# 2022 秋: 代数学一 (实验班) 期末考试版本A

**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. 若 $K$ 是域 $F$ 的一个有限伽罗华扩张且相应的伽罗华群是单群, 那么 $K/F$ 没有任何一个中间域 $E$ (除了 $K$ 和 $F$) 使得 $K$ 是 $E$ 的伽罗华扩张.

If the field $K$ is a finite Galois extension of the field $F$ whose Galois group is simple, then there is no intermediate fields $E$ of $K/F$ for which $K$ is Galois over $E$, except $K$ and $F$ themselves.

2. 设 $H$ 是一个 $G$ 的子群. 若 $H$ 的中心化子是整个群 $G$, 那么 $H$ 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 $G$.

3. 每一个 $G_1 \times G_2$ 的子群都是形如 $H_1 \times H_2$, 这里 $H_1 \leq G_1$ 和 $H_2 \leq G_2$ 是相应的子群.

Every subgroup of $G_1 \times G_2$ is of the form $H_1 \times H_2$ for subgroups $H_1 \leq G_1$ and $H_2 \leq G_2$.

4. 设 $p$ 是一个素数, $\alpha$ 是一个自然数. 那么每一个阶为 $2p^\alpha$ 的有限群都是可解的.

Let $p$ be a prime number and $\alpha \in \mathbb{N}$. Then every group of order $2p^\alpha$ is solvable.

5. 设 $\varphi : R \to R'$ 是一个满的环同态，并且假设 $R$ 是一个整环. 则 $R'$ 是一个整环.

Let $\varphi : R \to R'$ be a surjective ring homomorphism, and assume that $R$ is an integral domain. Then $R'$ is an integral domain.

6. 在 $\mathbb{Q}$ 中, $\frac{1}{2}$ 是 2 和 3 的一个最大公约元素.

A gcd of 2 and 3 in $\mathbb{Q}$ is $\frac{1}{2}$.

7. 设 $K$ 是一个 $\mathbb{Q}$ 的包含在某个 $\mathbb{Q}(\mu_n)$ 的域扩张. 那么 $K$ 在 $\mathbb{Q}$ 上的一个伽罗华扩张.

Let $K$ be an extension of $\mathbb{Q}$ that is contained in $\mathbb{Q}(\mu_n)$ for some $n$, then $K$ is Galois over $\mathbb{Q}$.

8. 若 $K$ 是正特征 $p$ 的域 $F$ 的一个有限不可分扩张, 那么对于任何一个元素 $\alpha \in K$, 若它满足 $K = F(\alpha)$, 则 $\alpha$ 的极小多项式可以被写为 $f(x^p)$ 的样子，这里 $f(x) \in F[x]$ 是一个多项式.

If $K$ is a finite inseparable field extension of a field $F$ of characteristic $p > 0$, then for every $\alpha \in K$ satisfying $K = F(\alpha)$, the minimal polynomial of $\alpha$ can be written as $f(x^p)$ for some $f(x) \in F[x]$.

9. 令 $K$ 是有限域 $F$ 的一个 $n$ 次扩张，那么 $K/F$ 的所有中间域的个数 (包括 $K$ 和 $F$) 和 $n$ 的约数的个数相等.

Let $K$ be a finite extension of degree $n$ of a finite field $F$, then the number of intermediate fields between $K$ and $F$ (including $F$ and $K$ themselves) is the same as the (positive) divisors of $n$.

10. 设 $x$ 为一个自由变元. 那么 $\mathbb{Q}(x)$ 是 $\mathbb{Q}(\frac{x^2+1}{x})$ 的一个二次扩张.

Let $x$ be an indeterminate variable. Then $\mathbb{Q}(x)$ is a quadratic extension of $\mathbb{Q}(\frac{x^2+1}{x})$.

**解答题一** (10 分) 令 $G$ 是一个有限群，$K$ 是其正规子群, $P$ 是 $K$ 的一个西罗 $p$-子群 ($p$ 为素数). 证明：$G = KN_G(P)$, 这里 $N_G(P)$ 是 $P$ 在 $G$ 中的正规化子.

Let $G$ be a finite group, $K$ a normal subgroup, and $P$ a $p$-Sylow subgroup of $K$ for some prime $p$. Prove that $G = KN_G(P)$, where $N_G(P)$ is the normalizer of $P$ in $G$.

**解答题二** (15 分) 环 $\mathbb{Z}[x]/(x^3+1,6)$ 中一共有多少个素理想？为什么？ (如果你引用一些定理或者熟知的结论，请清楚地注明，并验证所需的条件。)

How many prime ideals are there in the ring $\mathbb{Z}[x]/(x^3+1,6)$? Why? (If you make use of a known theorem or a well-known result, please state clearly which theorem or result you are using, and please verify the needed conditions.)

**解答题三** (15 分) 设 $n \geq 3$ 是一个无平方因子的整数. 令 $R = \mathbb{Z}[\sqrt{-n}] = \{a + b\sqrt{-n} \mid a, b \in \mathbb{Z}\}$ 是复数域 $\mathbb{C}$ 的子环.

(1) 证明：$\sqrt{-n}$ 和 $1+\sqrt{-n}$ 是 $R$ 中的不可约元.

(2) 证明 $R$ 不是一个唯一分解整环.

(3) 构造一个 $R$ 中的理想使得它不是主理想，并证明之.

Let $n$ be a square-free integer greater than 3. Let $R$ denote the subring $\mathbb{Z}[\sqrt{-n}] = \{a + b\sqrt{-n} \mid a, b \in \mathbb{Z}\}$ of the field of complex numbers $\mathbb{C}$.

(1) Show that $\sqrt{-n}$ and $1+\sqrt{-n}$ are irreducible in $R$.

(2) Prove that $R$ is not a unique factorization domain (UFD).

(3) Construct an ideal in $R$ that is not principal; prove it.

**解答题四** (10 分) 设 $\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n$ 是 $\mathbb{C}$ 中的一列域扩张使得对每个 $i \geq 0$, $K_{i+1}$ 是 $K_i$ 的三次伽罗华扩张. 证明： $\mathbb{Q}(\sqrt[3]{2})$ 不包含在 $K_n$ 中.

Let $\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n$ be a sequence of subfields of $\mathbb{C}$ such that $K_{i+1}$ is Galois over $K_i$ of degree 3 for each $i \geq 0$. Show that $\mathbb{Q}(\sqrt[3]{2})$ is not contained in $K_n$.

**解答题五** (15 分) 令 $p$ 为一个素数且设 $F$ 是一个包含所有 $p$次单位根的域. 令 $K$ 是 $F$ 的伽罗华扩张且伽罗华群为 $\mathbf{Z}_p \times \mathbf{Z}_p$.

(1) 证明：存在两个元素 $\alpha, \beta \in K^{\times}$ 使得 $K = F(\alpha, \beta)$ 且 $a = \alpha^p, b = \beta^p \in F$. (你可以使用Artin的特征线性无关的定理，但如果要使用 Kummer 定理，请证明)

(2) 列出扩张 $K/F$ 的所有的中间域，请写成在 $F(\eta)$ 的形式, 这里 $\eta$ 是 $K$ 中的某个元素. 并给出相应的 $\mathbf{Z}_p \times \mathbf{Z}_p$ 的子群 (给出生成元, 用 $\alpha$ 和 $\beta$ 表示).

Let $p$ be a prime number and let $F$ be a field containing $p$-th roots of unity. Let $K$ be a Galois extension of $F$ with Galois group $\mathbf{Z}_p \times \mathbf{Z}_p$.

(1) Show that there exist two elements $\alpha, \beta \in K^{\times}$ such that $K = F(\alpha, \beta)$ and $a = \alpha^p, b = \beta^p \in F$. (You can use Artin's theorem on independence of characters. But if you want to use Kummer theory, prove it.)

(2) List all intermediate fields between $K$ and $F$ and express each field in the form of $F(\eta)$ for some element $\eta \in K$ in terms of $\alpha$ and $\beta$. Moreover, give the corresponding Galois subgroups, in terms of generators.

**解答题六** (15 分) 设 $p$ 是一个素数, $q$ 为 $p$ 的幂次. 记 $\mathbb{F}_q$ 为有 $q$ 个元素的有限域, $\mathbb{F}_{q^n}$ 为其次数为 $n$ 的有限扩张.

(1) 证明：$q$-Frobenius 元素 $\sigma(x) = x^q$ 是循环群 $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ 的生成元.

(2) 考虑如下的范数映射 $N : \mathbb{F}_{q^n} \to \mathbb{F}_q$

$$N(x) = x\sigma(x)\sigma^2(x)\cdots\sigma^{n-1}(x).$$

证明：$N$ 是满射.

(3) 证明: $N^{-1}(1)$ 作为 $\mathbb{F}_q$-线性空间生成 $\mathbb{F}_{q^n}$.

Let $p$ be a prime integer, and $q$ be a power of $p$. Let $\mathbb{F}_q$ be the finite field with $q$ elements, and $\mathbb{F}_{q^n}$ be the degree $n$ extension of $\mathbb{F}_q$.

(1) Prove that the $q$-Frobenius $\sigma(x) = x^q$ generates $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ as a cyclic group.

(2) Consider the norm map $N : \mathbb{F}_{q^n} \to \mathbb{F}_q$ defined by

$$N(x) = x\sigma(x)\sigma^2(x)\cdots\sigma^{n-1}(x).$$

Prove that $N$ is surjective.

(3) Prove that $N^{-1}(1)$ spans $\mathbb{F}_{q^n}$ as an $\mathbb{F}_q$-vector space.

**解答题七** (10 分) 证明多项式 $x^4 + 1$ 在任何一个正特征域上是可约多项式.

Prove that the polynomial $x^4+1$ is not irreducible over any field of positive characteristic.

**解答题八** (10 分) 令 $F$ 是一个域且 $f(x) \in F[x]$ 是不可约多项式. 设 $K$ 是 $f(x)$ 在 $F$ 上的分裂域并假设存在某个元素 $\alpha \in K$ 使得 $\alpha$ 和 $\alpha + 1$ 都是 $f(x)$ 的根.

(1) 证明：$F$ 不是特征 0 的域.

(2) 证明：存在某个 $K/F$ 的中间域 $E$ 使得 $[K:E]$ 等于 $F$ 的特征.

Let $F$ be a field and let $f(x) \in F[x]$ be an irreducible polynomial. Suppose that $K$ is a splitting field for $f(x)$ over $F$ and assume that there exists an element $\alpha \in K$ such that both $\alpha$ and $\alpha + 1$ are roots of $f(x)$.

(1) Show that the characteristic of $F$ is not zero.

(2) Prove that there exists an intermediate field $E$ between $K$ and $F$ such that $[K:E]$ is equal to the characteristic of $F$.