抽象代数综合测验

一、不定项选择

1. G 是群，e 是单位元，H 是 G 的子集，下面说法正确的是：

   (a) 如果 H 是 G 的子群，则 $e \in H$ 且 $\forall a, b \in H, ab \in H$

   (b) 如果 $\forall a \in H$ 有 $a^{-1} \in H$，且 $\forall a, b \in H$ 有 $ab \in H$，则 H 是 G 的子群

   (c) 如果 $e \in H$ 且对任意 $a, b \in H$ 有 $ab \in H$，则 H 是 G 的子群

   (d) H 是 G 的子群当且仅当 $\forall a, b \in H$ 有 $b^{-1}a \in H$

   答案与解析： **A, B, D**. A 是子群的必要条件。B 是两步判别法（充分条件）。D 是一步判别法（充要条件）。B 和 D 在严格意义上都隐含了 H 非空的假设。C 是错误的，缺少逆元条件。

2. 下面哪些集合及其上面的加法、乘法运算不构成域：

   (a) $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ 关于普通复数加法和乘法构成的环

   (b) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ 关于普通实数加法和乘法构成的环

   (c) $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ 关于模 6 加法和模 6 乘法构成的环

   (d) $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ 关于模 7 加法和模 7 乘法构成的环

   答案与解析： **C**. 这是一个“选非题”。环 $\mathbb{Z}_n$ 是域当且仅当 n 是素数。6 不是素数，$\mathbb{Z}_6$ 中有零因子（如 $2 \cdot 3 = 0$），所以不是域。其他选项都是域。

3. $U(9) = \{1, 2, 4, 5, 7, 8\}$ 关于正规子群 $N = \{1, 8\}$ 得到商群 $G = U(9)/N$，下列说法正确的是：

   (a) $G = \{\{1, 8\}, \{2, 4\}, \{5, 7\}\}$

   (b) G 的单位元是 $\{2, 4\}$

   (c) $2N$ 的逆元是 $4N$

   (d) $2N$ 和 $5N$ 的运算结果是 $7N$

答案与解析： **C**. 只有一个选项是事实正确的。A 的陪集计算错误。B 的单位元应为 $N = \{1, 8\}$。D 的运算结果应为 N。C 的计算 $(2N)(4N) = (2 \cdot 4)N = 8N = N$ 正确。

4. R 是 S 的子环，下面说法正确的是：

   (a) 若 S 无零因子，则 R 也无零因子

   (b) 若 R 无零因子，则 S 也无零因子

   (c) 若 S 有单位元，则 R 也有单位元

   (d) 若 R 有单位元，则 S 也有单位元

   答案与解析： **A**. 只有一个选项是普遍成立的。无零因子（整环）的性质会被子环继承。B, C, D 都有明确的反例。

5. 环同态 $\varphi : S \to S'$ 下面说法正确的是：

   (a) 若 R 是 S 的子环，则 $R' = \varphi(R)$ 是 S' 的子环

   (b) 若 I 是 S 的理想，则 $I' = \varphi(I)$ 是 S' 的理想

   (c) 若 R' 是 S' 的子环，则 $R = \varphi^{-1}(R')$ 是 S 的子环

   (d) 若 I' 是 S' 的理想，则 $I = \varphi^{-1}(I')$ 是 S 的理想

   答案与解析： **A, C, D**. A, C, D 都是环同态的基本定理。B 是错误的，理想的同态像一般只是子环，不一定是理想（除非 φ 是满射）。

二、计算与证明

6. $U(9) = \{1, 2, 4, 5, 7, 8\}$ 是循环群吗，并求出其所有非平凡子群。

   解：

(a) **判断是否是循环群：** 检验元素 2 的阶：
$2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 \equiv 7$, $2^5 \equiv 5$, $2^6 \equiv 1 \pmod 9$。
因为元素 2 的阶为 6，等于群的阶，所以 $U(9)$ 是由 2 生成的循环群。

(b) **求非平凡子群：** 子群的阶必须是 6 的因子（1, 2, 3, 6）。非平凡子群的阶为 2 和 3。

- 阶为 2 的子群：由 $2^{6/2} = 2^3 = 8$ 生成，为 $\langle 8 \rangle = \{1, 8\}$。
- 阶为 3 的子群：由 $2^{6/3} = 2^2 = 4$ 生成，为 $\langle 4 \rangle = \{1, 4, 7\}$。

结论： $U(9)$ 是循环群。它有两个非平凡子群：$\{1, 8\}$ 和 $\{1, 4, 7\}$。

7. 求 $\mathbb{Z}_6$ 到 $\mathbb{Z}_{12}$ 的所有环同态。

解： 设 $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_{12}$ 是环同态，令 $k = \varphi(1)$。k 必须满足:

(i) k 是幂等元: $k^2 \equiv k \pmod{12}$。

(ii) 映射良定义: $6k \equiv 0 \pmod{12}$。

步骤 1: 在 $\mathbb{Z}_{12}$ 中找幂等元，解得 $k \in \{0, 1, 4, 9\}$。
步骤 2: 检验这些幂等元是否满足 $6k \equiv 0 \pmod{12}$。

- $k = 0 : 6 \cdot 0 = 0 \equiv 0 \pmod{12}$ (满足)
- $k = 1 : 6 \cdot 1 = 6 \not\equiv 0 \pmod{12}$ (不满足)
- $k = 4 : 6 \cdot 4 = 24 \equiv 0 \pmod{12}$ (满足)
- $k = 9 : 6 \cdot 9 = 54 \equiv 6 \pmod{12}$ (不满足)

结论： 存在两个环同态，由 $k = 0$ 和 $k = 4$ 确定：$\varphi_1(x) = 0$ 和 $\varphi_2(x) = 4x \pmod{12}$。

8. 在商环 $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle$ 中进行如下计算。

基本关系：在商环中，$x^2 + 1 = 0$，即 $x^2 = -1 \equiv 2 \pmod{3}$。

(a) **求加法单位元和乘法单位元**

答： 加法单位元是 0，乘法单位元是 1。

(b) **计算** $2x + 1 \otimes 2x + 2$

答：

$$\begin{aligned}(2x+1)(2x+2) &= 4x^2 + 4x + 2x + 2 \\ &\equiv x^2 + 6x + 2 \pmod{3} \\ &\equiv x^2 + 2 \\ &\equiv 2 + 2 \quad (\text{因为 } x^2 = 2) \\ &\equiv 4 \equiv 1 \pmod{3}\end{aligned}$$

(c) **计算** $2x + 1 \oplus 2x + 2$ **及其加法阶**

答：

- **计算：** $(2x + 1) + (2x + 2) = 4x + 3 \equiv x \pmod{3}$。
- **加法阶：** 我们求 x 的加法阶。
  - $1 \cdot x = x$
  - $2 \cdot x = x + x = 2x$
  - $3 \cdot x = x + x + x = 3x = 0$

所以 x 的加法阶是 **3**。

(d) **计算 $x+2\otimes 2x+1$ 及其乘法阶**

答：

- **计算：**

$$\begin{aligned}(x+2)(2x+1) &= 2x^2+x+4x+2\\ &\equiv 2x^2+5x+2 \pmod 3\\ &\equiv 2x^2+2x+2\\ &\equiv 2(2)+2x+2 \quad (\text{因为 } x^2=2)\\ &\equiv 4+2x+2=2x+6\equiv 2x \pmod 3\end{aligned}$$

- **乘法阶：**我们求 $2x$ 的乘法阶。令 $y=2x$。
  - $y^1=2x$
  - $y^2=(2x)^2=4x^2\equiv x^2\equiv 2$
  - $y^3=y^2\cdot y=2\cdot 2x=4x\equiv x$
  - $y^4=(y^2)^2=(2)^2=4\equiv 1$

  所以 $2x$ 的乘法阶是 **4**。

9. 设 $(R,+,\cdot)$ 是一个有单位元 1 的环，定义新运算:

$$x\oplus y=x+y-1 \quad \text{和} \quad x\otimes y=x+y-xy$$

求证 $(R,\oplus,\otimes)$ 也是一个有单位元的环。

证明：

- $(R,\oplus)$ **是阿贝尔群**: 封闭性、结合律、交换律易证。
  - 加法单位元 $e_\oplus$: $x\oplus e_\oplus=x \implies x+e_\oplus-1=x \implies e_\oplus=1$。
  - 加法逆元 x': $x\oplus x'=1 \implies x+x'-1=1 \implies x'=2-x$。
- $(R,\otimes)$ **结合律**: 经计算 $(x\otimes y)\otimes z=x\otimes(y\otimes z)=x+y+z-xy-xz-yz+xyz$。
- **分配律**: $x\otimes(y\oplus z)=(x\otimes y)\oplus(x\otimes z)$。经计算, 等式两边均为 $2x+y+z-xy-xz-1$。
- **乘法单位元** $e_\otimes$: $x\otimes e_\otimes=x \implies x+e_\otimes-xe_\otimes=x \implies e_\otimes(1-x)=0$。为对所有 x 成立，必有 $e_\otimes=0$。

结论：$(R,\oplus,\otimes)$ 满足所有环公理，且有乘法单位元 0，是一个有单位元的环。

10. 求证 $\langle x^2+1\rangle$ 是否为 $\mathbb{Z}_2[x]$ 的极大理想。

证明：根据定理，在域 F 上，理想 $\langle p(x)\rangle$ 是极大理想当且仅当 $p(x)$ 在 F 上不可约。这里 $F=\mathbb{Z}_2=\{0,1\}$，多项式为 $p(x)=x^2+1$。我们检验 $p(x)$ 在 $\mathbb{Z}_2$ 中是否有根：

- $p(0) = 0^2 + 1 = 1 \neq 0$
- $p(1) = 1^2 + 1 = 1 + 1 = 0 \pmod 2$

因为 $p(x)$ 在 $\mathbb{Z}_2$ 中有根 $x = 1$，所以 $p(x)$ 在 $\mathbb{Z}_2$ 上是可约的 (事实上 $x^2 + 1 = (x + 1)^2$)。
结论： 由于 $x^2 + 1$ 在 $\mathbb{Z}_2$ 上可约，所以 $\langle x^2 + 1 \rangle$ **不是** $\mathbb{Z}_2[x]$ 的极大理想。

A 附录：补充证明

A.1 一般环同态性质的证明

设 $\varphi : R \to S$ 是一个环同态。

命题 A.1 (子环的像)**.** 若 A 是 R 的子环，则 $\varphi(A)$ 是 S 的子环。

证明. 要证明 $\varphi(A)$ 是 S 的子环，需验证其对减法和乘法封闭且非空。

(1) **非空性**: 因为 A 是子环, 所以 $0_R \in A$。根据同态性质, $\varphi(0_R) = 0_S$, 因此 $0_S \in \varphi(A)$, 故 $\varphi(A)$ 非空。

(2) **对减法封闭**: 任取 $s_1, s_2 \in \varphi(A)$。则存在 $a_1, a_2 \in A$ 使得 $s_1 = \varphi(a_1)$ 且 $s_2 = \varphi(a_2)$。于是 $s_1 - s_2 = \varphi(a_1) - \varphi(a_2) = \varphi(a_1 - a_2)$。因为 A 是子环，‘$a_1 - a_2 \in A$‘，所以 $\varphi(a_1 - a_2) \in \varphi(A)$。

(3) **对乘法封闭**: $s_1 \cdot s_2 = \varphi(a_1) \cdot \varphi(a_2) = \varphi(a_1 \cdot a_2)$。因为 A 是子环，‘$a_1 \cdot a_2 \in A$‘，所以 $\varphi(a_1 \cdot a_2) \in \varphi(A)$。

因此，$\varphi(A)$ 是 S 的子环。 □

命题 A.2 (理想/子环的原像)**.** 若 I' 是 S 的理想（或子环），则 $\varphi^{-1}(I')$ 是 R 的理想（或子环）。

证明. 这里的 $\varphi^{-1}(I')$ 指的是原像集 $\{r \in R \mid \varphi(r) \in I'\}$。

(1) 我们先证明若 I' 是子环，则 $\varphi^{-1}(I')$ 是子环。

- **非空性**: 因为 I' 是子环，所以 $0_S \in I'$。由于 $\varphi(0_R) = 0_S$，所以 $0_R \in \varphi^{-1}(I')$，故 ‘$\varphi^{-1}(I')$‘ 非空。
- **对减法封闭**: 任取 $a, b \in \varphi^{-1}(I')$。这意味着 $\varphi(a) \in I'$ 且 $\varphi(b) \in I'$。于是 $\varphi(a - b) = \varphi(a) - \varphi(b) \in I'$。因此，‘$a - b \in \varphi^{-1}(I')$‘。
- **对乘法封闭**: $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \in I'$。因此，‘$a \cdot b \in \varphi^{-1}(I')$‘。

(2) 现在证明若 I' 是理想，则 $\varphi^{-1}(I')$ 满足吸收律。任取 $x \in \varphi^{-1}(I')$ 和环中任意元素 $r \in R$。根据定义，$\varphi(x) \in I'$。我们有 $\varphi(rx) = \varphi(r) \cdot \varphi(x)$。因为 I' 是 S 的理想，它能吸收来自 S 的任何元素 $\varphi(r)$ 的乘积。所以 $\varphi(r) \cdot \varphi(x) \in I'$。因此，‘$rx \in \varphi^{-1}(I')$‘。同理可证 ‘$xr \in \varphi^{-1}(I')$‘。

综上，若 I' 是理想，则 $\varphi^{-1}(I')$ 是 R 的理想。 □

A.2 极大理想与不可约多项式

定理 A.3. 设 F 是一个域，$p(x)$ 是多项式环 $F[x]$ 中的一个多项式。由 $p(x)$ 生成的理想 $\langle p(x)\rangle$ 是 $F[x]$ 中的极大理想，当且仅当 $p(x)$ 在域 F 上是不可约多项式。

证明. **若 $\langle p(x)\rangle$ 是极大理想，则 $p(x)$ 不可约。**
我们用反证法。假设 $p(x)$ 是**可约**的。则存在次数更低的多项式 $a(x), b(x) \in F[x]$ 使得 $p(x) = a(x)b(x)$。这导致理想链 $\langle p(x)\rangle \subset \langle a(x)\rangle \subset F[x]$。由于 $\langle p(x)\rangle$ 是极大理想，任何严格包含它的理想只能是 $F[x]$。所以 $\langle a(x)\rangle = F[x]$。这意味着 $a(x)$ 是一个单位（非零常数），其次数为 0。这与 $a(x)$ 是 $p(x)$ 的一个次数更低的非平凡因子相矛盾。故 $p(x)$ 必须是不可约的。

若 $p(x)$ 不可约，则 $\langle p(x)\rangle$ 是极大理想。
设 I 是 $F[x]$ 中的一个理想，且 $\langle p(x)\rangle \subseteq I \subseteq F[x]$。因为 $F[x]$ 是主理想整环，所以 $I = \langle g(x)\rangle$。包含关系 $\langle p(x)\rangle \subseteq \langle g(x)\rangle$ 意味着存在 $h(x) \in F[x]$ 使得 $p(x) = g(x)h(x)$。由于 $p(x)$ 是不可约的，这个分解只有两种可能：(1) $g(x)$ 是一个单位，此时 $I = \langle g(x)\rangle = F[x]$。(2) $h(x)$ 是一个单位，此时 $g(x)$ 与 $p(x)$ 相伴，这意味着 $I = \langle g(x)\rangle = \langle p(x)\rangle$。因此，$\langle p(x)\rangle$ 是一个极大理想。 □

A.3 绕过定理的直接证明方法

命题 A.4. 在 $\mathbb{Z}_3[x]$ 中，理想 $I_0 = \langle x^2 + 1\rangle$ 是极大理想。

证明. 设 I 是一个理想，且满足 $I_0 \subset I \subseteq \mathbb{Z}_3[x]$。我们的目标是证明 $I = \mathbb{Z}_3[x]$。

(1) 因为 $I_0 \subset I$，所以 I 中至少存在一个多项式 $f(x) \notin I_0$。

(2) 使用除法算法：$f(x) = q(x)(x^2 + 1) + r(x)$，其中 $r(x) = 0$ 或 $\deg(r) < 2$。

(3) $r(x) = f(x) - q(x)(x^2 + 1)$。由于 $f(x) \in I$ 且 $q(x)(x^2 + 1) \in I_0 \subset I$，则 $r(x) \in I$。

(4) 因为 $f(x) \notin I_0$，所以余式 $r(x)$ 不能为零。因此 $r(x) = ax + b$，其中 $a, b \in \mathbb{Z}_3$ 不全为零。

(5) 既然 $ax + b \in I$，那么 $(ax + b)(ax - b) = a^2x^2 - b^2$ 也在 I 中。

(6) 在 $\mathbb{Z}_3[x]$ 中，我们有 $x^2 \equiv -1 \equiv 2 \pmod{I_0}$。因此 $a^2x^2 - b^2 = a^2(2) - b^2 = 2a^2 - b^2$。这个常数 $c = 2a^2 - b^2$ 在理想 I 中。

(7) 我们证明这个常数 c 不为零。假设 $2a^2 = b^2$。若 $a = 0$，则 $b = 0$，与 $ax + b$ 非零矛盾。若 $a \neq 0$，则 $a^2 = 1$，代入得 $2 = b^2$，但在 $\mathbb{Z}_3$ 中没有元素的平方等于 2。

(8) 因此，常数 c 是一个非零常数（即 1 或 2），它是一个单位。

(9) 既然单位 $c \in I$，它的逆元 c^{-1} 存在于 $\mathbb{Z}_3[x]$ 中。根据理想的吸收律，$c^{-1} \cdot c = 1$ 也必须在理想 I 中。

(10) 一旦理想 I 包含了乘法单位元 1，那么它必然是整个环，即 $I = \mathbb{Z}_3[x]$。

□

证明 6 阶群 G 的元素只能是 1 阶、2 阶、3 阶和 6 阶，显然不可能是都是 1 阶元，如果都是 2 阶元，则对任意的 $a \in G$ 有 $a^2 = e$，从而 $a = a^{-1}$，即 G 的任意元素的逆都是这个元素自己。从而对任意 $a, b \in G$,

$$(ab)(ba) = a(bb)a = a(e)a = aa = e$$

也即 $(ab)^{-1} = ba$，但每个元素的逆元就是它自己，所以以 $ab = ba$，也即这时 G 是交换群，从而对于非单位元的两个不同元素 a, b, $H = \{e, a, b, ab\}$ 是 G 的子群，但 6 阶群不可能有 4 阶子群，矛盾！因此 6 阶群不可能所有元素都是 2 阶元，也即存在 3 阶元 g，或者 6 阶元 g。若 g 是 3 阶元，则 $H = \{e, g, g^2\}$ 是 G 的 3 阶子群，若 g 是 6 阶元，则 $H = \{e, g^2, g^4\}$ 是 G 的 3 阶子群。这就证明了 6 阶群必存在 3 阶子群。

若 6 阶群 G 存在两个不同的 3 阶子群 H 和 K，那么 $H \cap K$ 也 G 的子群，且由于 $H \cap K$ 也都是 H 和 K 的真子群，因此根据拉格朗日定理，必有 $H \cap K = \{e\}$，从而

$$|G| \geq |HK| = \frac{|H| \cdot |K|}{|H \cap K|} = \frac{3 \cdot 3}{1} = 9$$

与 G 是 6 阶群矛盾！因此必有 $H = K$，即 G 只有 1 个 3 阶子群。 □