姓名________ 学号________ 班级________ 专业________ 学院________

装 订 线

扬州大学试题纸

(2017－2018 学年第一学期)

数学学院数 2016(年)级课程近世代数(A)卷

题目	一	二	三	四	五	六	七	八	总分
得分									

一．(12 分) 设G是一个有限群，$a\in G$．

1. 证明：$|a^{-1}|=|a|$，$|a|$表示元素 a 的阶;
2. 设 a 的阶为 12．求a^{2018}的阶;
3. 设G是 9 阶群．证明：G中存在 3 阶元.

1. 证明：$\because$ G 是有限群

$\therefore o(a)<\infty$

令 $o(a)=n$　$o(a^{-1})=m$

$a^n=e$

那么 $e=a^{-n}=(a^{-1})^n$

$\therefore n\mid m$

同理可证 $m\mid n$

$\because m,n>0$

$\therefore m=n$

即 $|a^{-1}|=|a|$

2. $o(a)=12$

$o(a^{2018})=\dfrac{12}{(2018,12)}$

$=\dfrac{12}{2}$

$=6$

3. 由 Largrage 定理

推论 $o(a)\mid |G|=9$

$\therefore o(a)=1,3,9$

若 G 中不存在三阶元

则 $\exists a$ s.t $o(a)=9$ 那么 G 为循环群.

有 $o(a^3)=\dfrac{9}{(3,9)}=3$

∴ G中存在三阶元

二. (16分) 1. 写出四次交错群 A_4 的所有元素;

2. 在对称群 S_4 中将元素 (1324)(214)(132) 表示成互不相连的循环置换的乘积; 说明该元素是否在 A_4 中;

3. 问 S_4 中是否存在4阶子群? 为什么?

1. $A_4 = \{(1), (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}$

2. $(1324)(214)(132) = (12)$

显然 $(12) \notin A_4$

3. $K_4 = \{(1), (12)(34), (13)(24), (14)(23)\} \leq A_4 \leq S_4$

∴ 存在4阶子群 K_4

三. (10分) 设 H, K 是群 G 的两个正规子群且 $H \cap K = \{e\}$, 其中 e 是群 G 的单位元. 证明: 对任意 $a \in H, b \in K$, 有 $ab = ba$.

证明: 由题意 $H \trianglelefteq G$　$bH = Hb$

$K \trianglelefteq G$, $aK = Ka$

$\forall a \in H, b \in K$, $(ab)(ba)^{-1} = aba^{-1}b^{-1}$

∵ $H \trianglelefteq G$

∴ $bH = Hb \Leftrightarrow ba^{-1}b^{-1} \in H$

∵ $a \in H$

∴ $aba^{-1}b^{-1} \in H$

同理由 $aba^{-1} \in K$, $b^{-1} \in K$

$\Rightarrow aba^{-1}b^{-1} \in K$

∴ $aba^{-1}b^{-1} \in H \cap K = \{e\}$

所以 $aba^{-1}b^{-1} = e$

$ab = ba$

四．（16 分）1.叙述环同态基本定理；

2.证明存在环同构：$\mathbb{Z}[x]/(5,x)\cong\mathbb{Z}_5$.

1. 环同态基本定理：$f: R \to \bar{R}$ 上的一个环同态

那么 $R/\ker(f) \cong \mathrm{Im}(f)$

2. $\varphi: \mathbb{Z}[x] \longrightarrow \mathbb{Z}_5$

$f(x) \longmapsto [f(0)]$.

显然 φ 是满射

且 ① $\varphi(f(x)+g(x))$ $\qquad$ $\varphi(f(x)g(x))$

$= [f(0)+g(0)]$ $\qquad$ $= [f(0)g(0)]$

$= [f(0)]+[g(0)]$ $\qquad$ $= [f(0)][g(0)]$

$= \varphi(f(x))+\varphi(g(x))$ $\qquad$ $= \varphi(f(x))\varphi(g(x))$

∴ φ 是一个满环同态

显然 $(5,x) \subseteq \ker(\varphi)$

如果 $[f(0)]=[0] \Leftrightarrow 5 \mid f(0) \Leftrightarrow (5,x)$ 由环同态基本定理的推广：

$\therefore \ker(\varphi)=(5,x)$ $\therefore \mathbb{Z}[x]/(5,x) \cong \mathbb{Z}_5$.

五. (16 分) 设域 $F=\mathbb{Z}_3=\{0,1,2\}$, $f(x)=x^3-x+1\in F[x]$.

1. 证明: $(f(x))$ 是多项式环 $F[x]$ 中的极大理想;
2. 证明: 商环 F[x]/(f(x)) 是 27 个元素的域;
3. 求 $x+(f(x))$ 关于乘法的逆元.

1.证明: 因为 $f(0)=1\neq 0$

$f(1)=1\neq 0$

$f(2)=1\neq 0$

$\therefore f(x)$ 不可约.

那么由于 $F[x]$ 是 PID

$\therefore (f(x))$ 为 $F[x]$ 中的极大理想

2.证明: 由于 $(f(x))$ 是 $F[x]$ 中的极大理想

$\therefore F[x]/(f(x))$ 是个域.

令 $F'=F[x]/(f(x))$ 下的单位元为 $1+(f(x))$

显然 $Ch(F')=3$, 且 $[F':\mathbb{Z}_3]=3$

$\therefore |F'|=3^3=27$

令逆为 $g(x)+(f(x))$ 下求 $g(x)$

3. $(x+(f(x)))(g(x)+(f(x)))$

$=xg(x)+(f(x))$

$=1+(f(x))$

那 $xg(x)-1\in(f(x))$

$g(x)=-x^2+1$

逆元: $-x^2+1+(f(x))$

六. (18 分) 设 $\mathbb{Z}[i]=\{a+bi\mid a,b\in\mathbb{Z}\}$ 是高斯整数环.

1．求出 $\mathbb{Z}[i]$ 中的单位；

2. 设 $\alpha=a+bi\in\mathbb{Z}[i]$ 且 $|\alpha|^2=p$，p 是素数. 证明：α 是不可约元；

3．将 6+8i 在 $\mathbb{Z}[i]$ 中分解成不可约元的乘积；

4. 求 2（3+4i）和 1-2i 在 $\mathbb{Z}[i]$ 的最大公因子.

1、$U(\mathbb{Z}[i])=\{1,-1,i,-i\}$

2、证明：若 α 是可约元

则 $\alpha=mn$, m,n 不是单位和相伴元

那么 $|\alpha|^2=|m|^2|n|^2$

$\because |\alpha|^2=p$

$\therefore |m|^2|n|^2=p$

且 $|m|^2,|n|^2\in\mathbb{Z}$

$\therefore |m|^2=1$ or $|n|^2=1$

与 m,n 是真因子相矛盾

$\therefore \alpha$ 是不可约元

3、$|6+8i|^2=36+64=100$

$=10\times10$

$(1+3i)(3-i)$

4. $\because |1-2i|^2=1+4$

$=5$

$\therefore$ 1-2i 为不可约元

$(3+4i)=(1-2i)(a+bi)$

$\begin{cases}3=a+2b\\4=b-2a\end{cases}$

$10-$

$b=2$

$a=-1$

$(3+4i)=(1-2i)(-1+2i)$

$\therefore 1-2i\mid 2(3+4i)$

$\therefore (2(3+4i),(1-2i))$

$=1-2i$

装 订 线

$\therefore 6+8i=(1+3i)(3-i)=(1+i)(2+i)(1+i)(1-2i)$

$|1+3i|^2=10=2\times 5$

七. (12 分) 设 $\mathbb{Z}_n$ 是模 n 的剩余类环.

1. 给出模 8 的剩余类环 $\mathbb{Z}_8$ 所有零因子和可逆元。
2. 设 $a\in\mathbb{Z}$. 证明: $[a]$ 在 $\mathbb{Z}_n$ 中乘法可逆当且仅当 $(a,n)=1$;
3. 设 $a\in\mathbb{Z}$ 且 $(a,n)=1$ 证明: $n\mid(a^{\phi(n)}-1)$, 其中 $\phi(n)$ 是 n 的欧拉数, 即在 1 到 n 之间与 n 互素的自然数的个数.

解. 1. $\mathbb{Z}_8=\{[0],[1],\cdots[7]\}$

零因子: $[2]\ [4]\ [6]$

可逆元: $[1]\ [3]\ [5]\ [7]$

2. 证明: "$\Leftarrow$" $(a,n)=1$

$\therefore \exists s,t$, 有

$as+tn=1$

那 $[a][s]=[1]$

故 $[s]$ 为 $[a]$ 的可逆元

"$\Rightarrow$" 若 $[a]$ 可逆

$\therefore [a][s]=[1]$

$[a][s]+[n][t]=[1]$

$\exists s,t$, 使得

$as+nt=1$

$\therefore (a,n)=1$

3. $U(\mathbb{Z}_n)=\{[a]\mid(n,a)=1\}$

Thus $a\in U(\mathbb{Z}_n)$

且 $|U(\mathbb{Z}_n)|=\phi(n)$

由 Lagrange 定理知

$o(a)\mid|U(\mathbb{Z}_n)|=\phi(n)$

$\therefore a^{\phi(n)}=1$

故 $n\mid a^{\phi(n)}-1$.