# 浙江大学 2020－2021 学年秋冬学期

## 《抽象代数》课程期中考试试卷

开课学院：__理学院__ ，考试形式：闭卷，允许带___________入场

考试时间：2020 年 11 月 9 日, 所需时间：__120__ 分钟

考生姓名：________________学号：_________专业：____________________

| 题序 | 一 | 二 | 三 | 四 | 五 | 总 分 |
|---|---|---|---|---|---|---|
| 得分 | | | | | | |
| 评卷人 | | | | | | |

一 . Explain the following notion(10%×2=20%.)

1.Group.

2.G-set (where G is a group).

二.（20%） Let p be a prime number, $Z_p = \{\bar{a} | a \in Z\}$，where $\bar{a} = a + pZ = \{a + pc | c \in Z\}$. Set $SL(2, Z) \coloneqq \{A \in M_2(Z) | \det(A) = 1\}$ and $SL(2, Z_p) \coloneqq \{A \in M_2(Z_p) | \det(A) = \bar{1}\}$. Show that the mapping $\varphi: SL(2, Z) \to SL(2, Z_p), \varphi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$ is an epimorphism from $SL(2, Z)$ to $SL(2, Z_p)$.

三.（20%） (First fundamental theorem of homomorphism) Suppose G is a group and N is a subgroup of G. Show that N is a normal subgroup of G if and only if there exists a homomorphism $\pi: G \to H$ such that $\ker(\pi) = N$.

四.（20%）Let H be a subgroup of G and p = [G:H]. Suppose p is the least positive prime factor of |G|. Show that H is a normal subgroup of G.

五.（20%） Suppose G is a group of order 455. (1)Find the number of Sylow p-subgroups of G. (2)Show that G is a cyclic group.

参考答案：

一. 1. A nonempty ~~grou~~ set $G$ together with a binary operation $\cdot : G \times G \to G$, $(x,y) \mapsto x \cdot y$ is called a group if it satisfies:

① (associativity) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, ~~∀~~ for any $a, b, c \in G$;

② (identity) ~~there is~~ for any $a \in G$, $a \cdot e = e \cdot a = a$;

③ ~~(invertible~~ (inverse) for any $a \in G$, there is an element $b \in G$ such that $ab = ba = e$.

2. A nonempty set $X$ is called a $G$-set if there is a mapping $G \times X \to X$, $(g,x) \mapsto gx$ such that, for all $x \in X$ and $g_1, g_2 \in G$, $ex = x$ and $(g_1 g_2)x = g_1(g_2 x)$, where $e$ is the identity of ~~a~~ group $G$.

二. Proof: ① well-defined. ~~for~~ For any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z})$,

$ad-bc=1 \quad \therefore \ \bar{a}\bar{d}-\bar{b}\bar{c} = \overline{ad-bc} = \bar{1}$

$\therefore \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \in SL(2,\mathbb{Z}_p)$.

② homomorphism. For any $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} u & v \\ w & x \end{pmatrix} \in SL(2,\mathbb{Z})$,

$$\varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} u & v \\ w & x \end{pmatrix}\right) = \varphi\begin{pmatrix} au+bw & av+bx \\ cu+dw & cv+dx \end{pmatrix} = \begin{pmatrix} \overline{au+bw} & \overline{av+bx} \\ \overline{cu+dw} & \overline{cv+dx} \end{pmatrix}$$

$$= \begin{pmatrix} \bar{a}\bar{u}+\bar{b}\bar{w} & \bar{a}\bar{v}+\bar{b}\bar{x} \\ \bar{c}\bar{u}+\bar{d}\bar{w} & \bar{c}\bar{v}+\bar{d}\bar{x} \end{pmatrix} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}\begin{pmatrix} \bar{u} & \bar{v} \\ \bar{w} & \bar{x} \end{pmatrix} = \varphi\begin{pmatrix} a & b \\ c & d \end{pmatrix}\varphi\begin{pmatrix} u & v \\ w & x \end{pmatrix}.$$

③ surjective. First, we claim that $SL(2,\mathbb{Z}_p)$ is generated by $\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{k} & \bar{1} \end{pmatrix}$ and $\begin{pmatrix} \bar{1} & \bar{k'} \\ \bar{0} & \bar{1} \end{pmatrix}$, $\bar{k}, \bar{k'} \in \mathbb{Z}_p$.

(i) For any $\bar{k}, \bar{k'} \in \mathbb{Z}_p$, $\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{k} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{k'} \\ \bar{0} & \bar{1} \end{pmatrix} \in SL(2,\mathbb{Z}_p)$.

(ii). For any $\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \in SL(2,\mathbb{Z}_p)$, if $\bar{a} \neq \bar{0}$,

$$\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \xrightarrow{R_2 - \bar{a}^{-1}\bar{c}R_1} \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{0} & \underbrace{\bar{d}-\bar{a}^{-1}\bar{c}\bar{b}}_{=\bar{a}^{-1}} \end{pmatrix} \xrightarrow{C_2 - \bar{a}^{-1}\bar{b}C_1} \begin{pmatrix} \bar{a} & \bar{0} \\ \bar{0} & \bar{a}^{-1} \end{pmatrix}$$

$$\xrightarrow{C_1 + \bar{a}C_2} \begin{pmatrix} \bar{a} & \bar{0} \\ \bar{1} & \bar{a}^{-1} \end{pmatrix} \xrightarrow{R_1 - \bar{a}R_2} \begin{pmatrix} \bar{0} & -\bar{1} \\ \bar{1} & \bar{a}^{-1} \end{pmatrix} \xrightarrow{R_1 + R_2} \begin{pmatrix} \bar{1} & \bar{a}^{-1}-\bar{1} \\ \bar{1} & \bar{a}^{-1} \end{pmatrix}$$

$$\xrightarrow{R_2 - R_1} \begin{pmatrix} \bar{1} & \bar{a}^{-1}-\bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}.$$ By $\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{k} & \bar{1} \end{pmatrix}^{-1} = \begin{pmatrix} \bar{1} & \bar{0} \\ -\bar{k} & \bar{1} \end{pmatrix}$, $\begin{pmatrix} \bar{1} & \bar{k'} \\ \bar{0} & \bar{1} \end{pmatrix}^{-1} = \begin{pmatrix} \bar{1} & -\bar{k'} \\ \bar{0} & \bar{1} \end{pmatrix}$,

we can get $\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \in \left\langle \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{k} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{k'} \\ \bar{0} & \bar{1} \end{pmatrix}, \bar{k}, \bar{k'} \in \mathbb{Z}_p \right\rangle$.

If $\bar{a} = \bar{0}$, we can consider $\begin{pmatrix} \bar{a}+\bar{b} & \bar{b} \\ \bar{c}+\bar{d} & \bar{d} \end{pmatrix}$ instead. ~~and~~ ~~and~~ ~~$\bar{a}+\bar{b} \neq \bar{0}$~~

By $\begin{pmatrix}\bar a & \bar b\\ \bar c & \bar d\end{pmatrix} \xrightarrow{C_1+C_2} \begin{pmatrix}\bar a+\bar b & \bar b\\ \bar c+\bar d & \bar d\end{pmatrix}$ and $\bar a+\bar b \neq \bar 0$ (otherwise, $\overline{ad-bc}=\bar 0$), we can get our conclusion.

$$\therefore \quad SL(2,\mathbb{Z}_p) = \left\langle \begin{pmatrix}\bar 1 & \bar 0\\ \bar k & \bar 1\end{pmatrix}, \begin{pmatrix}\bar 1 & \bar k'\\ \bar 0 & \bar 1\end{pmatrix}, \bar k, \bar k' \in \mathbb{Z}_p \right\rangle.$$

Then, since ~~by~~ ~~the~~ the preimage of $\begin{pmatrix}\bar 1 & \bar 0\\ \bar k & \bar 1\end{pmatrix}, \begin{pmatrix}\bar 1 & \bar k'\\ \bar 0 & \bar 1\end{pmatrix}$ ~~are~~ can be $\begin{pmatrix}1 & 0\\ k & 1\end{pmatrix}, \begin{pmatrix}1 & k'\\ 0 & 1\end{pmatrix} \in SL(2,\mathbb{Z})$, we can find the preimage of any element in $SL(2,\mathbb{Z}_p)$. Thus, $\varphi$ is a surjection.

三. Proof: "$\Rightarrow$" Suppose that $N$ is a normal subgroup of $G$. Then $G/N$ is a group with its multiplication defined as $aN\cdot bN = abN$. For $aNa^{-1}\subset N$, for any $a\in G$, the multiplication is well-defined and the identity of $G/N$ is $N$, $(aN)^{-1}=a^{-1}N$.

Define $\pi: G \to G/N$

$$g \mapsto gN \quad \text{for any } g\in G.$$

$$\pi(gh) = ghN = gN\cdot hN = \pi(g)\pi(h) \quad \therefore \pi \text{ is a homomorphism}$$

$g\in \ker(\pi) \Leftrightarrow gN = N \Leftrightarrow g\in N \quad \therefore \ker(\pi) = N.$

"$\Leftarrow$". Suppose that there is a homomorphism $\pi: G\to H$ such that $\ker(\pi) = N$.

For any $g\in G$, $n\in N$, $\pi(gng^{-1}) = \pi(g)\pi(n)\pi(g^{-1})$

$$= \pi(g)\cdot e_H \cdot \pi(g)^{-1} = e_H.$$

where $e_H$ is the identity of $H$.

$\therefore gng^{-1} \in \ker(\pi) = N. \quad \therefore N$ is a normal subgroup of $G$.

③. Proof: Denote $G/H$ by $G/H := \{H_1, H_2, \cdots, H_p\}$, where $H_1 = H$. The action of $G$ on $G/H$: $\begin{matrix} G \times G/H \to G/H \\ (g, H_i) \mapsto gH_i \end{matrix}$ is ~~well~~ well-defined and $g$ can be viewed as a bijection of set $G/H$ for $gH_i = gH_j \Leftrightarrow H_i = H_j$ and ~~for any~~ $\forall H_i$, $\exists H_j = g^{-1}H_i$, such that $gH_j = H_i$.

Thus we can define a map $\varphi: G \to S_p$, $g \mapsto \sigma_g$, where ~~$g \mapsto \sigma_g$~~ $H_{\sigma_g(i)} = gH_i$: As for any $g, h \in G$, $i = 1, 2, \cdots, p$. $ghH_i = g(hH_i)$, we have $H_{\sigma_{gh}(i)} = ghH_i = g(hH_i) = gH_{\sigma_h(i)} = H_{\sigma_g\sigma_h(i)}$ and then $\sigma_{gh}(i) = \sigma_g\sigma_h(i)$. $\therefore \varphi(gh) = \varphi(g)\varphi(h)$, $\varphi$ is a homomorphism.

For $g \in \ker(\varphi)$, ~~$H_{\sigma_g(i)} =$~~ $gH_i = H_{\sigma_g(i)} = H_i$, $i = 1, 2, \cdots, p$. $\therefore gH = H$ $\therefore g \in H$ $\therefore \ker(\varphi) \leq H$. $\therefore [G:H] \mid [G:\ker\varphi]$.

On the other hand, $G/\ker\varphi \cong \mathrm{Im}\varphi$ and $\mathrm{Im}\varphi \leq S_p$.

$\therefore [G:\ker\varphi] = |\mathrm{Im}\varphi|$ and $|\mathrm{Im}\varphi| \mid |S_p|$.

Hence, $p \mid [G:\ker\varphi]$ and $[G:\ker\varphi] \mid p!$. As $p$ is the least positive prime factor of $|G|$ and $[G:\ker\varphi] \mid |G|$, we have $[G:\ker\varphi] = p$ $\therefore \ker(\varphi) = H$ $\therefore H$ is a normal subgroup of $G$.

2. Proof: $455=5\times7\times13$. By ~~st~~ sylow theorem the number of sylow 5-subgroups $k_5$ satisfies $k_5 \mid 91$ and $k_5 \equiv 1 \pmod 5$, so $k_5=1$ or $91$. ~~Sim~~ Similarly, the number of Sylow 7-subgroups $k_7=1$ and the number of Sylow 13-subgroups $k_{13}=1$.

If $k_5=91$, there are $91\times4=364$ elements whose order is 5. We use $M$ and $N$ to ~~d~~ denote the unique Sylow 7-subgroup and Sylow 13-subgroup. ~~For~~ Then $M \lhd G$, $N \lhd G$, $MN \le G$ and ~~the orders~~ ~~the elements in MN are all~~ for ~~any~~ any $a \in MN$, $|a| \neq 5$. By $|MN|=91$, $364+91=455$, we get all the elements of $G$.

Now we choose a Sylow 5-subgroup $H$. By Sylow theorem, group $HM$ has only one Sylow 5-subgroup and one Sylow 7-subgroup. So $H \lhd HM$, $M \lhd HM$. As $H \cap M=\{e\}$, $HM=H\times M$ is a cyclic group of order 35. So there is an element of order 35 in $G$. Contradiction.

Hence ~~k~~ $k_5=1$.

$\therefore$ $G=H\times M\times N$ is a cyclic group. ~~of order 455~~.

2. ~~Proof~~: Show that $(5, 2x+3)$ is a maximal ideal of $\mathbb{Z}[x]$. Determine the field $\mathbb{Z}[x]/(5, 2x+3)$.

Proof: (1) ~~Let~~ Suppose ~~ideal~~ there is an ideal $M$ contains $(5, 2x+3)$, and $M \neq (5, 2x+3)$.

Then there is an element $f(x)$ ~~$\in M$~~ such that $f(x) \in M$ and $f(x) \notin (5, 2x+3)$. As $3(2x+3) - 5(x+1) = x+4 \in (5, 2x+3)$ and $f(x) = g(x)(x+4) + 5p + r$, $0 \le r \le 4$, $g(x) \in \mathbb{Z}[x]$, $p \in \mathbb{Z}$, we can get an element $r$ such that $r \in M$ and $r \notin (5, 2x+3)$. $\therefore (5, r) = 1$.

~~$\therefore$ There~~ So there exists $u, v \in \mathbb{Z}$, such that $5u + rv = 1$.

$\therefore 1 \in M$ $\therefore \mathbb{Z}[x] \in M$ $\therefore M = \mathbb{Z}[x]$.

$\therefore (5, 2x+3)$ is a maximal ideal of $\mathbb{Z}[x]$.

(2) By ~~Second~~ Third fundamental Theorem of Homomorphism of Rings, $\mathbb{Z}[x]/(5, 2x+3) \simeq \dfrac{\mathbb{Z}[x]/5}{(5, 2x+3)/5} = \mathbb{Z}_5[x]/(\bar{2}x+\bar{3})$

For $\bar{3}(\bar{2}x+\bar{3}) = \bar{x}+\bar{4}$, $\mathbb{Z}_5[x]/(\bar{2}x+\bar{3}) = \mathbb{Z}_5[x]/(x+\bar{4}) \simeq \mathbb{Z}_5$.