2023 秋：代数学一 (实验班) 期中考试

姓名: ____________ 院系: ____________ 学号: ____________ 分数:

时间：110 分钟 满分：110 分, 总分不超过 100 分

判断题 在下表中填写 T 或 F (10 分)

1	2	3	4	5	6	7	8	9	10
F	F	T	F	F	T	F	F	T	T

1. 若 $\phi : G \to G$ 是一个群 G 到自身的满同态, 则它是一个同构.

If $\phi : G \to G$ is a surjective homomorphism from a group G to itself, then ϕ is an isomorphism.

False. This is true for finite groups but fails for infinite group in general. For example, $G = \mathbb{Q}/\mathbb{Z}$, multiplication by 2 induces a surjective homomorphism from G to itself, which is not an isomorphism.

2. 一个群同态 $\phi : G \to H$ 是单射当且仅当其核 $\ker \phi$ 是空集.

A group homomorphism $\phi : G \to H$ is injective if and only if $\ker \phi$ is the empty set.

False. The kernel of a group homomorphism is never empty, as it always contains the identity element. A group homomorphism is injective if and only if its kernel is a singleton consisting of the identity element.

3. 在一个奇数阶的循环群中，一个生成元的平方也是生成元.

In a cyclic group of *odd* order, the square of a generator is also a generator.

True. If we view the cyclic group as $\mathbb{Z}/n\mathbb{Z}$ with n odd and generator 1, then 2 is also a generator.

4. 若 G_1 和 G_2 为群, 则每个 $G_1 \times G_2$ 的子群都形如 $H_1 \times H_2$, 这里 $H_1 \leq G_1$ 且 $H_2 \leq G_2$.

Let G_1 and G_2 be groups. Then every subgroup of $G_1 \times G_2$ is of the form $H_1 \times H_2$ for some subgroups $H_1 \leq G_1$ and $H_2 \leq G_2$.

False. The simplest counterexample is, when $G_1 = G_2 = \mathbf{Z}_2$, the subgroup $\langle(1, 1)\rangle$ is not of the product form.

5. 设群 G 在集合 X 上作用. 若某个元素 $g \in G$ 固定了 X 中的每个元素, 则 $g = 1$.

A group G acts on a set X. If for some $g \in G$, g fixes every element of X, then $g = 1$.

False. For example, for a trivial action, every element of the group G fixes every element of X.

6. 设 p 是一个素数, α 是一个自然数. 则每个阶为 $2p^\alpha$ 的群 G 都是可解群.

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

True. By Sylow's theorem, there exists a Sylow p-subgroup P of order p^α. Since it has index 2 inside G, it is normal and $G/P \cong \mathbf{Z}_2$. In addition, as a p-group, P is nilpotent and hence solvable. So G is solvable.

7. 交换环 R 中 I 和 J 为理想. 则理想 IJ 中每个元素是形如 ab 的样子, 其中 $a \in I$, $b \in J$.

Let R be a commutative ring and let I and J be ideals. Then every element of the ideal IJ is of the form ab with $a \in I$ and $b \in J$.

False. An element of IJ is typically a *finite sum* of products of the form ab with $a \in I$ and $b \in J$.

8. 在唯一分解整环中, 每个非零元素都可以唯一的写成素元的乘积, 在交换因子的意义下.

In a UFD, every nonzero element can be uniquely written as a product of prime elements, up to permutation.

False. This is not accurate: every nonzero nonunit element can be written as a product of prime elements, unique up to permutation and associates.

9. 设 F 是一个域, 一个非常数的多项式 $f(x)$ 是不可约的当且仅当 $F[x]/(f(x))$ 是一个域.

Let F be a field, a nonconstant polynomial $f(x)$ is irreducible if and only if $F[x]/(f(x))$ is a field.

True. The polynomial $f(x)$ is irreducible if and only if it is prime (and nonzero), which is the same as generating a maximal ideal (because $F[x]$ is a PID), which in turn is equivalent to $F[x]/(f(x))$ being a field.

10. 一个 p 群 G 作用在一个有限集合 X 上, 则作用的不动点的个数和 $\#X$ 模 p 同余.

Let G be a p-group acting on a finite set X. Then the number of fixed points of the action is congruent modulo p to $\#X$.

True. By orbit-stabilizer formula,

$$\#X = \sum_{\mathcal{O}} \#(G/\mathrm{Stab}_G(x)).$$

When $\mathrm{Stab}_G(x) \neq G$, the quotient $G/\mathrm{Stab}_G(x)$ has nontrivial p-power elements, so divisible by p, and when $G = \mathrm{Stab}_G(x)$, x is a fixed point of the action and $\mathcal{O} = \{x\}$.

Grading table

T/F	1	2	3	4	5	6	7	Total
/10	/10	/15	/20	/15	/15	/15	/10	

解答题一 (10 分) 设 R 是一个唯一分解整环, Q 为其分式域. 设 $f(x)$ 是 $R[x]$ 中次数 ≥ 1 的不可约多项式. 记 $f(x)$ 在 $Q[x]$ 中生成的理想为 I. 证明 $Q[x]/I$ 是一个域. (如果你引用书中或者讲义中的定理, 请明确指出你引用的定理是哪个.)

Let R be a UFD with fraction field Q and let $f(x)$ be an irreducible polynomial of degree ≥ 1 in $R[x]$. Let I denote the ideal in $Q[x]$ generated by $f(x)$. Prove that $Q[x]/I$ is a field. (If you want to cite a result from the lectures or books, make it clear which one you are using.)

证明. By Gauss Lemma, if $f(x)$ factors as $g(x)h(x)$ in $Q[x]$, then we may adjust $g(x)$ and $h(x)$ by elements in Q so that both $g(x)$ and $h(x)$ belong to $R[x]$. But $f(x)$ is irreducible in $R[x]$, so one of $g(x)$ and $h(x)$ is a unit in $R[x]$ and thus a unit in $Q[x]$. It follows that $f(x)$ is irreducible in $Q[x]$ and hence generates a maximal ideal, as $Q[x]$ is a PID. From this, we know that $Q[x]/I$ is a field. □

解答题二 (15 分) 证明每个阶为 $1947 = 3 \cdot 11 \cdot 59$ 的群都是循环群.

Prove that every group of order $1947 = 3 \cdot 11 \cdot 59$ is cyclic.

证明. Consider the number n_{59} of Sylow 59-group. By Sylow's theorems, $n_{59} | 3 \cdot 11$ and $n_{59} \equiv 1 \bmod 59$. So $n_{59} = 1$, i.e. the Sylow 59-group P_{59} is a normal subgroup, which itself is isomorphic to $\mathbf{Z}_{59}$.

Next, consider the conjugation action of G on P_{59}:

$$\varphi : G \to \mathrm{Aut}(P_{59}) \cong \mathbf{Z}_{59}^{\times} \simeq \mathbf{Z}_{58}.$$

It is clear that $P_{59} \subseteq \ker \varphi$. So $\#\mathrm{Im}\varphi$ divides $3dot11$. Yet as a subgroup of $\mathbf{Z}_{58}$, $\#\mathrm{Im}\varphi$ has order divides 58. So $\#\mathrm{Im}\varphi$ is trivial. In other words, $P_{59} \subseteq Z(G)$.

Now consider the number n_{11} and n_3 of Sylow 11-subgroups and 3-subgroups. We have

$$n_{11} \equiv 1 \bmod 11, \qquad n_{11} | 3 \cdot 59.$$

$$n_3 \equiv 1 \bmod 3, \qquad n_3 | 11 \cdot 59.$$

In fact Z_{59} belonging to the center implies that $n_3 | 11$ as the conjugation action of G on the set of Sylow 3-subgroups factors through the quotient by P_3 and P_{59}. From these divisibilities, we see that $n_{11} = n_3 = 1$. So the Sylow 11-subgroup P_{11} and Sylow 3-subgroup P_3 are both normal. It then follows that $G = P_3 \times P_{11} \times P_{59} \cong \mathbf{Z}_{1947}$.

□

解答题三 (20 分) 对正整数 $n \geq 3$, 用 D_{2n} 表示阶为 $2n$ 的二面体群.

(1) 求 D_8 中每个元素的阶.

(2) 证明: 对一个 D_8 的自同构 φ, $\varphi(r)$ 至多有 2 个选择, $\varphi(s)$ 至多有 4 个选择. 由此证明 $\#\mathrm{Aut}(D_8) \leq 8$.

(3) 证明: $D_8 \lhd D_{16}$. (这里, 我们将 D_8 中的旋转元视为 D_{16} 中的旋转元的平方.)

(4) 证明: $\mathrm{Aut}(D_8) \cong D_8$.

For a positive integer $n \geq 3$, let D_{2n} denote the dihedral group of order $2n$.

(1) Find the orders of elements of D_8.

(2) Show that, for an automorphism $\varphi : D_8 \to D_8$, $\varphi(r)$ has at most 2 possible choices, and $\varphi(s)$ has at most 4 possible choices. Deduce that $\#\mathrm{Aut}(D_8) \leq 8$.

(3) Show that $D_8 \lhd D_{16}$ (here the rotation element of D_8 is sent to the square of the rotation element of D_{16}.)

(4) Prove that $\mathrm{Aut}(D_8) \cong D_8$.

证明. (1) We write $D_{2n} = \langle r, s \mid r^n = s^2 = 1, srs = r^{-1}\}$ in the usual notation. We list of order of elements in the following table.

Elements	1	r	r^2	r^3	s	sr	sr^2	sr^3
Order	1	4	2	4	2	2	2	2

(2) An automorphism must preserve the order of elements. So $\varphi(r)$ can only be r or r^3. The element $\varphi(s)$ has a priori five choices: r^2, s, sr, sr^2, sr^3. But if $\varphi(s) = r^2$, then $\mathrm{Im}\varphi \subseteq \langle r \rangle$. It cannot be an isomorphism. So $\varphi(s)$ has at most 4 choices. From this, we see that $\#\mathrm{Aut}(D_8) \leq 8$.

(3) If we write $D_{16} = \langle r_{16}, s \mid r_{16}^8 = s^2 = 1, sr_{16}s = r_{16}^{-1} \rangle$, then $D_8 = \langle r_{16}^2, s \rangle$. It suffices to check that

$$r_{16} D_8 r_{16}^{-1} \subseteq D_8 \quad \text{and} \quad s D_8 s^{-1} \subseteq D_8.$$

(Then the equalities hold by counting the number of elements.) To check inclusion, it is enough to check for generators. The first inclusion follows from that

$$r_{16} r_{16}^2 r_{16}^{-1} = r_{16}^2 \in D_8 \quad \text{and} \quad r_{16} s r_{16}^{-1} = r_{16}^2 s \in D_8.$$

The second inclusion follows from that

$$s r_{16}^2 s^{-1} = r_{16}^{-2} \in D_8 \quad \text{and} \quad s s s^{-1} = s \in D_8.$$

(4) Now, consider the conjugation action of D_{16} on D_8:

$$\varphi : D_{16} \to \mathrm{Aut}(D_8).$$

We compute the kernel of this map φ, it is the set of elements that commutes with s and with r_{16}^2.

For elements of the type r_{16}^a, it clearly commutes with r_{16}^2, but $sr_{16}^a s^{-1} = r^{-a}$, which is equal to r_{16}^a if and only if $a = 4$, i.e. the element r_{16}^8.

For elements of the form sr_{16}^a, $r_{16}^2 sr_{16}^a r_{16}^{-2} = sr_{16}^{a-4}$, so it never commutes with r^2.

It follows that $\ker\varphi = \{1, r_{16}^4\}$. So $\#\mathrm{Im}(\varphi) = 8$. Combining this with (2), we deduce that

$$\mathrm{Aut}(D_8) \cong \mathrm{Im}(D_{16}) \cong D_{16}/\langle r_{16}^4 \rangle.$$

It is clear that $D_{16}/\langle r_{16}^4 \rangle \cong \langle r_{16}, s \mid r_{16}^4 = s^2 = 1, sr_{16}s = r_{16}^{-1} \rangle$ is isomorphic to D_8. $\square$

解答题四 (15 分) 记群 G 的中心为 $Z(G)$. 记 $\lambda : G \to S_G$ 为群 G 在自己上的左平移作用, 并简记 $\lambda_g = \lambda(g)$, 即 $\lambda_g(h) = gh$ $(g, h \in G)$. 记 $\mu : G \to S_G$ 为群 G 在自己上的右平移作用, 并简记 $\mu_g = \mu(g)$, 即 $\mu_g(h) = hg^{-1}$ $(g, h \in G)$.

(1) 证明: 左作用 λ 和右作用 μ 交换, 即对 $g, h \in G$, $\lambda_g \circ \mu_h = \mu_h \circ \lambda_g$.

(2) 证明: $\lambda_g = \mu_g$ 当且仅当 g 是中心 $Z(G)$ 中阶为 1 或 2 的元素.

(3) 证明: 交 $\lambda(G) \cap \mu(G)$ 恰好等于 $\lambda(Z(G)) = \mu(Z(G))$.

Let G be a group with center $Z(G)$. Let $\lambda : G \to S_G$ be the left translation action of G on itself, and we write $\lambda_g = \lambda(g)$ so that $\lambda_g(h) = gh$ for $g, h \in G$. Similarly, let $\mu : G \to S_G$ be the right translation action of G on itself, and we write $\mu_g := \mu(g)$ so that $\mu_g(h) = hg^{-1}$.

(1) Prove that the action of λ and μ commute with each other, i.e. for $g, h \in G$, $\lambda_g \circ \mu_h = \mu_h \circ \lambda_g$.

(2) Prove that $\lambda_g = \mu_g$ if and only if g is an element of order 1 or 2 in the center $Z(G)$.

(3) Prove that the intersection $\lambda(G) \cap \mu(G)$ in G is equal to $\lambda(Z(G)) = \mu(Z(G))$.

证明. (1) For $x \in G$, we have

$$\lambda_g \circ \mu_h(x) = \lambda_g(xh^{-1}) = gxh^{-1}.$$

$$\mu_h \circ \lambda_g(x) = \mu_h(gx) = gxh^{-1}.$$

So $\lambda_g \circ \mu_h = \mu_h \circ \lambda_g$, i.e. the left and right actions commute.

(2) If $\lambda_g = \mu_g$, then for any $x \in G$, we have $\lambda_g(x) = \mu_g(x)$, i.e. $gx = xg^{-1}$. Setting $x = 1$ gives $g^2 = 1$. Putting this back to $gx = xg^{-1}$ gives that $gx = xg$ for every $x \in G$. So $g \in Z(G)$. Conversely, when $g^2 = 1$ and $g \in Z(G)$, this implies that $\lambda_g = \mu_g$.

(3) An element in the intersection $\lambda(G) \cap \mu(G)$ corresponds to an equality $\lambda_g = \mu_h$ for some $g, h \in G$. This means that for $x \in G$, $\lambda_g(x) = \mu_h(x)$ or equivalently $gx = xh^{-1}$. Putting $x = 1$ gives $g = h^{-1}$. Putting this back to the equality $gx = xh^{-1}$ gives $gx = xg$, i.e. $g \in Z(G)$. This implies that $\lambda(G) \cap \mu(G)$ is contained in $\lambda(Z(G))$ and in $\mu(Z(G))$.

Conversely, if we take any $g \in Z(G)$, $\lambda_g(x) = gx = xg = \mu_{g^{-1}}(x)$. So $\lambda(Z(G)) = \mu(Z(G))$ is contained in $\lambda(G) \cap \mu(G)$. □

解答题五 (15 分) 设 R 是一个唯一分解整环, 恰有两个互不相伴的素元 p, q 使得任意一个素元都与 p 或 q 相伴.

(1) 对正整数 m, n, 证明理想 $(p^m, q^n) = R$.

(2) 证明 R 是一个主理想整环.

Let R be a UFD with two nonassociate prime elements p and q such that every prime element is an associate of either p or q.

(1) Given positive integers m, n, prove that the ideal $(p^m, q^n) = R$.

(2) Deduce that R is a PID.

证明. (1) Consider $p^m + q^n \in (p^m, q^n)$. We note that neither p nor q divides $p^m + q^n$, so p and q does not appear in the factorization of $p^m + q^n$. Yet R has only two primes, $p^m + q^n$ must be a unit. So $(p^m, q^n) = R$.

(2) Let I be a nonunit ideal of R. For each nonzero element x of I, it factors as $x = p^{m(x)}q^{n(x)}u(x)$ in R, where $m(x), n(x) \in \mathbb{Z}_{\geq 0}$ and $u(x)$ is a unit. Let $m := \min_x m(x)$ and $n := \min_x n(x)$. We claim that $I = (p^m q^n)$. Clearly, by definition, $p^m q^n$ divides every $x = p^{m(x)}q^{n(x)}u(x)$. It remains to show that $p^m q^n \in I$.

Let $x \in I\backslash\{0\}$ and $y \in I\backslash\{0\}$ be so that $m = m(x)$ and $n = n(y)$. If $n = n(x)$ or $m = m(y)$, then $p^m q^n$ is a unit multiple of x or y, respectively, and thus $p^m q^n \in I$. Now we assume that $n > n(x)$ and $m > m(y)$. By (1), we know that

$$(q^{n(x)-n}u(x), p^{m(y)-m}u(y)) = R.$$

So there exists $r, s \in R$ such that

$$rq^{n(x)-n}u(x) + sp^{m(y)-m}u(y) = 1.$$

$$p^m q^n = rp^m q^{n(x)}u(x) + sp^{m(y)}q^n u(y) = rx + sy.$$

So $p^m q^n \in I$. Thus R is a PID. □

解答题六 (15 分)

对素数 p, 用 $\Phi_p(x) := \dfrac{x^p-1}{x-1} \in \mathbb{Z}[x]$ 记 p 次分圆多项式.

(1) 证明 $\Phi_p(x)$ 在 $\mathbb{Q}[x]$ 中不可约. (可以引用一般性定理, 不可以直接引用关于 Φ_p 的定理.)

(2) 记 $\zeta_p = e^{2\pi i/p}$ 为一个本元 p 次单位根. 证明：将 x 映到 ζ_p 建立了一个如下的同构

$$\mathbb{Z}[x]/(\Phi_p(x)) \xrightarrow{\cong} \mathbb{Z}[\zeta_p] = \{a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2} \mid a_0, \ldots, a_{p-2} \in \mathbb{Z}\}.$$

特别地, $\mathbb{Z}[\zeta_p]$ 是一个整环.

(3) 证明: 如果 n 是一个正整数在 $\mathbb{Z}[\zeta_p]$ 中被 $\zeta_p - 1$ 整除, 则 n 是 p 的倍数.

(在这道题中, 不可以使用代数数论中的工具. 证明只可以使用对多项式环和商环的讨论.)

Let p be a prime number. Let $\Phi_p(x) := \dfrac{x^p-1}{x-1} \in \mathbb{Z}[x]$ denote the pth cyclotomic polynomial.

(1) Show that $\Phi_p(x)$ is irreducible in $\mathbb{Q}[x]$. (It is okay to use a "general" theorem, but not okay to use a result specific to $\Phi_p(x)$.)

(2) Let $\zeta_p = e^{2\pi i/p}$ denote a primitive pth root of unity. Prove that there is an isomorphism

$$\mathbb{Z}[x]/(\Phi_p(x)) \xrightarrow{\cong} \mathbb{Z}[\zeta_p] = \{a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2} \mid a_0, \ldots, a_{p-2} \in \mathbb{Z}\}$$

sending x to ζ_p. In particular $\mathbb{Z}[\zeta_p]$ is an integral domain.

(3) Show that if n is an integer such that $\zeta_p - 1$ divides n in $\mathbb{Z}[\zeta_p]$, then n is divisible by p.

(You are not allowed to use heavy tools from algebraic number theory. Just manipulate with the polynomial ring and its quotients.)

证明. (1) Note that $\Phi_p(x+1) = \dfrac{(x+1)^p - 1}{x} = x^{p-1} + px^{p-2} + \cdots + p$. By Eisenstein criterion, p divides all the non-leading coefficients and p^2 does not divide the constant coefficient; so $\Phi_p(x+1)$ is irreducible in $\mathbb{Z}[x]$, and thus $\Phi_p(x)$ is irreducible in $\mathbb{Z}[x]$. By Gauss' lemma, $\Phi_p(x)$ is also irreducible over $\mathbb{Z}[x]$.

(2) The natural homomorphism

$$\varphi : \mathbb{Z}[x] \to \mathbb{Z}[\zeta_p]$$

sending x to ζ_p clearly has the property that $\ker\varphi$ contains $\Phi_p(x)$. So we have a homomorphism

$$\bar{\varphi} : \mathbb{Z}[x]/(\Phi_p(x)) \to \mathbb{Z}[\zeta_p].$$

For the quotient $\mathbb{Z}[x]/(\Phi_p(x))$, each coset can be represented by a polynomial $a_0 + a_1 x + \cdots + a_{p-2}x^{p-2}$ (as any terms that have degree $\geq p-1$ can be substituted into lower degree terms using $\Phi_p(x)$). From this, it is clear that $\bar{\varphi}$ is an isomorphism.

(3) If n is divisible by $\zeta_p - 1$, then $n = (\zeta_p - 1)g(\zeta_p)$ for some polynomial $g(x) \in \mathbb{Z}[x]$. Using the isomorphism from (2), we see that

$$n + (\Phi_p(x)) = (x-1)g(x) + (\Phi_p(x)).$$

So there exists some polynomial $h(x) \in \mathbb{Z}[x]$ such that

$$n - (x-1)g(x) = \Phi_p(x)h(x)$$

Evaluating this equality at $x = 1$ gives $n = \Phi_p(1)h(1)$. But $\Phi_p(1) = p$ so n is divisible by p. $\square$

解答题七 (10 分) 对素数 p, G 是一个 p-群. 设 A 是一个 G 中的极大正规交换群. 证明: A 是 G 中的极大交换群.

Let p be a prime, let G be a finite p-group. Let A be a maximal normal abelian subgroup of G. Prove that A is also a maximal abelian subgroup of G.

证明. Suppose that A is strictly contained in another abelian group A'. Let H be the subgroup of G generated by $gA'g^{-1}$ for all $g \in G$; clearly H is a normal subgroup of G and contains A.

We claim that H centralize A. For this, it is enough to check that for every $a' \in A'$ and $g \in G$, $ga'g^{-1}$ commutes with every element $a \in A$. Indeed,

$$ga'g^{-1} \cdot a \cdot ga'^{-1}g^{-1} = ga' \cdot g^{-1}ag \cdot a'^{-1}g^{-1}.$$

But A is normal, so $g^{-1}ag \in A$; so a' commutes with $g^{-1}ag$, and thus the above is equal to

$$g \cdot g^{-1}ag \cdot a' \cdot a'^{-1}g^{-1} = a.$$

Now consider $\overline{G} := G/A$ and let $\pi : G \to \overline{G}$ be the projection. Write $\bar{H}$ for the image of H, which is a nontrivial p-group. By a proposition we have proved in class, $\bar{H}$ intersects nontrivially with the center $Z(\bar{G})$. Pick any element $\bar{n} \in \bar{H} \cap Z(\bar{G})$, and set $\bar{N} := \langle \bar{n} \rangle \subseteq \bar{G}$. Since $\bar{N} \subseteq Z(\bar{G})$, $\bar{N}$ is a normal subgroup of $\bar{G}$, and thus N is a normal subgroup of G.

In addition, if we pick a preimage $n \in H$ of $\bar{n} \in \bar{H}$, then n centralizes A and thus N is abelian.

This then gives a normal abelian subgroup N strictly containing A, we arrive at a contradiction. □

An alternative proof is to take the centralizer $Z_G(A)$ of A inside G. Since A is normal, $Z_G(A)$ is a normal subgroup of G: for any $z \in Z_G(A)$, $g \in G$, we want to show that $gzg^{-1} \in Z_G(A)$, i.e. for $a \in A$,

$$gzg^{-1} \cdot a \cdot gz^{-1}g^{-1} = gz \cdot g^{-1}ag \cdot z^{-1}g^{-1} = g(g^{-1}ag)zz^{-1}g^{-1} = a,$$

where we used that $g^{-1}ag \in A$ by normality of A. So $gzg^{-1} \in Z_G(A)$ and thus $Z_G(A) \lhd G$.

If A is not a maximal abelian subgroup, then $A \subsetneq Z_G(A)$ is a strict inclusion.

Consider the subgroup $Z_G(A)/A \subseteq G/A$; it is a normal subgroup. We note that $(Z_G(A)/A) \cap Z(G/A)$ is nontrivial. Picking an element from this intersection, and the rest of the argument is similar to above.