AI for Math 数学形式化抽象代数期末考试

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) (15 分)

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

1. 对群 G 的子群 H, 若 H 的中心化子是整个 G, 则 H 是 G 的中心的子群.

Let H be a subgroup of G. If the centralizer of H is the entire group G, then H is a subgroup of the center of G.

True. If the centralizer of H is the entire group G, then every element of H commutes every element of G. So H is contained in the center of G.

2. 循环群 $\mathbf{Z}_6$ 包含同构于 $\mathbf{Z}_3$ 的子群.

The cyclic group $\mathbf{Z}_6$ contains a subgroup isomorphic to $\mathbf{Z}_3$.

True. The subgroup $\langle 2 \rangle$ of $\mathbf{Z}_6$ is isomorphic to $\mathbf{Z}_3$.

3. 若 a 是群 G 的元素, 则它的交换化子 $C_G(a)$ 是交换群.

If a is an element of a group G, then its centralizer $C_G(a)$ is an abelian group.

False. If a lies in the center of G, then $C_G(a)$ is the entire group G. No reason for $C_G(a)$ to be abelian.

4. 若 G 是 256 阶的群, 则 G 是可解的.

Let G be a group of order 256. Then G is a solvable group.

True. G is a 2-group. All p-groups are nilpotent, so are solvable.

5. 若 K 是 H 的特征子群, H 是 K 的特征子群, 则 K 是 G 的特征子群. 这里, 一个子群 H 被称作是特征的, 若对 G 的任意自同构 σ, 都有 $\sigma(H) = H$.

Let K be a characteristic subgroup H and H be a characteristic subgroup of G. Then K is a characteristic subgroup G. Recall that a subgroup H is *characteristic* if for any automorphism σ of G, $\sigma(H) = H$.

True.

6. 一个无扭 $\mathbf{Z}$-模是自由的.

A torsion free $\mathbf{Z}$-module is free.

False. $\mathbf{Q}$ is not a free $\mathbf{Z}$.

7. 若 G 是群, H 和 K 是其正规子群, 则 HK 也是 G 的正规子群.

Let G be a group and H and K be its normal subgroup. Then HK is a normal subgroup of G.

True.

8. 令 $\varphi(n)$ 是 Euler φ-函数, 则 $\varphi(p^5) = p^4(p-1)$.

Let $\varphi(n)$ be the Euler φ-function. Then $\varphi(p^5) = p^4(p-1)$.

False. Since we don't know if p is a prime.

9. 域是主理想整环.

Field is a PID.

True.

10. 次数为 n 的多项式 $f(x)$ 的分裂域 E/F 的扩张次数至多为 $n!$.

The dimension of a splitting field E/F of a polynomial $f(x)$ of degree n is at most $n!$.

True.

11. $X^3 - X + 1$ 在模 3 后是可约的多项式.

$X^3 - X + 1$ reduces modulo 3 to a reducible polynomial.

False. It is irreducible since it has no roots modulo 3.

12. 一个判别式 $d = 0$ 的三次实多项式有三个不同的实根.

A cubic real polynomial with discrimiant $d = 0$ has three distinct real roots.

False. It has multiple roots.

13. $\mathbf{Q}$ 的域扩张 $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ 不是本源的.

The extension $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbf{Q}$ is not primitive.

False. It is primitive since it is an extension of char. 0 field.

14. 令 R 是含幺环, 则所有自由 R-模都有基.

Let R be a ring with unit. Every free R-module has a base.

False. It is true if the ring R has the invariant base property.

15. 令 R 是环, I 是 R 的理想, 则 I 是 R-模.

Let R be a ring and I be an ideal of R. Then I is a R-module.

True.

Grading table

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

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

(1) 令 H 是 G 的正规子群, $\pi : G \to G/H$ 是自然同态. 若 $\phi : G \to K$ 是同态, 且 "分解经过" π, 即存在映射 $\psi : G/H \to K$ 满足 $\phi = \psi \circ \pi$. 求证 ψ 是群同态.

Let H be a normal subgroup of G and $\pi : G \to G/H$ the natural homomorphism. Suppose further that $\phi : G \to K$ is a homomorphism such that the map ϕ "factors through" π, namely, there exists a map $\psi : G/H \to K$ such that $\phi = \psi \circ \pi$. Prove that ψ is a homomorphism of groups.

证明. Every element of G/H takes the form of gH for some $g \in G$. We verify that ψ is a homomorphism as follows: for $g_1, g_2 \in G$

$$\psi(g_1H)\cdot\psi(g_2H) = \psi(\pi(g_1)\cdot\psi(\pi(g_2)) = \phi(g_1)\cdot\phi(g_2) = \phi(g_1g_2) = \psi(\pi(g_1g_2)) = \psi(g_1g_2H) = \psi(g_1H\cdot g_2H).$$

□

(2) 令 G 是阶至少为 3 的有限群, (即 $|G| \geq 3$). 求证 G 包含至少 3 个不同的共轭类.

注意, 上述陈述对于无限群不成立. 也就是说, 存在只包含两个共轭类的无限群.

Let G be a finite group of order at least 3, (i.e., $|G| \geq 3$). Show that G has at least 3 distinct conjugacy classes.

Remark that this statement is not true for infinite groups. That is, there exist infinite groups with exactly two conjugacy classes.

证明. By $|G| \geq 3$, G contains at least two conjugacy classes. Assume that G has exactly two conjugacy classes. Then G is non-abelian and $|Z(G)| = 1$. By the Class equation, we have $|G| = |Z(G)| + |G|/|C_G(x)|$ for some $x \notin Z(G)$. Thus $|G| - 1 = |G|/|C_G(x)|$ forces $|G| = 2$, a contradiction.

□

(3) 请证明, 若 N 是有限群 G 的正规子群, 且 $(|N|, |G|/|N|) = 1$, 则 N 是 G 的特征子群.

Prove that if N is a normal subgroup of the finite group G and $(|N|, |G|/|N|) = 1$ then N is a characteristic subgroup of G.

证明. We show that N is the unique subgroup of G of order $|N|$.

Let H be a subgroup of G of order $|H| = |N|$. Since N is a normal subgroup, NH is a subgroup of order $|N|^2/|N \cap H|$. By the Lagrange Theorem, $|NH| = |N|^2/|N \cap H|$ divides $|G|$. By $(|N|, |G|/|N|) = 1$, we have $|N \cap H| = |N|$. Thus $H = N$ and N is the unique subgroup of G order $|N|$, so is characteristic. □

(4) 请求出自由 $\mathbf{Z}$-模 $\mathbf{Z}^{(3)}$ 中由 $f_1 = (1, 0, -1)$, $f_2 = (2, -3, 1)$, $f_3 = (0, 3, 1)$ 和 $f_4 = (3, 1, 5)$ 生成的子模的基.

Find a base for the submodule of the free $\mathbf{Z}$-module $\mathbf{Z}^{(3)}$ generated by $f_1 = (1, 0, -1)$, $f_2 = (2, -3, 1)$, $f_3 = (0, 3, 1)$ and $f_4 = (3, 1, 5)$.

证明. $f_2 - 2f_1 = (0, -3, 3)$, $f_4 - 3f_1 = (0, 1, 8)$, $(0, -3, 3) - 3f_3 = (0, -12, 0)$, $(0, 1, 8) - 8f_3 = (0, -23, 0)$. $(0, -23, 0) - 2(0, -12, 0) = (0, 1, 0)$, $f_3 - 3(0, 1, 0) = (0, 0, 1)$, $f_1 + (0, 0, 1) = (1, 0, 0)$, hence $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$ are generated by f_1, f_2, f_3, and f_4, that is, the submodule generated by f_1, f_2, f_3, and f_4 is precisely $\mathbf{Z}^{(3)}$. □

举例 Examples (4 分 $\times 5 = 20$ 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) 给出一个群 G, 使得 $G \times G$ 的子群不止有 $\{(e,e)\}$, $\{e\} \times G$, $G \times \{e\}$, 和 $G \times G$.

Give an example of a group G such that $G \times G$ contains a subgroup other than $\{(e,e)\}$, $\{e\} \times G$, $G \times \{e\}$, and $G \times G$.

例子 $G = \mathbf{Z}/2\mathbf{Z}$.

(2) 给出一个有限非交换群 G 的例子, 使得 G 的所有子群都是正规子群.

Give an example of a finite non-abelian group G such that every subgroup of G is a normal subgroup.

例子 Q_8.

(3) 给出一个是唯一分解整环但不是主理想整环的环的例子.

Give an example of UFD which is not PID.

例子 $\mathbf{Z}[X]$

(4) 给出一个扭 $\mathbf{Z}$-模的例子.

Give an example of torsion $\mathbf{Z}$-module.

例子 $\mathbf{Z}/6\mathbf{Z}$.

(5) 给出一个 Galois 扩张, 使得其 Galois 群同构于 $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

Give an example of Galois extension whose Galois group is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

例子 $\mathbf{Q}(\sqrt[8]{1}, \sqrt{2})$ over $\mathbf{Q}$.

证明题一 (15 分) 分类所有的 50 阶群.

Classify groups of order 50.

证明. An abelian group of order 50 is isomorphic to $\mathbb{Z}_{50}$ or $\mathbb{Z}_{10} \times \mathbb{Z}_5$.

Assume that G is a non-abelian group of order 50. By Sylow Theorem, G has a normal Sylow 5-subgroup, denoted by P of order 25. Let Q be a Sylow 2-subgroup. Then $P \cong \mathbb{Z}_{25}$ or $\mathbb{Z}_5 \times \mathbb{Z}_5$, and

$$\mathrm{Aut}(P) \cong \mathbb{Z}_{25}^{\times} = \langle 2 \rangle \cong \mathbb{Z}_{20}, \text{ or } \mathrm{GL}_2(\mathbb{Z}_5).$$

Assume that $P \cong \mathbb{Z}_{25}$. Then $\mathrm{Aut}(P)$ has a unique subgroup of order 2, which is $\{1, 2^{10} = 24 = -1\}$. Take $\varphi\colon Q \to \mathrm{Aut}(P)$ such that $\varphi(Q) = \langle -1 \rangle$. Then $G \cong \mathbb{Z}_{25} \rtimes_{\varphi} \mathbb{Z}_2 \cong D_{50}$.

Assume that $P \cong \mathbb{Z}_5 \times \mathbb{Z}_5$. Since all elements of order 2 in $\mathrm{GL}_2(\mathbb{Z}_5)$ are conjugate to $-I_2$ and $\mathrm{diag}\{1, -1\}$. Define $\varphi_i\colon Q \to \mathrm{GL}_2(\mathbb{Z}_5)$ by $\varphi_1(Q) = \langle -I_2 \rangle$ and $\varphi_2(Q) = \langle \mathrm{diag}\{1, -1\} \rangle$. Then there are two non-isomorphism groups of order 50,

$$(\mathbb{Z}_5 \times \mathbb{Z}_5) \rtimes_{\varphi_1} \mathbb{Z}_2 \cong \langle a, b, s\colon a^5 = b^5 = s^2 = 1, ab = ba, sa = a^{-1}s, sb = b^{-1}s \rangle.$$

and

$$(\mathbb{Z}_5 \times \mathbb{Z}_5) \rtimes_{\varphi_2} \mathbb{Z}_2 \cong \mathbb{Z}_5 \times D_{10}.$$

□

证明题二 (15 分) 令 $\xi = e^{2i\pi/15} \in \mathbf{C}$.

(1) 找出 ξ^3 在 $\mathbf{Q}$ 上的极小多项式.

(2) 求出 $\mathrm{Gal}(\mathbf{Q}(\xi)/\mathbf{Q})$.

(3) 找出满足 $[F : \mathbf{Q}] = 2$ 的 $\mathbf{Q}(\xi)$ 的子域 F 的数量.

(4) 是否存在 4 次多项式 $P(X) \in \mathbf{Q}[X]$, 使得 $\mathbf{Q}(\xi)$ 是 $P(X)$ 在 $\mathbf{Q}$ 上的分裂域?

Let $\xi = e^{2i\pi/15} \in \mathbf{C}$.

(1) Find the minimal polynomial of ξ^3 over $\mathbf{Q}$.

(2) Determine $\mathrm{Gal}(\mathbf{Q}(\xi)/\mathbf{Q})$.

(3) Find the number of subfields $F \subset \mathbf{Q}(\xi)$ satisfying $[F : \mathbf{Q}] = 2$.

(4) Does there exist a polynomial $P(X) \in \mathbf{Q}[X]$ of degree 4 such that $\mathbf{Q}(\xi)$ is the splitting field of $P(X)$ over $\mathbf{Q}$?

证明. (1) Noticed that ξ^3 is a fifth root of unity, its minimal polynomial is the fifth cyclotomic polynomial $X^4 + X^3 + X^2 + X + 1$.

(2) Since ξ is a root of unity, $\mathrm{Gal}(\mathbf{Q}(\xi)/\mathbf{Q}) = \mathbf{Z}_{15}^{\times} \cong \mathbf{Z}_2 \times \mathbf{Z}_4$.

(3) The group $\cong \mathbf{Z}_2 \times \mathbf{Z}_4$ contains 2 subgroups of order 2.

(4) Otherwise $\mathrm{Gal}(\mathbf{Q}(\xi)/\mathbf{Q})$ is a transitive subgroup of S_4. Noticed that the only transitive subgroups of S_4 are S_4, A_4, D_8, $\mathbf{Z}_4$, $\mathbf{Z}_2 \times \mathbf{Z}_2$, non of which is isomorphic to $\mathrm{Gal}(\mathbf{Q}(\xi)/\mathbf{Q})$. □

证明题三 (10 分) 令 $f(X) = X^4 - X^2 - 1 \in \mathbf{Q}[X]$.

(1) 找到 $\mathbf{F}_3[X]$ 中所有的首一 2 次不可约多项式.

(2) 证明 $f(X) \mod 3$ 是 $\mathbf{F}_3[X]$ 中的不可约多项式.

Let $f(X) = X^4 - X^2 - 1 \in \mathbf{Q}[X]$.

(1) Determine all monic irreducible polynomial of degree 2 in $\mathbf{F}_3[X]$.

(2) Prove that $f(X) \mod 3$ is irreducible in $\mathbf{F}_3[X]$.

证明. (1) The monic reducible polynomials are X^2, $X(X-1) = X^2-X$, $X(X+1) = X^2+X$, $(X-1)^2 = X^2+X+1$, $(X+1)(X-1) = X^2-1$, $(X+1)^2 = X^2-X+1$. Hence the monic irreducible polynomials are X^2+1, X^2+X-1, X^2-X-1.

(2) Since $f(X)$ has no root in $\mathbf{F}_3[X]$, if $f(X)$ is reducible, it factors as a product of two monic irreducible polynomials of degree 2. By (1), the product of two monic irreducible polynomials of degree 2 are $(X^2+1)^2 = X^4-X^2+1$, $(X^2+1)(X^2+X-1) = X^4+X^3+X-1$, $(X^2+1)(X^2-X-1) = X^4-X^3-X-1$, $(X^2+X-1)^2 = X^4-X^3-X^2+X+1$, $(X^2+X-1)(X^2-X-1) = X^4+1$, $(X^2-X-1)^2 = X^4+X^3-X^2+X+1$, hence $f(X)$ is irreducible. □

证明题四 (10 分)

假设群 G 在集合 X (可能是无限集) 上作用, H 是群 G 中指数有限的子群. 对 $x \in X$, 用 H_x 和 G_x 分别表示群 H 和 G 在 x 处的稳定子群.

(1) 证明: H 在 X 上有有限个轨道.

(2) 证明: 如果群 H 在 X 上的作用是传递的, 且对某 $x \in X$ 有 $H_x = G_x$, 则 $H = G$.

(3) 证明: 如果 H 是一个正规子群, 则指数 $[G_x : H_x]$ (不管有限与否) 不依赖于 x 的选取.

Suppose that G is a group acting transitively on a set X (which may be infinite) and that H is a finite index subgroup of G. For $x \in X$, write H_x and G_x for its stabilizers in H and G, respectively.

(1) Show that H has finitely many orbits on X.

(2) Show that, if the action of H on X is transitive and for some $x \in X$, $H_x = G_x$; then H is all of G.

(3) Show that if H is normal, then $[G_x : H_x]$ (finite or not) is independent of x.

证明. (1) Write G as the union of right cosets of H: $G = Hg_1 \sqcup Hg_2 \sqcup \cdots \sqcup Hg_r$ for some $g_1, \ldots, g_r \in G$ and $r = [G : H]$. Fix $x \in X$. We show that every point $x' \in X$ is in the same H-orbit of at least one of $\{g_1x, g_2x, \ldots, g_rx\}$. Indeed, since G acts transitively on X, $x' = g \cdot x$ for some $g \in G$. In the coset decomposition, $g = hg_i$ for some $i \in \{1, \ldots, r\}$ and $h \in H$. Thus

$$x' = gx = hg_ix$$

lies in the same H-orbit of g_ix. So there are only finitely many H-orbits on X.

(2) We keep the notation as in (1) and assume that x is the chosen point. Suppose that $r > 1$ and hence we may assume that $g_2 \notin H$. Consider the point $g_2x \in X$. By the transitivity of the action of H, $g_2x = hx$ for some $h \in H$. Thus, $h^{-1}g_2x = x$. Thus, $h^{-1}g_2 \in G_x = H_x$. This in particular implies that $g_2 \in H$, contradicting our earlier assumption. So $H = G$.

(3) Once again, keep the notation as in (1). For $x' = gx$ for some $g \in G$, we note that $G_{x'} = gG_xg^{-1}$; indeed,

$$h \in G_{x'} \Leftrightarrow hx' = x' \Leftrightarrow hgx = gx \Leftrightarrow g^{-1}hgx = x \Leftrightarrow g^{-1}hg \in G_x \Leftrightarrow h \in gG_xg^{-1}.$$

Similarly, as H is normal,

$$H_{x'} = gG_xg^{-1} \cap H = gG_xg^{-1} \cap gHg^{-1} = g(G_x \cap H)g^{-1} = gH_xg^{-1}.$$

There is obviously a one-to-one correspondence between G_x/H_x and gG_xg^{-1}/gH_xg^{-1}, sending aH_x to $gag^{-1} \cdot gH_xg^{-1}$. In particular, $[G_x : H_x] = [G_{x'} : H_{x'}]$ and therefore, $[G_x : H_x]$ is independent of x. $\square$

证明题五 (10 分) 令 $f(X) = X^4 - X^2 - 1 \in \mathbf{Q}[X]$.

(1) 求出 $\mathrm{Gal}(K/\mathbf{Q})$, 这里 K 是 f 在 $\mathbf{Q}$ 上的分裂域. (回忆: 若 $f(X) = X^4 + bX^3 + cX^2 + dX + e$, 则其三次预解式为 $g = X^3 - cX^2 + (bd - 4c)X - b^2e + 4ce - d^2$.)

(2) 求出 $K/\mathbf{Q}$ 全部中间域的数量 (包含 K 和 $\mathbf{Q}$).

Let $f(X) = X^4 - X^2 - 1 \in \mathbf{Q}[X]$.

(1) Determine $\mathrm{Gal}(K/\mathbf{Q})$, where K is the splitting field of f over $\mathbf{Q}$. (Recall: if $f(X) = X^4 + bX^3 + cX^2 + dX + e$, then its cubic resolvent is $g = X^3 - cX^2 + (bd - 4c)X - b^2e + 4ce - d^2$.)

(2) Count the number of intermediate fields of $K/\mathbf{Q}$ (including K and $\mathbf{Q}$).

证明. (1), Let $\alpha = \sqrt{\frac{1+\sqrt{5}}{2}}$, then α, $-\alpha$, $i\alpha^{-1}$, and $-i\alpha^{-1}$ are all roots of $f(X)$, hence $K = \mathbf{Q}(\alpha, i)$. Notice that $K/\mathbf{Q}(i)$ is a Galois extension of degree 4, then $[K : \mathbf{Q}] = 8$. Recall that the Galois groups of a quartic polynomial can only be S_4, A_4, D_8, Z_4 or $\mathrm{Z}_2 \times \mathrm{Z}_2$, hence $\mathrm{Gal}(K/\mathbf{Q}) = D_8$.

(2), The number of subgroups of D_8 is 10. □