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

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.

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.

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 $I_2 \subseteq R_2$.

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.

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.

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.

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.

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 $K_1 = K_2$.

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.

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.

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.

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.

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 $L = K(\alpha + \beta)$.

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.)

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.

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 $\{\sigma(x) \mid \sigma \in G\}$ 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 $\{\sigma(x) \mid \sigma \in G\}$ 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).)

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. You need to give a proof of your statement.

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.)