2022 秋: 代数学一 (实验班) 期末考试版本B

时间：120 分钟　　满分：110 分，最高得分不超过 100 分

所有的环都有乘法单位元, 且与其加法单位元不相等; 所有环同态把 1 映到 1.

All rings contain 1_R and $1_R \neq 0_R$; all ring homomorphisms take 1 to 1.

判断题 请在答卷纸上整齐编号书写 T 或 F (10 分)

1. 一个有限单群的一维复表示一定是平凡的.

The only one-dimensional representation over $\mathbb{C}$ of a finite simple group is the trivial representation.

2. 设群 G 作用在集合 X 上. 如果 $g_1, g_2 \in G$ 和元素 $x \in X$ 满足 $g_1 \cdot x = g_2 \cdot x$, 那么 $g_1 = g_2$.

Let G be a group acting on a set X. If $g_1, g_2 \in G$ and $x \in X$, then $g_1 \cdot x = g_2 \cdot x$ implies $g_1 = g_2$.

3. 设 (ρ, V) 是有限群 G 的有限维不可约复表示且 $g \in Z(G)$ 是群 G 中心中的元素. 则 $\rho(g)$ 是一个纯量矩阵.

Let (ρ, V) be a finite dimensional irreducible representation over $\mathbb{C}$ of a finite group G, and let $g \in Z(G)$ be an element in the center. Then $\rho(g)$ is a scalar matrix.

4. 两个整环的直积还是一个整环.

The direct product of two integral domains is again an integral domain.

5. 若 P_1 和 P_2 是一个交换环 R 的两个素理想, 则 $P_1 + P_2$ 也是 R 的一个素理想.

If P_1 and P_2 are prime ideals in a commutative ring R, then $P_1 + P_2$ is a prime ideal.

6. 特征为 0 的域 F 的有限域扩张 K 一定可以由某个元素 $\alpha \in K$ 生成.

A finite extension K of a field F of characteristic zero can be generated by some element $\alpha \in K$.

7. 设 F 是一个域，$f(x), g(x) \in F[x]$ 是两个次数相同的不同的首一不可约多项式. 则 $f(x)$ 和 $g(x)$ 的分裂域不同构.

Let F be a field and $f(x), g(x) \in F[x]$ be two distinct irreducible monic polynomials of the same degree, then the splitting fields of $f(x)$ and $g(x)$ are not isomorphic.

8. 设 F 是一个域, E 是一个 F 的二次扩张. 则这个域扩张 E/F 是伽罗华的.

Let F be a field and E an extension of F of degree 2. Then E is a Galois extension of F.

9. 令 F 是一个特征为 $p>0$ 的域，并设 $f(x)$ 是一个 $F[x]$ 中次数与 p 互素的不可约多项式. 那么多项式 $f(x)$ 是可分的.

Let F be a field of positive characteristic $p>0$. Let $f(x)$ be an irreducible polynomial in $F[x]$ with degree relatively prime to p. Then $f(x)$ is separable.

10. 设 $K/E/F$ 是有限扩张塔. 若 E/F 是可分的, $x\in K$ 是一个元素在 E 上可分. 则 x 在 F 上可分.

Let $K/E/F$ be finite field extensions. Suppose that E/F is separable and an element $x\in K$ is separable over E. Then x is separable over F.

解答题一 (10 分) 证明：每个有限群都同构于某个交错群 A_n 的子群.

Prove that every finite group is isomorphic to a subgroup of an alternating group A_n for some n.

解答题二 (15 分) 决定多项式 x^6+3 在 $\mathbb{Q}$ 上的伽罗华群.

Determine the Galois group of the polynomial x^6+3 over $\mathbb{Q}$.

解答题三 (10 分) 设 $f(x)\in K[x]$ 是一个 n 次不可约多项式. 假设 L/K 是一个 m 次的域扩张. 若 m 与 n 互素, 证明：$f(x)$ 在 $L[x]$ 中也不可约.

Suppose $f(x)\in K[x]$ is an irreducible polynomial of degree n over the field K. Suppose that L/K is a field extension with finite degree $[L:K]=m$. If m and n are relatively prime, prove that $f(x)$ is irreducible in $L[x]$.

解答题四 (15 分) 令 G 为一有限群, p 为一素数. 假设 H 是 G 某个西罗 p-子群的一个子群. 证明: 若 $f(H)$ 记录包含 H 的西罗 p-子群的个数, 则 $f(H)\equiv 1 \bmod p$.

Let G be a finite group and fix a prime number p. Assume that H is a subgroup of G contained in some Sylow p-subgroup of G. If $f(H)$ denotes the number of Sylow p-subgroups of G containing H, then $f(H)\equiv 1 \bmod p$.

解答题五 (15 分) 令 $\omega=e^{2\pi i/3}$ 为一个三次本原单位根.

(1) 证明 $R=\mathbb{Z}[\omega]=\{a+b\omega\,|\,a,b\in\mathbb{Z}\}$ 是一个欧几里得整环，所对应的模函数 $N: R\to\mathbb{Z}$ 为 $N(a+b\omega)=(a+b\omega)(a+b\omega^2)\in\mathbb{Z}$.

(2) 证明：若 π 是一个 R 中的素元, 则 $N(\pi)$ 是一个素数或者是一个素数的平方.

(3) 证明：若一个素数 $p\equiv 1 \bmod 3$, 那么存在整数 $a,b\in\mathbb{Z}$ 使得 $p=a^2+ab+b^2$.

Let $\omega=e^{2\pi i/3}$ be a primitive third root of unity.

(1) Show that $R=\mathbb{Z}[\omega]=\{a+b\omega\,|\,a,b\in\mathbb{Z}\}$ is an Euclidean domain, with norm $N:R\to\mathbb{Z}$ given by $N(a+b\omega)=(a+b\omega)(a+b\omega^2)\in\mathbb{Z}$.

(2) Show that, if π is a prime element in R, then $N(\pi)$ is either a prime or a square of a prime.

(3) Show that if a prime $p \equiv 1 \bmod 3$, then there exist integers $a, b \in \mathbb{Z}$ such that $p = a^2 + ab + b^2$.

解答题六 (15 分) 设 G 是一个阿贝尔群，它由 n 个元素生成. 证明每个 G 的子群也可以被最多 n 个元素生成.

Let G be an abelian group, generated by at most n elements. Prove that each subgroup of G can be generated by at most n elements.

解答题七 (10 分) 在此问题中，我们构造一个有理系数多项式使得它的伽罗华群是 S_5.

(1) 证明：如果 K 是一个五次有理系数不可约多项式 $f(x) \in \mathbb{Q}[x]$ 的分裂域, 记 $f(x)$ 在 K 中的零点为 $\{\alpha_1, \ldots, \alpha_5\}$. 证明: 如果 $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \neq K$, 那么 $\mathrm{Gal}(K/\mathbb{Q}) \cong S_5$.

(2) 构造一个不可约五次有理系数多项式 $f(x) \in \mathbb{Q}[x]$ 使得它只有三个实根，并以此证明这个多项式 $f(x)$ 在 $\mathbb{Q}$ 上的伽罗华群是 S_5.

In this problem, we construct explicitly a polynomial in $\mathbb{Q}[x]$ with Galois group S_5.

(1) Let K be the splitting field of a irreducible quintic polynomial $f(x) \in \mathbb{Q}[x]$ and let $\{\alpha_1, \ldots, \alpha_5\}$ be zeros of $f(x)$ in K. Show that if $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \neq K$, then $\mathrm{Gal}(K/\mathbb{Q}) \cong S_5$.

(2) Give an irreducible quintic polynomial $f(x) \in \mathbb{Q}[x]$ with only three real zeros and show that the Galois group of $f(x)$ is isomorphic to S_5.

解答题八 (10 分) 令 K 是域 F 的有限伽罗华扩张，它的伽罗华群是 $G = \mathrm{Gal}(K/F)$. 假设有一个 K/F 的中间域 $E \neq F$ 使得任何一个中间域 $E' \neq F$, 都有$E \subseteq E'$. 证明：G 是一个循环群且它的阶是素数的幂次.

Let K be a finite Galois extension of F with Galois group $G = \mathrm{Gal}(K/F)$. Assume that there exists an intermediate field $E \neq F$ between K and F such that for any such intermediate field $E' \neq F$, we have $E \subseteq E'$. Prove that G is a cyclic group whose order is a prime-power.