{p-1} \zeta_p^{k^d}$，则

$$g_2 = \sum_{a=1}^{p-1} (\frac{a}{p}) \zeta_p^a$$

(3) $g_2^2 = (-1)^{\frac{p-1}{2}} p$.

分析

利用**(1)**得出

$$g_2 = \sum_{a=0}^{p-1}(1 + \frac{a}{p})\zeta_p^a$$

分析

计算$g_2^2 = (\sum_{a=0}^{p-1}(1+(\frac{a}{p}))\zeta_p^a)(\sum_{b=0}^{p-1}(1+\frac{b}{p})\zeta_p^b)$ 打开合并，归结为计算$\sum_{a=1}^{p-1}(\frac{a(t-a)}{p})$

分析

关键是注意到$(\frac{a(t-a)}{p}) = (\frac{a^{-1}t-1)}{p})$，因此

$$\sum_{a=1}^{p-1}(\frac{a(t-a)}{p}) = \sum_{a=1}^{p-1}(\frac{at-1)}{p})$$

练习7

求$(2+\sqrt{2})^{100}$的整数部分被**56**除的余数。

分析

首先所求的整数部分为$(2+\sqrt{2})^{100}+(2-\sqrt{2})^{100}-1$
其次利用$3^2 \equiv 2 \pmod 7$得

$$(2+\sqrt{2})^{100}+(2-\sqrt{2})^{100} \equiv (2+3)^{100}+(2-3)^{100} \pmod 7$$

分析

说清楚这件事就

令$f(x)=(2+x)^{100}+(2-x)^{100}=g(x^2)$，$f,g$都是整系数多项式。

练习8

证明对任意素数p，存在正整数n满足$p|2^n - n^2$.

分析

令$n \equiv 0 \pmod{p-1}$和$n \equiv 1 \pmod{p}$

练习9

对哪些素数p，存在正整数n满足$p|2^n+n^2$？关键点：若p满足条件$\frac{2}{p}=1$和$\frac{-1}{p}=-1$，则不行。想法说清楚这是全部。

练习10

解同余方程：$x^8 \equiv 2 \pmod{73}$. （考虑上次课中讲的关于解特殊的二次同余方程的想法）

分析

分析

分析