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	2	3	4	5	6	7	8	9	10
F	T	F	T	F	T	T	T	T	T

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.

False. The statement would be correct if we require no intermediate fields E of K/F for which E is Galois over F, 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.

True. If the centralizer of H is the entire group G, then every element of H commutes with every element of G. This is equivalent to say that H is contained in $Z(G)$.

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 $H_2 \leq G_2$.

False. For example, $G_1 \times G_2 = \mathbf{Z}_2 \times \mathbf{Z}_2$ has a subgroup $\langle (1,1) \rangle$, which is not of the form $H_1 \times H_2$ for $H_i \leq G_i$ $(i = 1, 2)$.

4. 设 p 是一个素数, α 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.

True. When $p = 2$, a 2-group is clearly solvable. When p is odd, This is because the Sylow p-subgroup of G is a normal subgroup and itself is clearly 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.

False. For example, take $R = \mathbb{Z}$ and $R' = \mathbb{Z}/4\mathbb{Z}$, and consider the surjective natural quotient map $\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$.

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 $\frac{1}{2}$.

True. This is correct.

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 $\mathbb{Q}$.

True. The Galois group of $\mathbb{Q}(\mu_n)/\mathbb{Q}$ is abelian and thus any intermediate field 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 α 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 α can be written as $f(x^p)$ for some $f(x) \in F[x]$.

True. Clearly, α cannot be separable over F, as it would then imply that K is separable over F. Thus the minimal polynomial of α is inseparable, and thus is of the form $f(x^p)$ 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.

True. Say $F = \mathbb{F}_q$ and thus $\mathbb{F}_{q^n}$. The correspondence is given by: each divisor d of n corresponds to the extension $\mathbb{F}_{q^d}$ of $\mathbb{F}_q$.

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 $\mathbb{Q}(\frac{x^2+1}{x})$.

True. Setting $z = \frac{x^2+1}{x}$, then we have $x^2 + 1 = xz$. This is an irreducible polynomial of degree 2.

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.

Solution: For each $g \in G$, as K is normal in G, $gKg^{-1} = K$. Thus gPg^{-1} is a Sylow p-subgroup of K. By Sylow's second theorem, gPg^{-1} is conjugate to P by an element of K, namely, there exists $k \in K$ such that $gPg^{-1} = kPk^{-1}$. This implies that $k^{-1}gPg^{-1}k = P$ and thus $k^{-1}g \in N_G(P)$. In other words, $g \in kN_G(P) = KN_G(P)$. This shows that $G = KN_G(P)$.

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.)

Solution: First of all, by Chinese remainder theorem, applied to the ideal (2) and (3) in the quotient ring $\mathbb{Z}[x]/(x^3+1)$ (note that $(2)+(3)=(1)$ is comaximal), we have

$$\mathbb{Z}[x]/(x^3+1,6) \cong \mathbb{Z}[x]/(x^3+1,2) \times \mathbb{Z}[x]/(x^3+1,3) \cong \mathbb{F}_3[x]/(x^3+1) \times \mathbb{F}_2[x]/(x^3+1).$$

It is well-known that prime ideals of a product ring $R_1 \times R_2$ takes the form of $\mathfrak{p}_1 \times R_2$ or $R_1 \times \mathfrak{p}_2$ for prime ideals $\mathfrak{p}_1 \subset R_1$ and $\mathfrak{p}_2 \subset R_2$. (To see this, if $\mathfrak{p} \subseteq R_1 \times R_2$ is a prime ideal, then $(0,1) \times (1,0) \in \mathfrak{p}$, forcing either $(0,1)$ or $(1,0)$ belongs to $\mathfrak{p}$. Without loss of generality, assume that $(1,0) \in \mathfrak{p}$, then $\mathfrak{p}$ takes the form of $R_1 \times I$ for some set I. Note also that, if $a, b \in R$ is such that $ab \in I$, then $(1,a) \times (1,b) \in I$, it would imply that either a or b belongs to I. So I is a prime ideal of R_2. Conversely, for all such ideal $R_1 \times I$, $(R_1 \times R_2)/(R_1 \times I) \cong R_2/I$ is an integral domain.)

So it is enough to find the prime ideals of $\mathbb{F}_3[x]/(x^3+1)$ and of $\mathbb{F}_2[x]/(x^3+1)$, respectively.

For $\mathbb{F}_3[x]/(x^3+1)$, it is isomorphic to $\mathbb{F}_3[x]/(x+1)^3$. The only prime ideal in this ring is $(x+1)$.

For $\mathbb{F}_2[x]/(x^3+1)$, we note that

$$x^3+1 = (x+1)(x^2-x+1)$$

and that both $x+1$ and x^2-x+1 are irreducible and they are relatively prime. It then follows again by Chinese Remainder Theorem that we have an isomorphism

$$\mathbb{F}_2[x]/(x^3+1) \cong \mathbb{F}_2[x]/(x+1) \times \mathbb{F}_2[x]/(x^2-x+1).$$

The latter have two prime ideals.

To sum up, the ring $\mathbb{Z}[x]/(x^3+1,6)$ has three prime ideals.

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

Solution: Consider the norm map $N : R \to \mathbb{Z}$ given by

$$N(a + b\sqrt{-n}) = (a + b\sqrt{-n})(a - b\sqrt{-n}) = a^2 + nb^2.$$

It is multiplicative.

We directly observe that, for $x = a + b\sqrt{-n}$, $N(x) = a^2 + nb^2 = 1$ if and only if $a = \pm 1$ and $b = 0$, namely, $N(x) = 1$ if and only if $x = \pm 1$. In particular, if $N(x) = 1$, then x is a unit in R.

Moreover, we point out that, for any positive integer $d \in (1, n)$, there is no $x \in R$ with norm d, unless d is a square and in this case $x = \pm\sqrt{d}$. This is because when solving $a^2 + nb^2 = d$ with $d < n$, we can only have $b = 0$. Thus either d is not a square, in which case, there is no such x, or d is a square, in which case, $x = \pm\sqrt{d}$.

(1) Suppose $\sqrt{-n} = xy$ for $x, y \in R$ non-unit. Then, we must have

$$N(x)N(y) = N(xy) = N(\sqrt{-n}) = n.$$

Yet, n is square free, $N(x)$ and $N(y)$ are integers between 1 and n. By the discussion above, there is no such x or y in R. Contradiction. So $\sqrt{-n}$ is irreducible.

Similarly, suppose $1 + \sqrt{-n} = xy$ for $x, y \in R$. Then

$$N(x)N(y) = N(xy) = N(1 + \sqrt{-n}) = 1 + n$$

Again, $N(x)$ and $N(y)$ are integers between 1 and n. The only possibility is that $x = \pm d$ for some integer $d \in (1, \sqrt{n})$ such that $d^2 | n + 1$. But then it would follow that $y = \pm\frac{n+1}{d} \notin R$.

(2) If n is even, then

$$n = 2 \cdot \frac{n}{2} = \sqrt{-n} \cdot (-\sqrt{-n}).$$

This will certainly give two different factorizations of n in R, as $\sqrt{-n}$ is irreducible as proved, yet not equal to any factors of 2 or $\frac{n}{2}$.

If n is odd, then

$$n+1 = 2 \cdot \frac{n+1}{2} = (1+\sqrt{-n})(1-\sqrt{-n}).$$

Similarly, this will give two different factorizations of $n+1$ in R.

(3) When n is even, we will show that $(2, \sqrt{-n})$ is an ideal but not principal. Suppose $(2, \sqrt{-n}) = (x)$ for some $x \in R$, then $x|2$ and $x|\sqrt{-n}$. Now we have

$$N(x) \,|\, N(2) = 4, \quad N(x), | \, N(\sqrt{-n}) = -n.$$

As n is a square-free even integer, $N(x) = 1$ or 2. But no elements in R has norm 2. So $N(x) = 1$, i.e. $x\bar{x} = 1$. So x is a unit in R, i.e. $(2, \sqrt{-n}) = (1)$. Thus, $1 = 2(a + b\sqrt{-n}) + \sqrt{-n}(c + d\sqrt{-n})$ for some $a, b, c, d \in \mathbb{Z}$. We then deduce that

$$1 = 2a - nd \quad \text{and} 2b + c = 0.$$

But n is even, this gives a contradiction.

When n is odd, we will show that $(2, 1+\sqrt{-n})$ is an ideal but not principal. Suppose that $(2, 1+\sqrt{-n}) = (x)$. Similarly, we deduce that $N(x) = 4$. This implies that $N(x) = 1, 2, 4$. As no elements in R has norm 2. Also, if $x = \pm 2$, we must have $2 = x \,|\, 1 + \sqrt{-n}$, which is not possible. So again, $x = \pm 1$, i.e. $(2, 1+\sqrt{-n}) = (1)$. Now, we have $1 = 2(a + b\sqrt{-n}) + (1+\sqrt{-n})(c + d\sqrt{-n})$ for some $a, b, c, d \in \mathbb{Z}$. This implies that

$$1 = 2a + c - nd \quad \text{and} \quad 2b + c + d = 0.$$

As n is odd, the first equality implies that $c + d$ is odd, yet the second equality forces $c + d$ to be even. This is a contradiction. So $(2, 1+\sqrt{-n})$ is not a principal ideal.

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.

Solution: Let r be the minimal number such that $\sqrt[3]{2} \in K_r$. Since K_r is Galois over K_{r-1}, so it is normal. As the polynomial $x^3 - 2$ has one zero in K_r, it must splits in K_r, namely, $\sqrt[3]{2} \cdot e^{2\pi i/3}$ and $\sqrt[3]{2} \cdot e^{4\pi i/3}$ both belong to K_r. This then implies that $e^{2\pi i/3} \in K_r$, and thus

$$\mathbb{Q}(e^{2\pi i/3}) \subseteq K_r.$$

Yet K_r is of degree 3^r over $\mathbb{Q}$, it cannot contain a quadratic field $\mathbb{Q}(e^{2\pi i/3})$. This gives a contradiction.

解答题五 (15 分) 令 p 为一个素数且设 F 是一个包含所有 p次单位根的特征不为 p 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)

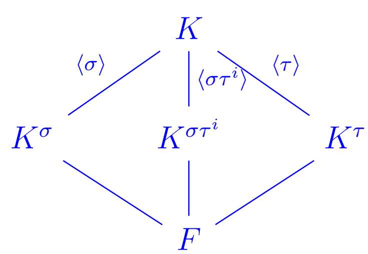
(2) 列出扩张 K/F 的所有的中间域，请写成在 $F(\eta)$ 的形式, 这里 η 是 K 中的某个元素. 并给出相应的 $\mathbf{Z}_p \times \mathbf{Z}_p$ 的子群 (给出生成元, 用 α 和 β 表示).

Let p be a prime number and let F be a field of characteristic not p, 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 α and β. Moreover, give the corresponding Galois subgroups, in terms of generators.

Solution: (1) Let ζ_p denote a primitive pth root of unity. Write the Galois group of K over F by $\langle \sigma, \tau \,|\, \sigma^p = \tau^p = 1, \sigma\tau = \tau\sigma \rangle$. We hope to be able to find all intermediate fields.



We first understand the subfields K^σ and K^τ. Pick an element $x \in K^\sigma$ and put

$$\alpha := x + \zeta_p \tau(x) + \zeta_p^2 \tau^2(x) + \cdots + \zeta_p^{p-1} \tau^{p-1}(x).$$

By independence of characters, there exists $x \in K^\sigma$ such that $\alpha \neq 0$. We note that $\tau(\alpha) = \zeta_p^{-1}\alpha$. This implies that $a = \alpha^p$ is fixed under the τ-action. So $a \in F^\times$. Also, as α is not fixed by τ, so $\alpha \in (K^\sigma)^\times$ and $K^\sigma = F(\alpha)$. (In particular, $\sigma(\alpha) = \alpha$.

A similar argument constructs $\beta \in (K^\tau)^\times$ with $\sigma(\beta) = \zeta_p^{-1}\beta$, and shows that $K^\tau = F(\beta)$. Put $b = \beta^p \in F^\times$. We note that $K = K^\sigma K^\tau$; so $K = F(\alpha, \beta)$.

(2) The subgroups of $\mathbf{Z}_p \times \mathbf{Z}_p$ are $\{1\}$, $\mathbf{Z}_p \times \mathbf{Z}_p$, and the subgroups generated by τ and by $\sigma\tau^i$ for $i = 0, \ldots, p-1$, respectively. We need to explain the corresponding field. The fields corresponding to $\{1\}$, $\mathbf{Z}_p \times \mathbf{Z}_p$, $\langle \tau \rangle$, and $\langle \sigma \rangle$ are K, F, $F(\alpha)$, and $F(\beta)$, respectively.

We note that for $i = 1, \ldots, p-1$,

$$\sigma\tau^i(\alpha\beta^{-i}) = \tau^i(\alpha) \cdot \sigma(\beta)^{-i} = \zeta_p^{-i}\alpha \cdot (\zeta_p^{-1}\beta)^{-i} = \alpha\beta^{-i}.$$

Thus, $\alpha\beta^{-i} \in K^{\langle\sigma\tau^i\rangle}$. Yet $\tau(\alpha\beta^{-i}) = \tau(\alpha)\beta^{-i} = \zeta_p^{-1}\alpha\beta^{-i} \neq \alpha\beta^{-i}$. So $\alpha\beta^{-i} \notin F$. Thus, we have $K^{\langle\sigma\tau^i\rangle} = F(\alpha\beta^{-i})$.

To complete the proof, we need to show that $K = F(\alpha+\beta)$ is monogenic. Indeed, $\tau(\alpha+\beta) = \zeta_p^{-1}\alpha + \beta \neq \alpha+\beta$. For any element $\sigma\tau^i$ (with $i \in \mathbf{Z}_p$),

$$\sigma\tau^i(\alpha+\beta) = \zeta_p^{-i}\alpha + \zeta_p^{-1}\beta.$$

If $\zeta_p^{-i}\alpha + \zeta_p^{-1}\beta = \alpha+\beta$, we must have

$$\beta = \alpha(1 + \zeta_p^{-1} + \cdots + \zeta_p^{1-i}).$$

Yet, if we apply σ to both sides of this, the RHS is invariant under σ-action, and $\sigma(\beta) = \zeta_p^{-1}\beta$. This is a contradiction.

From this, we deduce that $\alpha+\beta$ does not belong to any intermediate field and thus $K = F(\alpha+\beta)$.

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.

Solution: (1) Clearly, $\sigma(x) = x^q$ is an automorphism of $\mathbb{F}_{q^n}$ that fixes $\mathbb{F}_q$. Moreover, for every divisor d of n, the number of elements satisfying $\sigma^d(x) = x$ is q^d; so if $d \neq n$ not the entire $\mathbb{F}_{q^n}$. This means that the subgroup generated by σ inside $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is of order n. Thus $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle\sigma\rangle$.

(2) We may rewrite the norm map as $N(x) = x^{1+q+\cdots q^{n-1}}$. But $\mathbb{F}_{q^n}^\times$ is cyclic of order $q^n - 1$. So via isomorphisms $\mathbb{F}_{q^n}^\times \simeq \mathbf{Z}_{q^n-1}$ and $\mathbb{F}_q^\times \simeq \mathbf{Z}_{q-1}$, we may identify N with a map

$$N : \mathbf{Z}_{q^n-1} \to \mathbf{Z}_{q-1}$$

The kernel of N consists of elements in $\mathbf{Z}_{q^n-1}$ that are $(1 + q + q^2 + \cdots + q^{n-1})$-torsion. So $\#\ker N = 1+q+q^2+\cdots+q^{n-1}$. This in turn shows that $\#\mathrm{Im}(N) = q-1$. So $N : \mathbb{F}_{q^n}^\times \to \mathbb{F}_q^\times$ is surjective. Clearly, $N(0) = 0$. We are done.

(3) By the discussion above, the number of elements in $N^{-1}(1)$ is $\dfrac{q^n-1}{q-1} = q^{n-1}+q^{n-2}+\cdots+q+1 > q^{n-1}$. But if $N^{-1}(1)$ does not span $\mathbb{F}_{q^n}$, the subspace it spans can only have at most q^{n-1} elements. This is a contradiction.

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.

Solution: It suffices to show that $x^4 + 1$ is reducible over $\mathbb{F}_p$ for every prime number p (and thus reducible over F).

But we claim that $x^4 + 1$ splits completely over $\mathbb{F}_{p^2}$ already. But we note that for every prime number p, $8 \mid p^2 - 1$. In particular, $\mathbb{F}_{p^2}$ contains 8th roots of unity, and thus $x^4 + 1$ splits completely in $\mathbb{F}_{p^2}$. So x^4+1 cannot be irreducible over $\mathbb{F}_p$ as the splitting field of x^4+1 over $\mathbb{F}_p$ has degree at most 2.

This proves that $x^4 + 1$ is reducible over $\mathbb{F}_p$ and F.

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 α 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 α 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.

Solution: (1) Note that α and $\alpha + 1$ are zeros of $f(x)$. Then α is the zero of $f(x)$ and of $f(x-1)$. But $f(x)$ is irreducible over $F[x]$. So the only possibility is that $f(x)$ divides $f(x) - f(x-1)$ and thus $f(x-1) = f(x)$. This can only happen when the characteristic of F is positive.

(2) Continue with the discussion in (1), we note that $f(x) = f(x-1)$ implies that all terms in $f(x)$ have degrees divisible by p. Indeed, if not, take the term $a_n x^n$ with highest degree n relatively prime to p. Then $f(x) - f(x-1)$ contains a term $a_n n x^{n-1}$; so it is not zero. This means that $f(x)$ has only terms whose degrees are divisible by p.

Write $f(x) = g(x^p)$. Consider the splitting field of $g(x)$ inside K, denoted by L. In $L[x]$, the $g(x)$ factors as $g(x) = (x-\alpha_1)\cdots(x-\alpha_r)$. As discussed above, L is a proper subfield of K because otherwise each α_i is a pth power and then $f(x)$ is a p-th power as well, contradicting with the irreducibility of f. From K to L, we need to join $\alpha_1^{1/p}, \dots, \alpha_r^{1/p}$ to K. Put

$$K_i = K(\alpha_1^{1/p}, \dots, \alpha_i^{1/p})$$

Then each extension K_i/K_{i-1} is of degree 1 or p. Take the "last" subfield of K, which gives a subfield E of K such that $[K : E] = p$.