AI for Math 数学形式化抽象代数期中考试

姓名: ____________ **学校:** ____________ **分数:**

时间：120 分钟 满分：110 分, 总分不超过 100 分

所有的环都假设含有乘法单位元 1, 且所有的环同态都将 1 映到 1.

All rings contain a multiplicative unit 1, and all ring homomorphisms are assumed to send 1 to 1.

判断题 判断下述命题是否正确。在下表中填写 T (正确) 或 F (错误), 不需要解释判断的缘由 (15 分)

1	2	3	4	5
T	F	T	T	T
6	7	8	9	10
F	F	T	F	F
11	12	13	14	15
F	T	T	F	F

1. 在有限群 G 中, 存在正整数 n , 使得 $g^n = 1$ 对所有 $g \in G$ 成立.

In a finite group G, there exists a positive integer n such that for every $g \in G$, $g^n = 1$.

True. By Lagrange theorem, take $n = \#G$, then $g^n = 1$ for every $g \in G$.

2. 空集可以被看作为群.

The empty set can be viewed as a group.

False. A group must contain a unit element.

3. 考虑 G 在自身上的左乘作用. 这个作用是可迁的.

Consider a group G acting on itself by left multiplication. The action is transitive.

True. Any element $g \in G$ is the translate of 1 by g under the left multiplication action.

4. 令 X 是正 n 边形, A 是 X 的所有顶点的集合. 则 D_{2n} 在 A 上显然的群作用是可迁的.

Let X be a regular n-gon and A the set of all vertices of X. Then the obvious action of D_{2n} on A is transitive.

True. The action is indeed transitive.

5. 令 $f : G \to H$ 是群同态. 若 f 是双射, 则 f^{-1} 也是群同态.

Let $f : G \to H$ be a homomorphism. If f is a bijection then f^{-1} is also a homomorphism.

True. This is standard fact.

6. 在交换群中, 若 x 是 n 阶元, y 是 m 阶元, 其中 n 和 m 都是正整数, 则 xy 是 nm 阶元.

In a commutative group if x is an element of order n and y is an element of order m, where n and m are positive integers, then xy is an element of order nm.

False. This is true if n and m are relatively prime, but not true in general. For example, if the order of x is n, then the order of x^{-1} is n, and the order of $x \cdot x^{-1}$ is 1.

7. 若群 G 中的所有元素都满足 $g^p = 1$, 其中 p 是素数, 则 G 是交换群.

Suppose every element g of a group G satisfies $g^p = 1$ for some prime number p. Then G is abelian.

False. The group $G = \begin{pmatrix} 1 & k_1 & k_2 \\ 0 & 1 & k_3 \\ 0 & 0 & 1 \end{pmatrix}$ where $k_i \in \mathbb{Z}/3\mathbb{Z}$ satisfies $g^3 = 1$ for every $g \in G$, but G is not abelian.

8. 交换群的商群也是交换的.

All quotient group of a commutative group are commutative.

True. Clear.

9. $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ 中的元素都是 8 阶的.

Every element of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ has order 8.

False. The order of every element is a divisor of 8. The order of 0 is 1.

10. 若 G 是单群, 则 G 的换位子群等于 G.

The commutator group G of a simple group is G.

False. This is true for noncommutative simple groups, yet it is untrue for commutative groups, e.g. $\mathbb{Z}/p\mathbb{Z}$ for a prime p.

11. 令 I 和 J 都是交换环 R 的理想. 则 $\{ab \mid a \in I, b \in J\}$ 是 R 的理想.

Let I and J be ideals in a commutative ring R. Then $\{ab \mid a \in I, b \in J\}$ is an ideal of R.

False. This IJ may not be an ideal. For example, in $\mathbb{Z}[x]$, $I = J = (2, x)$. Consider the element $f = x^2 + 4$; it belongs to the ideal IJ, but it is not a product of the form fg with $f, g \in I$.

12. 令 G 是有限群, H 是 Sylow p-子群, 其中 p 是素数. 则正规化子子群 $N_G(H)$ 包含正规的 Sylow p-子群.

Let G be a finite group and H a Sylow p-subgroup, where p is a prime. Then the normalizer subgroup $N_G(H)$ admits a normal Sylow p-subgroup.

True. As H is normal in $N_G(H)$, and is clearly a Sylow p-subgroup of $N_G(H)$; so $N_G(H)$ contains a normal Sylow p-subgroup.

13. 所有无限群都包含有限子群.

Every infinite group contains a subgroup of finite order.

True. Every infinite group contains $\{1\}$ as a subgroup.

14. 令 $\varphi : R \to R'$ 是环同态. 则对 $u \in R$, 若 $\varphi(u)$ 是 R' 中的单位, 则 u 是 R 中的单位.

Let $\varphi : R \to R'$ be a ring homomorphism. Then for an element $u \in R$, if $\varphi(u)$ is a unit in R', then u is a unit in R.

False. For example, $\varphi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ is the natural modulo 3 homomorphism. Then the number $u = 4$ satisfies $\varphi(u) = 1$ yet $u = 4$ is not a unit.

15. 令 $\phi : G \to H$ 是群同态. 若对于某个 H 中的元素 h_0 , 存在唯一 $g_0 \in G$, 使得 $\phi(g_0) = h_0$, 则任取 $h \in H$, 存在唯一 $g \in G$ 使得 $\phi(g) = h$.

Let $\phi : G \to H$ be a homomorphism. If for some element h_0 of H, there exists a unique $g_0 \in G$ such that $\phi(g_0) = h_0$, then for every $h \in H$, there exists a unique $g \in G$ such that $\phi(g) = h$.

False. The uniqueness part is true, but the existent part of g in general needs ϕ to be surjective.

Grading table

T/F	Easy ques.	Examples	1	2	3	4	5	6	Total
/15	/20	/15	/8	/15	/15	/7	/10	/5	/110

简单题目 Quick questions (5 分 $\times 4 = 20$ 分)

(1) 若 A 和 B 是 G 中共轭的子群, N 是 G 的正规子群. 证明: AN 和 BN 是 G 中共轭的子群.

Let A and B be conjugate subgroups of G and N a normal subgroup of G. Show that AN and BN are conjugate subgroups of G.

证明. Suppose that $A = gBg^{-1}$ for $g \in G$. We have

$$gBNg^{-1} = gBg^{-1} \cdot gNg^{-1} = A \cdot N$$

So BN and AN are conjugate subgroups. □

(2) 令 $\varphi : R \to R'$ 是环同态, I' 是 R' 的双边理想. 证明: $\varphi^{-1}(I')$ 也是 R 的双边理想.

Let $\varphi : R \to R'$ be a ring homomorphism of rings, and let I' be a two-sided ideal of R'. Show that $\varphi^{-1}(I')$ is a two-sided ideal of R.

证明. This is standard fact. □

(3) 证明: 从 A_5 到 750 阶群的群同态一定是平凡的.

Prove that a homomorphism from A_5 to a group of order 750 must be trivial.

证明. Note that the order $\#A_5 = 60$. Let $\varphi : A_5 \to G$ be a homomorphism to a group G of order 750. The image $\varphi(A_5)$ is a subgroup of G and thus has order being a factor of 750. Yet $60 \nmid 750$. So $\ker\varphi$ is nontrivial. But A_5 is a simple group; so φ is trivial. □

(4) 若 G 是循环群, 令 $\varphi : G' \to G$ 是同态, 使得 $\ker(\varphi)$ 被包含于 G' 的中心. 证明: G' 是交换群.

If G is a cyclic group and let $\varphi : G' \to G$ is a homomorphism whose kernel $\ker(\varphi)$ lies in the center of G'. Show that G' is abelian.

证明. Noticed that $G/Z(G)$ is a quotient of $G/\ker(\varphi) \cong G'$, which implies $G/Z(G)$ is cyclic. Let $g \in G$ be a generator of $G/Z(G)$, then every elements of G is of form $g^n z$, where $n \in \mathbb{Z}$ and $z \in Z(G)$. Since $(g^n z)(g^{n'} z') = g^n z g^{n'} z' = g^{n+n'} z z' = g^{n'} z' g^n z$, G is abelian. □

举例 Examples (3 分 ×5 = 15 分)

无需证明你的例子或者答案满足要求，只需要清楚叙述你的例子或者答案。

(1) 给出: 两个拥有相同的 Jordan–Hölder 因子, 且每个因子都只出现一次, 但是不同构的群的例子.

Give an example of two non-isomorphic groups with the same set of Jordan–Hölder factors, where each factor has multiplicity one.

例子 The group S_3 and $\mathbb{Z}/6\mathbb{Z}$; both have Jordan–Hölder factors $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$.

(2) 给出: 非交换可解群的例子.

Give an example of a non-abelian solvable group.

例子 If k is a field, the group $G = \begin{pmatrix} 1 & k & k \\ 0 & 1 & k \\ 0 & 0 & 1 \end{pmatrix}$ is solvable as $[G, G] = \begin{pmatrix} 1 & 0 & k \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cong k$ lies in the center of G.

(3) 构造: 满的环同态 $\varphi : R \to R'$, 其中 R 是整环, 但 R' 不是整环.

Construct a surjective homomorphism $\varphi : R \to R'$ of rings in which R is an integral domain and but R' is not an integral domain.

例子 $\varphi : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ is surjective yet $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain.

(4) 给出: 群 G 及子群 H 和 K, 满足 K 是 H 的正规子群, H 是 G 的正规子群, 但 K 不是 G 的正规子群.

Give an example of a group G with subgroups H and K, s.t. K is a normal subgroup of H and H is a normal subgroup of G, but K is not a normal subgroup of G.

例子 Consider $G = D_8$, $H = \langle s, r^2 \rangle$, $K = \langle s \rangle$, then $[G : H] = [H : K] = 2$, hence H is normal in G and K is normal in H. On the other hand, $rsr^{-1} = r^2 s$, which implies that K is not normal in G.

(5) 给出: 群 G 及两个正规子群 H_1 和 H_2, 满足 $H_1 \cong H_2$, 但 $G/H_1 \ncong G/H_2$ 的例子.

Give an example of a group G and two normal subgroups H_1 and H_2 such that $H_1 \cong H_2$ but $G/H_1 \ncong G/H_2$.

例子 Take $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $H_1 = \langle (1, 0) \rangle$ and $H_2 = \langle (0, 2) \rangle$ be subgroups of G. Then $H_1 \cong \mathbb{Z}/2\mathbb{Z} \cong H_2$. Yet we have $G/H_1 \cong \mathbb{Z}/4\mathbb{Z}$ and $G/H_2 \cong \mathbb{Z}/2\mathbb{Z} \times 2\mathbb{Z}/4\mathbb{Z}$; they are not isomorphic.

证明题一 (8 分) 令 G 是群, 使得 "对角子群" $\Delta = \{(g,g) \mid g \in G\}$ 是 $G \times G$ 的正规子群. 求证: G 是交换群.

Let G be a group for which the "diagonal subgroup" $\Delta = \{(g,g) \mid g \in G\}$ is a normal subgroup of $G \times G$. Show that G is commutative.

证明. For $g \in G$, then the normality of Δ implies that $(1,x)(g,g)(1,x)^{-1} \in \Delta$ for every $x \in G$, hence $xgx^{-1} = g$ for every $x \in G$. $\square$

证明题二 (15 分)

令 R 是交换环, e 是 R 的幂等元, 即 $e^2 = e$.

(1) 证明: 对任意的 $x \in I = Re$, 则有 $ex = x$. 同样地, 对所有 $y \in J = R(1-e)$, 则有 $(1-e)y = y$.

(2) 证明: $I + J = R$, 并且 $I \cap J = (0)$.

(3) 证明: 存在环同构 $R \cong R/(I) \times R/(J)$.

Let R be a commutative rings and let e be an *idempotent* element of R, i.e. $e^2 = e$.

(1) Show that for every element $x \in I = Re$, we have $ex = x$. Similarly, for every element $y \in J = R(1-e)$, we have $(1-e)y = y$.

(2) Show that $I + J = R$ and $I \cap J = (0)$.

(3) Show that, as rings, we have $R \cong R/(I) \times R/(J)$.

证明. (1)For $x \in I$, write x as $x = re$, then $ex = ere = ree = re^2 = re = x$. Noticed that $(1-e)^2 = 1 - e - e + e^2 = 1 - e$ is also an idempotent, hence $(1-e)y = y$ holds for every $y \in J$.

(2) $1 = e + (1-e) \in I + J$, hence $I + J = R$. Noticed that $e(1-e) = e - e^2 = 0$. If $x \in I \cap J$, then $ex = (1-e)x = x$, hence $x = e(1-e)x = 0$.

(3) This follows from the Chinese reminder theorem. □

证明题三 (15 分)

令 $D_{2n} = \langle r, s \mid r^n = s^2 = 1 \rangle$ 是 $2n$ 阶的二面体群.

(1) 证明: 若 φ 是 D_{2n} 的自同构, 则 $\varphi(r) = r^a$, 其中 a 是整数, 且 $(a, n) = 1$, 而 $\varphi(s) = r^b s$, 其中 b 是整数.

(2) 反之, 对于整数 a, b 满足 $(a, n) = 1$, 证明: 存在唯一 D_{2n} 的自同构 φ, 满足 $\varphi(r) = r^a$ 且 $\varphi(s) = r^b s$.

Let $D_{2n} = \langle r, s \mid r^n = s^2 = 1 \rangle$ be the dihedral group of order $2n$.

Let $D_{2n} = \langle r, s \mid r^n = s^2 = 1 \rangle$ be the dihedral group of order $2n$.

(1) Show that if φ is a automorphism of D_{2n}, then $\varphi(r) = r^a$ for some integer a such that $(a, n) = 1$ and $\varphi(s) = r^b s$ for some integer b.

(2) Conversely, given a pair of integer a, b such that $(a, n) = 1$, show that there is a unique automorphism φ of D_{2n} such that $\varphi(r) = r^a$ and $\varphi(s) = r^b s$.

证明. (1) Noticed that we always assume $n > 2$ when talking about the dihedral groups, then r^a, where $(a, n) = 1$ are the only elements of order n in D_{2n}. For $\varphi \in \mathrm{Aut}(D_{2n})$, it must map an element of order n to an element of order n; this gives the existence of a. On the other hand, suppose $\varphi(s) = r^b$, then $\varphi(D_{2n}) \subset \langle r \rangle \subsetneqq D_{2n}$, contradicting the fact that φ is an automorphism. Hence $\varphi(s) = r^b s$.

(2) For existence, we only need to verify that $\varphi(r)^n = \varphi(s)^2 = 1$ and $\varphi(s)\varphi(r)\varphi(s) = \varphi(r)^{-1}$. The uniqueness is obvious.

$\square$

证明题四 (7 分)

若 H 和 K 都是群 G 的正规子群, 使得 G/H 和 G/K 都是可解的.

证明: $G/(H \cap K)$ 是可解的.

(提示: $G/(H \cap K)$ 存在同构于 G/H 的商群)

Suppose that H and K are both normal subgroups of a group G and such that G/H and G/K are both solvable.

Prove that $G/(H \cap K)$ is solvable.

(Hint: $G/(H \cap K)$ admits a quotient that is isomorphic to G/H.)

证明. We have a natural homomorphism $\varphi : G/(H \cap K) \to G/H$, which is clearly surjective. The kernel of φ is $H/(H \cap K) \cong HK/K$ by second isomorphic theorem. This is a subgroup of G/K, so $H/(H \cap K)$ is a solvable group. On the other hand, $G/\ker\varphi \cong G/H$ is also a solvable group. Putting these two together, we deduce that G is solvable. $\square$

证明题五 (10 分)

证明: 所有 $5 \cdot 7 \cdot 47$ 阶群一定是交换且循环的.

Show that every group of order $5 \cdot 7 \cdot 47$ is abelian and cyclic.

证明. By Sylow's third theorem, the number of sylow 5, 7 and 47 is 1. Hence a group of order $5 \cdot 7 \cdot 47$ must contain normal subgroups P_1, P_2, P_3, where $|P_1| = 5$, $|P_2| = 7$ and $|P_3| = 47$. Therefore $G = P_1 \times P_2 \times P_3$. $\square$

证明题六 (5 分)

回忆群 G 的交换子群 $[G,G]$ 是被交换化子 $a^{-1}b^{-1}ab$, 其中 $a,b\in G$, 生成的子群. 一般来说, 并非所有 $[G,G]$ 中的元素都形如交换化子. 我们举一个 Derek Holt 在 MathOverflow 问题 7811 中给出的例子.

令 p 是素数, n 是正整数. 考虑由 a_i $(1\le i\le n)$ 生成的群 G, 其中

- $a_i^p=1$ 对所有 i 成立.
- 对所有 $1\le i<j\le n$, 交换化子 $b_{ij}=a_i^{-1}a_j^{-1}a_ia_j$ 是 G 的中心元, 且 $b_{ij}^p=1$.

请证明以下陈述:

(1) 交换子群 $[G,G]$ 的阶为 $p^{n(n-1)/2}$, 且被 b_{ij} 生成.

(2) 另一方面, 形如 $[x,y]$ 的元素, 其中 $x,y\in G$, 至多只有 p^{2n} 个.

(3) 综上所述, 固定 $k>0$, 当 n 充分大时, 存在群 G, 使得 $[G,G]$ 中的元素并非全部形如至多 k 个交换化子的乘积.

Recall that the commutator subgroup $[G,G]$ of a group G is generated by the commutators $a^{-1}b^{-1}ab$ for $a,b\in G$. It is not true in general that every element in $[G,G]$ is of the form of a commutator. We will work out an example following MathOverflow question number7811, due to Derek Holt.

Let p be a prime number and $n\in N$. Consider a group G generated by elements a_i $(1\le i\le n)$, such that

- $a_i^p=1$ for every i,
- for $1\le i<j\le n$, the commutator $b_{ij}=a_i^{-1}a_j^{-1}a_ia_j$ is central in G, and satisfies $b_{ij}^p=1$.

Prove the following statements:

(1) The commutator subgroup $[G,G]$ has order $p^{n(n-1)/2}$ and is generated by b_{ij}.

(2) On the other hand, show that elements of the form $[x,y]$ with $x,y\in G$ can have at most p^{2n} elements.

(3) Deduce from this that for any fixed $k>0$, by choosing n sufficiently large, we can find G such that not all elements of $[G,G]$ are products of at most k commutators.

证明. (1) For $g\in G$, we have $[a_ig,a_j]=g^{-1}a_i^{-1}a_j^{-1}a_iga_j=g^{-1}b_{ij}a_j^{-1}ga_j=$. Since b_{ij} is central, then $[a_ig,a_j]=[a_i,a_j][g,a_j]$. a_i generates G, hence $[gg',a_j]=[g,a_j][g',a_j]$ for all $g,g'\in G$, $1\le j\le n$, and every $[g,a_j]$ is also central. Similary, we have $[g,g'g'']=[g,g'][g,g'']$ for every $g,g',g''\in G$ and every $[g,g']$ is central. Specifically, we know that b_{ij} generate $[G,G]$. Noticed that $b_{ij}^{-1}=b_{ji}$ is the only relation between b_{ij}, hence $[G,G]$ is of order $p^{n(n-1)/2}$.

(2) Suppos $x = a_{i_1}^{n_1} a_{i_2}^{n_2} \dots a_{i_s}^{n_s}$ and $y = a_{j_1}^{n_1} a_{j_2}^{n_2} \dots a_{j_t}^{m_t}$, then $[x, y] = \prod_{\substack{1 \le p \le s \\ 1 \le q \le t}} [a_{i_p}, a_{j_q}]^{n_p m_q} = \prod_{\substack{1 \le i \le n \\ 1 \le j \le n}} b_{ij}^{g_{ij}}$, where $g_{ij} = \sum_{\substack{i_p = i \\ j_q = q}} n_p m_q$. Hence the times b_{ij} occurs in $[x, y]$ only depends on the times a_i, a_j occurs in x and y. And since $a_i^p = 1$, $[x, y]$ only depends on $\sum_{i = i_p} n_p \mathrm{mod} p$, hence the elemets of form $[x, y]$ can have at most p^{2n} elements.

(3) Clearly, from (1) and (2).

$\square$