数论与代数练习

2020 年 4 月 25 日

Contents

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。

(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$G\cong K\times \mathrm{Ker}\ \phi$.

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

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$G[p^{n-1}]=\mathrm{Ker}\ \phi$，也等价于$G[p^{n-1}]\supset \mathrm{Ker}\ \phi$.

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$\bar{a}\in G$，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。)

(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。

(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）。

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$G[d]=sG$

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。

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

7. 求$(2+\sqrt{2})^{100}$的整数部分被56除的余数。

8. 证明对任意素数p，存在正整数n满足$p|2^n-n^2$.

9. 对哪些素数p，存在正整数n满足$p|2^n+n^2$？

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）