2023 秋: 代数学一 (实验班) 期末考试

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	F	T	F	F	T	T	F	T	T

1. 每个 $\mathbf{Z}_4 \times \mathbf{Z}_8$ 中的元素的阶都是 8.

Every element of $\mathbf{Z}_4 \times \mathbf{Z}_8$ has order 8.

False. For example, $(0,0) \in \mathbf{Z}_4 \times \mathbf{Z}_8$ has order 1.

2. 如果 H 是 G 的子群，则 $N_G(H)$ 是 G 的正规子群。

If H is a subgroup of G, then $N_G(H)$ is a normal subgroup of G.

False. There is no reason for $N_G(H)$ to be normal in G. For example, $H = \{1, (12)\} \in S_3 = G$ is a subgroup, $N_G(H) = H$ is not normal in G.

3. 环 $R_1 \times R_2$ 的理想都形如 $I_1 \times I_2$，这里 I_1 是 R_1 的理想，I_2 是 R_2 的理想。

Every ideal of the product of the ring $R_1 \times R_2$ is of the form $I_1 \times I_2$ for ideals $I_1 \subseteq R_1$ and $I_2 \subseteq R_2$.

True. Let I be the idea of $R_1 \times R_2$. Put $I_1 = \{a_1 \,|\, \text{there exists } (a_1, a_2) \in I\}$ and $I_2 = \{a_2 \,|\, \text{there exists } (a_1, a_2) \in I\}$. Indeed, for (a_1, a_2), $(a_1, a_2)(1, 0) = (a_1, 0)$ and $(a_1, a_2)(0, 1) = (0, a_2)$; so $I_1 = \{a_1 \,|\, (a_1, 0) \in I\}$ and $I_2 = \{a_2 \,|\, (0, a_2) \in I\}$. It is clear that I_1 is an ideal of R_1, and I_2 is an ideal of R_2. On the other hand, $I_1 \times I_2 = I_1 + I_2$; so all ideals are of the form $I_1 \times I_2$.

4. 设 R 是整环，$\varphi : R \to R'$ 是交换环之间的满射。则 $\varphi(R) = R'$ 也是一个整环。

Let R be an integral domain and $\varphi : R \to R'$ a surjective homomorphism of commutative rings, then $\varphi(R) = R'$ is an integral domain.

False. There is no reason for R' to be an integral domain. For example, $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is surjective but $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain unless n is a prime number.

5. 若 p 是一个整环 D 中的不可约元素，则 p 是一个 D 中的素元。

If p is an irreducible element in an integral domain D, then p is a prime element.

False. In an integral domain, a prime element is always irreducible, but not conversely.

6. 设 M 和 N 是两个 $\mathbb{Q}$-线性空间，$\varphi : M \to N$ 是一个 $\mathbb{Z}$-模同态。则 φ 是一个 $\mathbb{Q}$-线性映射。

Let M and N be two $\mathbb{Q}$-vector spaces and $\varphi : M \to N$ is a $\mathbb{Z}$-module homomorphism. Then φ is a $\mathbb{Q}$-linear map.

True. We need to show that $\varphi(\frac{a}{b}m) = \frac{a}{b}\varphi(m)$ for $\frac{a}{b} \in \mathbb{Q}$. This is because $b \cdot \varphi(\frac{a}{b}m) = \varphi(b \cdot \frac{a}{b}m) = \varphi(am) = a\varphi(m)$. In $\mathbb{Q}$-vector space, we may "divide by b" to get $\varphi(\frac{a}{b}m) = \frac{a}{b}\varphi(m)$.

7. 任何一个域要么包含 $\mathbb{Q}$，要么包含某个 $\mathbb{F}_p$ (p 为素数).

A field either contains $\mathbb{Q}$ or contains $\mathbb{F}_p$ for some prime number p.

True. If the field F has characteristic 0, it contains $\mathbb{Q}$. If the field F has characteristic $p > 0$, it contains $\mathbb{F}_p$.

8. 设 K/F 是一个有限的域扩张。若中间域 K_1 和 K_2 满足 $\mathrm{Gal}(K/K_1)$ 与 $\mathrm{Gal}(K/K_2)$ 同构，则 $K_1 = K_2$.

Let K be a finite Galois extension of F. If two intermediate fields K_1 and K_2 satisfies $\mathrm{Gal}(K/K_1)$ is isomorphic to $\mathrm{Gal}(K/K_2)$, then $K_1 = K_2$.

False. To prove that $K_1 = K_2$, it is not enough to require two Galois group $\mathrm{Gal}(K/K_1)$ and $\mathrm{Gal}(K/K_2)$ to be isomorphic, we need $\mathrm{Gal}(K/K_1)$ and $\mathrm{Gal}(K/K_2)$ to be the *same* group. For example, $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. For $K_1 = \mathbb{Q}(\sqrt{2})$ and $K_2 = \mathbb{Q}(\sqrt{3})$, the Galois groups $\mathrm{Gal}(K/K_1) = \{0\} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{Gal}(K/K_2) = \mathbb{Z}/2\mathbb{Z} \times \{0\}$ are isomorphic. Yet $K_1 \neq K_2$.

9. 设域扩张塔 $F \subseteq K_1 \subseteq K_2 \subseteq \cdots$ 中每一个 K_i/F 都是有限伽罗华扩张。记 $K = \bigcup_i K_i$. 则 K 是一个 F 的伽罗华扩张。

Let $F \subseteq K_1 \subseteq K_2 \subseteq \cdots$ be field extensions such that each K_i is finite and Galois over F. Put $K = \bigcup_i K_i$. Then K is a Galois extension of F.

True. Both properties of being separable and being normal are preserved under increasing union.

10. 设 K/F 是一个次数为 7 的扩张。则任何一个在 K 中但不在 F 中的元素 α 都在 F 上生成 K.

Let K/F be a field extension of degree 7. Then any element $\alpha \in K$ that does not belong to F generates K over F.

True. If $\alpha \notin F$, then $F(\alpha) \neq F$. We have $[K : F] = [K : F(\alpha)] \cdot [F(\alpha) : F]$. Since $[K : F] = 7$ is a prime number, $[F(\alpha) : F]$ can only be 7. So $K = F(\alpha)$.

解答题一 (15 分) 记 $\zeta_{13} := e^{2\pi \mathbf{i}/13} \in \mathbb{C}$ 和 $\alpha := \zeta_{13} + \zeta_{13}^{-1}$.

(1) 决定 $\mathbb{Q}(\alpha)/\mathbb{Q}$ 的伽罗华群. (需要给出一个严格的证明.)

(2) 确定 $\mathbb{Q}(\alpha)/\mathbb{Q}$ 的所有中间域，并给出伽罗华群与域对应的图表。对每个中间域 (不包括 $\mathbb{Q}(\alpha)$ 和 $\mathbb{Q}$), 给出一个 $\mathbb{Q}$ 上的生成元，并计算它的极小多项式。

Let $\zeta_{13} := e^{2\pi \mathbf{i}/13} \in \mathbb{C}$, and let $\alpha := \zeta_{13} + \zeta_{13}^{-1}$.

(1) Determine the Galois group of $\mathbb{Q}(\alpha)/\mathbb{Q}$. (You need to give a rigorous proof.)

(2) Determine all intermediate fields of $\mathbb{Q}(\alpha)/\mathbb{Q}$, and draw the diagram of Galois correspondence of these intermediate fields. For each intermediate field (*excluding* $\mathbb{Q}(\alpha)$ and $\mathbb{Q}$), give a generator over $\mathbb{Q}$ and compute its minimal polynomial.

证明. (1) The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{13})/\mathbb{Q}) \cong (\mathbb{Z}/13\mathbb{Z})^\times$. For $a \in (\mathbb{Z}/13\mathbb{Z})^\times$, let σ_a denote the corresponding automorphism. We note that α is invariant under the action of σ_a if and only if

$$\sigma_a(\zeta_{13} + \zeta_{13}^{-1}) = \zeta_{13}^a + \zeta_{13}^{-a} = 2\cos\frac{a\pi}{13}$$

is equal to $\zeta_{13} + \zeta_{13}^{-1} = 2\cos\frac{\pi}{13}$. This is further equivalent to $a \in \{\pm 1\}$. So the Galois group of $\mathrm{Gal}(\mathbb{Q}(\zeta_{13})/\mathbb{Q}(\zeta_{13} + \zeta_{13}^{-1})) = \{\pm 1\}$. The Galois group

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{13} + \zeta_{13}^{-1})/\mathbb{Q}) \cong (\mathbb{Z}/13\mathbb{Z})^\times/\{\pm 1\}.$$

It is a cyclic group of order 6.

(2) We have the following diagram of intermediate fields and subgroups.

$$\begin{tikzcd}[column sep=small]
 & \{\pm1\}/\{\pm1\} \arrow[dl, dash] \arrow[dr, dash] & \\
\{\pm1,\pm5\}/\{\pm1\} \arrow[dr, dash] & & \{\pm1,\pm3,\pm4\}/\{\pm1\} \arrow[dl, dash] \\
 & (\mathbb{Z}/13\mathbb{Z})^\times/\{\pm1\}. &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\zeta_{13}+\zeta_{13}^{-1}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\zeta_{13})^{\{\pm1,\pm5\}} \arrow[dr, dash] & & \mathbb{Q}(\zeta_{13})^{\{\pm1,\pm3,\pm4\}} \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Here $\{\pm 1, \pm 5\}/\{\pm 1\}$ is the unique subgroup of $(\mathbb{Z}/13\mathbb{Z})^\times/\{\pm 1\}$ of order 2, and $\{\pm 1, \pm 3, \pm 4\}/\{\pm 1\}$ is the unique subgroup of order 3.

Write $\zeta = \zeta_{13}$. For $a \in \mathbb{N}$, put $\alpha_a = \zeta^a + \zeta^{-a}$ and $\alpha_1 = \alpha$. Put

$$\beta = \alpha_1 + \alpha_5 = \zeta + \zeta^{-1} + \zeta^5 + \zeta^{-5} \in \mathbb{Q}(\zeta)^{\{\pm 1, \pm 5\}}.$$

We compute that

$$
\begin{aligned}
\beta^2 &= (\alpha_1+\alpha_5)^2 = \alpha_1^2 + 2\alpha_1\alpha_5 + \alpha_5^2 = \alpha_2 + 2 + 2\alpha_4 + 2\alpha_6 + \alpha_3 + 2,\\
\beta^3 &= (\alpha_1+\alpha_5)^3 = \alpha_1^3 + 3\alpha_1^2\alpha_5 + 3\alpha_1\alpha_5^2 + \alpha_5^3\\
&= (\alpha_3+3\alpha_1) + 3(\alpha_6+\alpha_3+2\alpha_5) + 3(\alpha_2+\alpha_4+2\alpha_1) + (\alpha_2+3\alpha_5)\\
&= 9\alpha_1 + 4\alpha_2 + 4\alpha_3 + 3\alpha_4 + 9\alpha_5 + 3\alpha_6.
\end{aligned}
$$

Using that $1+\zeta_{13}+\cdots+\zeta_{13}^{12} = 1+\alpha_1+\cdots+\alpha_6 = 0$, we see that

$$
0 = 5(1+\alpha_1+\cdots+\alpha_6) = 5+\beta^3+(\beta^2-4)-4\beta = \beta^3+\beta^2-4\beta+1.
$$

Thus, we have $\mathbb{Q}(\zeta_{13})^{\{\pm1,\pm5\}} = \mathbb{Q}(\beta)$ and β has minimal polynomial x^3+x^2-4x+1.

Put

$$
\gamma = \alpha_1+\alpha_3+\alpha_4 = \zeta+\zeta^{-1}+\zeta^3+\zeta^{-3}+\zeta^4+\zeta^{-4} \in \mathbb{Q}(\zeta)^{\{\pm1,\pm3,\pm4\}}.
$$

We compute that

$$
\begin{aligned}
\gamma^2 &= \alpha_1^2+\alpha_3^2+\alpha_4^2+2\alpha_1\alpha_3+2\alpha_1\alpha_4+2\alpha_3\alpha_4\\
&= (\alpha_2+2)+(\alpha_6+2)+(\alpha_5+2)+2(\alpha_2+\alpha_4)+2(\alpha_3+\alpha_5)+2(\alpha_1+\alpha_6)\\
&= 6+3\alpha_2+3\alpha_5+3\alpha_6+2\alpha_1+2\alpha_3+2\alpha_4
\end{aligned}
$$

Using that $1+\zeta_{13}+\cdots+\zeta_{13}^{12} = 1+\alpha_1+\cdots+\alpha_6 = 0$, we see that

$$
0 = 3(1+\alpha_1+\cdots+\alpha_6) = 3+(\gamma^2-6)+\gamma = \gamma^2+\gamma-3.
$$

This $\gamma = \frac{-1+\sqrt{13}}{2}$ so that $\mathbb{Q}(\gamma) = \mathbb{Q}(\sqrt{13})$. $\square$

解答题二 (10 分) 设 G 是一个阶为 $2^m k$ 的群，这里 k 是一个奇数且 m 为正整数。假设 G 包含一个阶恰为 2^m 的元素 g。

(a) 左乘 $x \in G$ 定义了一个 G 中元素的置换 (正如 Cayley 定理中所叙述)。证明 π_g 是一个奇置换 (这里 g 是前述阶为 2^m 的元素)。

(b) 令 H 为 G 中所有满足 π_h 为偶置换的元素 $h \in G$. 证明：$|H| = 2^{m-1}k$ 且 H 包含一个元素其阶恰为 2^{m-1}.

(c) 证明 G 包含一个子群其元素个数为 k.

Let G be a group of order $2^m k$ with k odd and with $m \geq 1$. Assume that G contains an element g of order 2^m.

(a) Multiplication (from the left) by $x \in G$ gives a permutation π_x of the elements of G, as in Cayley's theorem. Show that π_g is an odd permutation (where g is the element of order 2^m).

(b) Let H be the subgroup of $h \in G$ such that π_h is an even permutation. Show that $|H| = 2^{m-1}k$ and that H contains an element of order 2^{m-1}.

(c) Show that G contains a subgroup of order k.

证明. (a) Since g has order 2^m, there are exactly k right $\langle g \rangle$-cosets of G. So π_g is a product of k 2^m-cycles. But every 2^m-cycle is an odd permutation, so π_g is an odd permutation.

(b) Consider the homomorphism

$$\varphi : G \xrightarrow{x \mapsto \pi_x} S(G) \xrightarrow{\text{sgn}} \{\pm 1\}$$

The kernel of φ is precisely the subgroup H of those $h \in G$ for which π_h is an even permutation.

By first isomorphism theorem, $G/H \cong \{\pm 1\}$; so $|H| = 2^{m-1}k$ and it is clear that $g^2 \in H$ and g^2 generate a subgroup of H of order 2^{m-1}.

(c) Use induction on m, we first see that G admits a subgroup G_{m-1} of order $2^{m-1}h$ which contains an element of order 2^{m-1}. Applying (b) in turn to G_{m-1} shows that G_{m-2} admits a subgroup G_{m-2} of order $2^{m-2}h$ which contains an element of order 2^{m-2}. Continue this way, we arrive at the group G_0 of order exactly k. □

解答题三 (10 分) 设 L/K 是一个伽罗华扩张，且其伽罗华群为由 σ 生成的 n 阶循环群。设 $n = ab$, $\gcd(a, b) = 1$. 令 F_1 为 σ^a 的固定域，F_2 为 σ^b 的固定域. 假设 $F_1 = K(\alpha)$, $F_2 = K(\beta)$. 证明：$L = K(\alpha + \beta)$.

Let L/K be a Galois extension of fields such that $\mathrm{Gal}(L/K)$ is cyclic of order n, generated by σ. Write $n = ab$ with $\gcd(a, b) = 1$. Let F_1 be the fixed field of σ^a and F_2 be the fixed field of σ^b. Suppose that $F_1 = K(\alpha)$ and $F_2 = K(\beta)$. Prove that $L = K(\alpha + \beta)$.

证明. If $L \neq K(\alpha + \beta)$, then $K(\alpha + \beta)$ is fixed by some σ^i with $i \neq 0$. By taking some multiple of i, we may assume that i is divisible by either a or b. WLOG, i is divisible by b. In particular, $\sigma^i(\alpha + \beta) = \alpha + \beta$. So

$$\sigma^i(\alpha) - \alpha = \beta - \sigma^i(\beta) = 0,$$

as β is fixed by σ^b. It then follows that α is also fixed by σ^i. So $K(\alpha) \subseteq L^{\langle \sigma^a, \sigma^i \rangle} \subsetneq F_1$. Contradiction!

So $L = K(\alpha + \beta)$. □

解答题四 (15 分) 设 R 是一个唯一分解整环. 假设 R 中所有非零的素理想都是极大理想。证明：R 是一个主理想整环。(允许使用 Zorn 引理的推论，虽然不必要。)

Let R be a unique factorization domain. Suppose that every nonzero prime ideal of R is maximal. Show that R is a principal ideal domain. (You may make apply corollaries of Zorn's lemma, although not necessarily needed.)

证明. We first show that if p and q are nonassociated prime (or equivalently irreducible) elements, then there exist $a, b \in R$ such that $ap + bq = 1$.

Now, let I be an ideal of R. For each nonzero element of I, the UFD property ensures that it factors uniquely as a product of irreducible elements (which is the same as prime elements). Take f to be the nonzero element of I with minimal number of prime factors, say $f = p_1 \cdots p_r$ with irreducible elements $p_1, \dots, p_r \in R$. We claim that $I = (f)$.

Let g be another element of I that is not a multiple of f. WLOG, we assume that g has prime factorization $p_{s+1} \cdots p_r q_1 \cdots q_t$ with each $q_1, \dots, q_t$ irreducible, and that each of $p_1, \dots, p_s$ is nonassociate with each of $q_1, \dots, q_t$. For each pair $(i, j) \in \{1, \dots, s\} \times \{1, \dots, t\}$ there exist $a_{ij}, b_{ij} \in R$ such that $a_{ij}p_i + b_{ij}q_j = 1$. So we have

$$1 = \prod_{i=1}^{s} \prod_{j=1}^{t} (a_{ij}p_i + b_{ij}q_j)$$

Expanding the RHS, we note that every term is either a multiple of $p_1 \cdots p_s$ or a multiple of $q_1 \cdots q_t$. (Indeed, if for every i, some $a_{ij}p_i$ term is taken, the product is a multiple of $p_1 \dots p_s$. If for some i, none of $a_{ij}p_i$ is taken, we must have chosen all of $b_{ij}q_j$; so the product is a multiple of $q_1 \cdots q_t$.)

Thus, $p_{s+1} \cdots p_r = p_{s+1} \cdots p_r \prod_{i=1}^{s} \prod_{j=1}^{t} (a_{ij}p_i + b_{ij}q_j)$ is a linear combination of f and g; so $p_{s+1} \cdots p_r \in I$, but this contradicts with the minimal number of prime factors of nonzero elements in I. Thus $I = (f)$ is principal. $\square$

解答题五 (10 分) 设 G 是一个有限群，固定 G 的阶的一个素因子 p。记 $K = \bigcap N_G(P)$，这里相交取遍 G 的所有西罗 p-子群 P，$N_G(-)$ 为正规化子。证明

(a) $K \lhd G$.

(b) G 和 G/K 有相同数量的西罗 p-子群。

Let G be a finite group and assume that p is a fixed prime divisor of its order. Set $K = \bigcap N_G(P)$ where the intersection is taken over all Sylow p-subgroups P of G and $N_G(-)$ denotes the normalizer. Show that

(a) $K \lhd G$.

(b) G and G/K have the same number of Sylow p-subgroups.

证明. (a) For $g \in G$, we have

$$gKg^{-1} = g\Big(\bigcap N_G(P)\Big)g^{-1} = \bigcap gN_G(P)g^{-1} = \bigcap N_G(gPg^{-1}) = \bigcap N_G(P) = K.$$

The second last equality is because that all p-Sylow subgroups are conjugate. So K is normal in G.

(b) Put $\overline{G} = G/K$ and for any subgroup H of G, denote its image in G/K by $\overline{H}$ (so $\overline{H} = H/H \cap K$).

Fix a p-Sylow subgroup Q of G, then its image $\overline{Q}$ in G/K is a p-Sylow subgroup. Let N denote the normalizer of Q, i.e. $N = N_G(Q)$. So the number of p-Sylow subgroups is precisely $\#(G/N)$. Similarly, the number of p-Sylow subgroups in G/K is precisely $\#\overline{G}/N_{\overline{G}}(\overline{Q})$.

First note that $K = \bigcap N_G(P) \subseteq N_G(Q) = N$. We claim that $N_{\overline{G}}(\overline{Q}) \cong \overline{N}$. For any $n \in N$, $n\overline{Q}n^{-1} = \overline{nQn^{-1}} = \overline{Q}$; so the image of N is contained in $N_{\overline{G}}(\overline{Q})$. Conversely, if some $\bar{n} \in \overline{G}$ normalizes $\overline{Q}$, it must be the case that $nQn^{-1} \subseteq QK$ for some lift n of $\bar{n}$ in G. But on the other hand, Q is a p-Sylow subgroup in G, so it is a p-Sylow subgroup of QK. On the other hand, K normalizes Q; so QK normalizes Q. Inside QK, the p-Sylow subgroup Q is normal; so $Q = nQn^{-1}$. It follows that $n \in N$ and hence $\bar{n} \in \overline{N}$.

Now, we see that $G/N \cong \overline{G}/\overline{N}$; it follows that the number of p-Sylow subgroups in G and the number of p-Sylow subgroups in G/K are the same. □

解答题六 (15 分) 此问题与标准基定理有关。

(a) 设 K/F 是一个有限伽罗华扩张，伽罗华群为 G. 证明：将 K 自然地看做群环 $F[G]$ 的模是秩为 1 的自由模当且仅当存在元素 $x \in K$ 使得 $\{\sigma(x) \,|\, \sigma \in G\}$ 为 K 作为 F-线性空间的一组基.

标准基定理 是指上述两个等价条件永远成立。接下来，我们在特殊情形下证明此定理。(当然，不可以直接使用此定理。)

(b) 设 K/F 是一个有限域的有限扩张，这里 $|F| = q$. 用 $\Phi : x \mapsto x^q$ 记 K 上的 q 次幂 Frobenius 映射, 并记 $G := \mathrm{Gal}(K/F)$. 求 Φ 作为 F-线性空间 K 上线性映射的极小多项式.

(c) 符号和标记如 (b). 利用 (b) 证明有限域有限扩张的标准基定理。(如果没有证明 (b) 可以使用 (b) 的结论。)

This problem concerns normal basis theorem.

(a) Let K/F be a finite Galois extension with Galois group G. Prove that K viewed as a module over the group ring $F[G]$ is free of rank 1 if and only if there exists $x \in K$ such that $\{\sigma(x) \,|\, \sigma \in G\}$ form an F-basis of K.

The normal basis theorem states that the above equivalent condition always holds. In the following, we verify this in a very special case. (Clearly, you cannot use normal basis theorem to prove results.)

(b) Consider the case when K/F is an extension of finite fields with $\#F = q$. Let $\Phi : x \mapsto x^q$ denote the qth power Frobenius map on K, and let $G := \mathrm{Gal}(K/F)$. Compute the minimal polynomial of Φ as a F-linear endomorphism of K.

(c) Keep the setup as in (b). Use (b) to prove the *normal basis theorem* for extensions of finite fields. (Even if you do not know how to prove (b), you can still use the result of (b) to deduce (c).)

证明. (a) If K is an $F[G]$-module free of rank 1, say with generator x. Let $\varphi : F[G]x \cong K$. Then

$$K = \bigoplus_{\sigma \in G} F\sigma(x).$$

Conversely, if $x \in K$ is so that $\{\sigma(x) \,|\, \sigma \in G\}$ form an F-basis of K, we have an isomorphism

$$\begin{aligned} F[G] &\xrightarrow{\;\;\cong\;\;} K \\ \sum_\sigma a_\sigma[\sigma] &\longmapsto \sum_\sigma a_\sigma \sigma(x). \end{aligned}$$

This proves (a).

(b) Assume that $[K : F] = n$. Consider Φ as an F-linear operator acting on K; let $P(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in F[x]$ denote its minimal polynomial. Since $\Phi^n = 1$ on K, we must have $P(x)|(x^n - 1)$. In particular, $m \leq n$.

If $m < n$, we must have $\Phi^m + a_{m-1}\Phi^{m-1} + \cdots + a_0 \cdot \mathrm{id} = 0$ on K. Yet by Artin's independence of characters, $1, \Phi, \Phi^2, \ldots, \Phi^{n-1}$ are linearly independent as functions on K. So the above linear relation cannot happen with $m < n$. So $m = n$ and thus $P(x) = x^n - 1$.

(c) Since $\dim_F K$ is equal to the degree of the minimal polynomial of Φ, the F-vector space K, as a $F[t]$-module where t acts by Φ, is isomorphic to $F[t]/(t^n - 1)$. This means that K is a free module of $F[\mathrm{Gal}(K/F)]$ of rank 1. □

解答题七 (15 分) 给定交换幺环 R。令 N 为由 R 中幂零的元素构成的集合 (即是具有如下性质的元素 $r \in R$ 的集合：存在 $n \geq 1$ 使得 $r^n = 0$). 由课上的一个定理知 N 是 R 的一个理想。证明如下的三个命题(a)–(c)等价. (不允许直接使用大定理如：幂零理想是所有素理想的交。如果一定要使用，需要先给出证明。)

(a) R/N 是一个域。

(b) R 中的每个元素要么是一个单位，要么是幂零的。

(c) N 是一个素理想，且它是 R 的唯一的素理想。

现在，假设 p 是一个素数且 $n \in \mathbb{Z}_{\geq 1}$。确定环

$$R = \mathbb{Z}[X]/(X^p - 1, p^n)$$

是否满足上述等价条件。给出证明。

Let R be a commutative ring with 1. Let N be the set of nilpotent elements of R (that is the set of $r \in R$ such that $r^n = 0$ for some $n \geq 1$). By a theorem from the class, N is an ideal of R. Prove that the following statements (a)–(c) are equivalent. (One cannot quote big theorems such as nilpotent radical of a commutative ring is the intersection of all prime ideals; if one has to use this, please provide a proof.)

(a) R/N is a field.

(b) Every element of R is either a unit or nilpotent.

(c) N is a prime ideal and it is the only prime ideal of R.

Now assume that p is a prime number and $n \in \mathbb{Z}_{\geq 1}$. Determine whether the ring

$$R = \mathbb{Z}[X]/(X^p - 1, p^n)$$

satisfies the above equivalence conditions.

证明. We first point out that a unit of R can never be nilpotent. First prove the equivalence of (a)–(c).

(a) $\Rightarrow$ (b). Let $a \in R$ be an element that is not nilpotent. We need to show that a is a unit. Clearly, $a \notin N$. Thus the image $\bar{a}$ of a in R/N is nonzero. Since R/N is a field, there exists $\bar{b} \in R/N$ such that $\bar{a} \cdot \bar{b} = \bar{1}$ in R/N. Take any lift $b \in R$ of $\bar{b}$. Then $ab - 1 = n$ for some $n \in N$. But n is nilpotent, so $n^r = 0$ for some $r \in \mathbb{Z}_{\geq 1}$. Then we have

$$1 = ab - n = (ab - n)^r = \sum_{i=0}^{r} \binom{r}{i} (ab)^i n^{r-i}$$

But the term with $i = 0$ vanishes, so the RHS is a multiple of a. Thus a is a unit.

(b) $\Rightarrow$ (c). First show that N is a prime ideal. Indeed, if $ab \in N$ for some $a, b \in R$. Suppose that $a, b \notin N$, then a, b are both units, so ab is also a unit, and thus $ab \notin N$. Contradiction. So N is a prime ideal.

Now we show that every prime ideal $\mathfrak{p}$ is equal to N. Indeed, for every element $n \in N$, $n^r = 0 \in \mathfrak{p}$ for some r. So $n \in \mathfrak{p}$, and thus $N \subseteq \mathfrak{p}$. But every element that is not in N is a unit, and a prime ideal cannot contain a unit. So $N = \mathfrak{p}$.

(c) $\Rightarrow$ (a) Since N is the only prime ideal of R, it is a maximal ideal. Thus R/N is a field.

Now, we prove that the ring $R = \mathbb{Z}[X]/(X^p - 1, p^n)$ satisfies the above equivalence conditions. It is clear that $p \in N$ because p^n is zero in R. Moreover, we claim that $X - 1 \in N$, this is because $(X-1)^p = X^p - 1 + p*$ is a multiple of p; so $(X-1)^{pn}$ is zero in R. It then follows that $(p, X-1) \subseteq N$. But on the other hand,

$$R/(p, X-1) = \mathbb{F}_p[X]/(X-1) \cong \mathbb{F}_p$$

is already a field. So $N = (p, X-1)$ is a maximal ideal and the quotient R/N is a field. The ring R satisfies condition (a). $\square$

解答题八 (10 分) 固定素数 p. 设 L/K 是特征 p 的域的一个有限扩张. 记 σ 为域 L 的 p-Frobenius 自同态，显然 σ 将 K 映到自身.

(a) 考虑 L/K 的中间域:

$$K \subseteq \cdots \subseteq K\sigma^3(L) \subseteq K\sigma^2(L) \subseteq K\sigma(L) \subseteq L.$$

证明：对所有非负整数 n,

$$[K\sigma^n(L) : K\sigma^{n+1}(L)] \geq [K\sigma^{n+1}(L) : K\sigma^{n+2}(L)].$$

(b) 证明：如果 $[L : K\sigma(L)] \leq p$, 那么域扩张 L/K 可以由一个元素生成. (可以使用课上证明或者作业中的结论，使用其它结论需要给出证明。)

Let p be a prime number. Let L/K be a finite extension of fields of characteristic p, and let σ denote the p-Frobenius endomorphism on L, which of course stabilizes K.

(a) Consider the intermediate fields between K and L:

$$K \subseteq \cdots \subseteq K\sigma^3(L) \subseteq K\sigma^2(L) \subseteq K\sigma(L) \subseteq L.$$

Prove that for any $n \in \mathbb{Z}_{\geq 0}$,

$$[K\sigma^n(L) : K\sigma^{n+1}(L)] \geq [K\sigma^{n+1}(L) : K\sigma^{n+2}(L)].$$

(b) Prove that if $[L : K\sigma(L)] \leq p$, then L/K can be generated by one element. (You are allowed to use theorems proved in class or in exercises; for all other theorems, you need to provide proofs.)

证明. (a) Consider the following tower of extensions

$$\begin{tikzcd}
 & & & K\sigma^n(L) \arrow[dl, dash] \arrow[ddrr, dash, dashed] & & \\
 & & K\sigma^{n+1}(L) \arrow[dll, dash] \arrow[drrr, dash] \arrow[ddr, dash, dashed] & & & \\
K\sigma^{n+2}(L) \arrow[drrr, dash] & & & & & \sigma(K)\sigma^{n+1}(L) \arrow[dll, dash] \\
 & & & \sigma(K)\sigma^{n+2}(L) & &
\end{tikzcd}$$

The extension $\sigma(K)\sigma^{n+1}(L)/\sigma(K)\sigma^{n+2}(L)$ is isomorphic to the extension $K\sigma^n(L)/K\sigma^{n+1}(L)$ (under the isomorphism via σ), and the extension $K\sigma^{n+1}(L)/K\sigma^{n+2}(L)$ is the composition of the extension $\sigma(K)\sigma^{n+1}(L)/\sigma(K)\sigma^{n+2}(L)$ with K. So we have

$$[K\sigma^n(L) : K\sigma^{n+1}(L)] = [\sigma(K)\sigma^{n+1}(L) : \sigma(K)\sigma^{n+2}(L)] \geq [K\sigma^{n+1}(L) : K\sigma^{n+2}(L)].$$

(b) First of all, the p-th power of every element of $K\sigma^n(L)$ belongs to $K\sigma^{n+1}(L)$; the extension $K\sigma^n(L)/K\sigma^{n+1}(L)$ is a power of p (or 1).

By (a), we know that

$$p \geq [L : K\sigma(L)] \geq [K\sigma(L) : K\sigma^2(L)] \geq \cdots$$

So there must be a positive integer n such that

$$[L : K\sigma(L)] = \cdots = [K\sigma^{n-1}(L) : K\sigma^n(L)] = p, \quad K\sigma^n(L) = K\sigma^{n+1}(L) = K\sigma^{n+2}(L) = \cdots$$

Let α be an element of L that generates L over $K\sigma(L)$. Then $\alpha^p \in K\sigma(L)$. By the exact proof of (a), we see that α^p generates $\sigma(K)\sigma(L)$ over $\sigma(K)\sigma^2(L)$ and hence generates $K\sigma(L)$ over $K\sigma^2(L)$. Continue this way, we have $\alpha^{p^{n-1}}$ generates $K\sigma^{n-1}(L)$ over $K\sigma^n(L)$. Thus, α generates L over $K\sigma^n(L)$.

On the other hand, put $F = \sigma^n(L)$. We show that $KF = K\sigma(F)$ implies that KF is separable over K. Indeed, we first prove that for any intermediate field E of KF/K, $E = \sigma(E)K$. Clearly, $E \supseteq K\sigma(E)$. Then we have the following diagram

$$\begin{tikzcd}
KF \arrow[r, equal] \arrow[d, dash] & K\sigma(F) \arrow[dd, dash] \arrow[dr, dash] & \\
E \arrow[dd, dash] \arrow[dr, dash] & & \sigma(KF) \arrow[dd, dash] \\
 & K\sigma(E) \arrow[dl, dash] \arrow[dr, dash] & \\
K & & \sigma(E)
\end{tikzcd}$$

From this, we have

$$[K\sigma(F) : K\sigma(E)] = [KF : E][E : K\sigma(E)] \geq [KF : E] = [\sigma(KF) : \sigma(E)] \geq [K\sigma(F) : K\sigma(E)].$$

Here the last equality follows from the isomorphism σ, and the last inequality follows from composing the extension $\sigma(KF)/\sigma(E)$ with K. From this series of inequalities, we see that all equality holds; in particular $E = K\sigma(E)$.

Now suppose that KF is not separable over K. If $\alpha \in KF$ is inseparable over K, with minimal polynomial $g(t^p)$ for a polynomial $g(x) \in F[x]$ of degree m. Then $[K(\alpha) : K] = pm$ and $[K(\alpha^p) : K] = m$. Yet $\alpha^p \in K\sigma(K(\alpha))$ which is equal to $KK(\alpha) = K(\alpha)$ by the discussion of intermediate field. This is a contradiction.

Now, we conclude by noting that $K\sigma^n(L)/K$ is separable and hence generated by one element β. Thus α and β generate L over K with β separable over K. By a theorem in class, L/K is generated by one element. $\square$