期中考试

试卷共 8 页, 共 16 题, 满分 30 分.

判断题, 填空题: 无需写出证明.

1. (1 分) 使用命题逻辑的自然演绎. 对于任何公式 φ, 有 $\vdash \varphi$ 当且仅当 $\vDash \varphi$.

   解 是

2. (1 分) 去掉 RAA 的命题逻辑自然演绎系统可以推出 $P \to \neg\neg P$.

   解 是

3. (1 分) 在满足 ZFC 的模型中, 可以给每个 S 赋予一个"层数"$h_S \in \mathbb{N}$, 使得对于任何 $A \in S$, 都有 $h_A < h_S$.

   解 否

   $0 \in 1 \in 2 \in \dots$ 且都在 $\mathbb{N}$ 中.

4. (1 分) 对任意素数 p, 大小为 $2p$ 的群都是阿贝尔群.

   解 否

   反例为二面体群 D_p.

5. (1 分) 对任意素数 p, 大小为 p^2 的群都是阿贝尔群.

   解 是

   课上例题.

6. (1 分) 在主理想整环 (PID) $\mathcal{R}$ 中, 定义预序关系 $x \le y$ 表示 $x \mid y$. 那么以下定义的 $\gcd, \gcd'$ 等价.

   - $\gcd(x, y)$ 是最大的能同时整除 x, y 的数 (不唯一).
   - $\gcd'(x, y)$ 是 $ax + by$ 中最小的数 (不唯一).

   解 是

   一方面 $\gcd(x, y) \mid x, y, ax + by, \gcd'(x, y)$.

   另一方面, $\gcd'$ 的定义说明 $(x, y) = (\gcd'(x, y))$, 所以 $\gcd'(x, y) \mid x, y, \gcd(x, y)$.

7. (1 分) 对任意不可约多项式 $f(x) \in \mathbb{F}[x]$, 令 $\mathbb{K}/\mathbb{F}$ 是一个扩域且 $f(x) = 0$ 在 $\mathbb{K}$ 中有解, 那么 $f(x)$ 在 $\mathbb{K}$ 中分裂. (分裂指可以拆成一次式的乘积.)

解 否

反例为 $x^3 - 2 \in \mathbb{R}[x]$, 在 $\mathbb{R}[\sqrt[3]{2}]$ 中有解但不分裂.

8. (1 分) 对任意 $n, m \in \mathbb{N}_+$ 满足 $0 < m < 2n$, $\binom{2n}{m}$ 都是偶数.

解 否

$\binom{6}{2} = 15$.

9. (1 分) $\mathbb{F}_2[x]$ 中有几个 (首一的) 2026 次不可约多项式. (1013 是素数.)

解 $\dfrac{2^{2026} - 2^{1013} - 2}{2026}$

$x^{2^{2026}} - x$ 是所有次数为 1,2,1013,2026 的不可约多项式的乘积. $x^{2^{1013}} - x$ 是所有次数为 1,1013 的不可约多项式的乘积. $x^{2^2} - x$ 是所有次数为 1,2 的不可约多项式的乘积. $x^2 - x$ 是所有次数为 1 的不可约多项式的乘积. 因此 $(x^{2^{2026}} - x)(x^2 - x)/(x^{2^{1013}} - x)(x^{2^2} - x)$ 是所有 1013 次不可约多项式的乘积. 说明 1013 次不可约多项式的个数为 $(2^{2026} - 2^{1013} - 2^2 + 2)/2026$.

10. (1 分) 令 a_n 表示 $\mathrm{Sym}(n+1)$ 的大小, 写出其对应的指数生成函数 $\tilde{A}(x)$.

解 $\tilde{A}(x) = 1 + 2x + 3x^2 + 4x^3 + \cdots = (\frac{1}{1-x})' = \frac{1}{(1-x)^2}$.

解答题: 请至多选择 4 道作答. 题目按照涉及知识在课程中的出现次序排序.

11. (5 分) 考虑含有二元谓词符号 $\in$ 的一阶逻辑. 考虑 ZF 公理的一个子集 $A = \{\mathrm{AE}, \mathrm{AR}, \mathrm{AP}\} \cup \mathrm{AS}$

- 用 AE 表示外延公理 (Axiom of extensionality)
  $\forall x \forall y((\forall z(z \in x \leftrightarrow z \in y)) \to (x = y))$
- 用 AR 表示正则公理 (Axiom of regularity)
  $\forall x((\exists a(a \in x)) \to (\exists y((y \in x) \wedge \forall z \neg(z \in x \wedge z \in y))))$
- 用 AS 表示分离公理模式 (Axiom schema of specification)
  $\forall x \forall w_1 \ldots \forall w_n \exists y \forall z(z \in y \leftrightarrow (z \in x \wedge \varphi(x, w_1, \ldots, w_n, z)))$ 对于任何自由变量是 $x, w_1, \ldots, w_n, z$ 的公式 φ
- 用 AP 表示配对公理 (Axiom of pairing)
  $\forall x \forall y \exists z(x \in z \wedge y \in z)$

我们希望证明 $A \vdash \forall x \neg(x \in x)$, 证明思路为

$$\dfrac{\dfrac{\dfrac{[x \in x]}{\text{第一问}}}{\exists y \forall z(z \in y \leftrightarrow z = x)}}{\dfrac{\dfrac{\dfrac{\text{第二问}}{\bot}}{\neg(x \in x)}\to\text{I}}{\forall x \neg(x \in x)}\forall\text{I}}$$

(1) 请使用自然演绎法, 证明 $A,\ x \in x \vdash \exists y \forall z(z \in y \leftrightarrow z = x)$

(2) 请使用自然演绎法, 证明 $A,\ x \in x,\ \exists y \forall z(z \in y \leftrightarrow z = x) \vdash \bot$

建议使用树式证明: 使用公理时标明来源; 标明 $\to I$, RAA 对应的假设. 如果使用线形证明: 使用公理时标明来源; 标明每次推导使用的规则; 标明每个中间命题所依赖的假设.

解 第一问:

$$\dfrac{\dfrac{\dfrac{

12. (5 分) (1) 证明一阶逻辑的紧致性定理 (Compactness Theorem): Γ 是一阶逻辑公式的集合.

$$\Gamma \text{ 可满足} \iff \Gamma \text{ 的每个有限子集都可满足}$$

(2) 设 $G = (V, E)$ 是一个无向图, 其中 V 不一定有限.

对于任意有限子集 $V_0 \subseteq V$, 其诱导子图 $G[V_0]$ 可以三染色. (三染色, 指用三种颜色对点染色, 使得任意两个相邻点的颜色不相同.)

证明: G 可以三染色.

解

(1) Γ 可满足 $\iff \Gamma \nvdash \bot \iff$ 对每个有限 $\Gamma' \subseteq \Gamma, \Gamma' \nvdash \bot \iff \Gamma$ 的每个有限子集都可满足

前后的等价来自于一致完备性, 中间的等价来自于自然演绎证明大小有限.

(2) 不妨令颜色集合为 $[3] = \{1, 2, 3\}$, 考虑含有命题符号 $\{P_{v,i} | v \in V, i \in \{1, 2, 3\}\}$ 的命题逻辑. 这里我们希望命题 $P_{v,i}$ 表示点 v 被染成 i 色.

图可以三染色, 可以翻译为以下命题集合可满足

$$\Gamma = \left\{ P_{v,1} \vee P_{v,2} \vee P_{v,3} \;\middle|\; v \in V \right\} \cup \left\{ \neg(P_{v,i} \wedge P_{v,j}) \;\middle|\; v \in V, \{i, j\} \in \binom{[3]}{2} \right\} \cup \left\{ \neg(P_{v,i} \wedge P_{u,i}) \;\middle|\; (u, v) \in E, i \in [3] \right\}$$

考虑 Γ 的任意有限子集 Γ', 用 V_0 表示 Γ' 中出现的所有点. 那么

$$\Gamma' \subseteq \left\{ P_{v,1} \vee P_{v,2} \vee P_{v,3} \;\middle|\; v \in V_0 \right\} \cup \left\{ \neg(P_{v,i} \wedge P_{v,j}) \;\middle|\; v \in V_0, \{i, j\} \in \binom{[3]}{2} \right\} \cup \left\{ \neg(P_{v,i} \wedge P_{u,i}) \;\middle|\; (u, v) \in G[V_0], i \in [3] \right\}$$

右侧可以被满足, 因为 $G[V_0]$ 可以三染色. 其子集 Γ' 也可以被满足.

根据紧致性, Γ 可以被满足, 于是 G 可以三染色.

13. (5 分) 本题证明唯一分解整环 (Unique Factorization Domain) 的一个重要性质: 唯一分解整环的多项式环也是也是一个唯一分解整环.

在本题中, R 都表示一个唯一分解整环.

(1) 称非零多项式 $f(x) \in R[x]$ 是本原的 (primitive), 如果 $f(x)$ 的所有系数的 gcd 是单位 (unit). 不难看出, 对于任何非零多项式 $f(x) \in R[x]$, 都存在 $\alpha \in R$ 和本原多项式 $p(x)$ 满足 $f(x) = \alpha \cdot p(x)$.

证明: 对于任意本原多项式 $f(x), g(x) \in R[x]$, $h(x) = f(x)g(x)$ 也是本原多项式.

(2) 证明: 对方任意非常数 (次数 >0) 的本原多项式 $f(x) \in R[x]$, $f(x)$ 是 $R[x]$ 中的不可约多项式当且仅当 $f(x)$ 是 $F[x]$ 中的不可约多项式, 其中 $F = \mathrm{Frac}(R)$.

(3) 证明: $R[x]$ 是唯一分解整环.

解

(1) 假设 $h(x)$ 不是本原多项式, 那么一定有素数 $\alpha \in R$ 可以整除 $h(x)$ 的所有系数. 因为 $f(x), g(x)$ 都是本原多项式, 它们都一定有某些系数无法被 α 整除. 分别用 c_i, d_i 表示 $f(x), g(x)$ 的 i 次项系数. 令 m 是满足 $\alpha \nmid c_m$ 中最小的. 令 n 是满足 $\alpha \nmid d_n$ 中最小的. 那么 $f(x)g(x)$ 的 $m+n$ 次项系数

$$\underbrace{c_0 d_{m+n} + c_1 d_{m+n-1} + \ldots c_{m-1} d_{n+1}}_{\alpha\text{的倍数}} + c_m d_n + \underbrace{c_{m+1} d_{n-1} + \cdots + c_{m+n} d_0}_{\alpha\text{的倍数}}$$

也不能被 α 整除. 这与对 α 的假设矛盾.

(2) 显然 $f(x)$ 是 $F[x]$ 上的不可约多项式 $\implies$ $f(x)$ 是 $R[x]$ 中的不可约多项式.

对于非平凡方向, 假设 $f(x)$ 在 $F[x]$ 中可约, 分解为 $f(x) = q_1(x)q_2(x)\ldots q_t(x)$, 其中 $q_1, \ldots, q_t$ 是 $F[x]$ 中不可约多项式. 利用通分, $q_i(x) = \alpha_i p_i(x)$, 其中 $\alpha_i \in F$ 且 p_i 是 $R[x]$ 中不可约多项式. 令 $\alpha = \alpha_1 \ldots \alpha_t = \beta/\gamma$, 其中 $\beta, \gamma \in R$ 且互素.

$$f(x) = q_1(x)q_2(x)\ldots q_t(x) = \alpha p_1(x)p_2(x)\ldots p_t(x) = \frac{\beta}{\gamma} p_1(x)p_2(x)\ldots p_t(x)$$

γ 整除 $\beta p_1(x)p_2(x)\ldots p_t(x)$, 也就是整除 $\beta p_1(x)p_2(x)\ldots p_t(x)$ 的每一项的系数. 因为 β, γ 互素, 所以 γ 整除 $p_1(x)p_2(x)\ldots p_t(x)$ 的每一项的系数. 所以 γ 整除 $p_1(x)p_2(x)\ldots p_t(x)$. 根据前一问, $p_1(x)p_2(x)\ldots p_t(x)$ 是本原多项式, 所以 γ 是单位.

因此 $f(x) = \beta\gamma^{-1} p_1(x)p_2(x)\ldots p_t(x)$ 在 $R[x]$ 中可约.

(3) 非常数非本原的多项式显然在 $R[x]$ 中可约. 因此 $R[x]$ 中的不可约多项式, 要么是常数, 要么是本原多项式.

对于任意非零多项式 $f(x) \in R[x]$. 假设其存在不同的分解

$$f(x) = \alpha_1 \ldots \alpha_s p_1(x)\ldots p_t(x) = \beta_1 \ldots \beta_u q_1(x)\ldots q_v(x),$$

其中 α_i, β_i 是素元, p_i, q_i 是不可约的非常数本原多项式.

常数部分 $\alpha_1 \ldots \alpha_s$ 和 $\beta_1 \ldots \beta_u$ 都是 f 系数的 gcd 的分解. 因为 R 是 UFD, 这两种分解等价.

本原多项式部分 根据上一问结论, p_i, q_i 都是 $F[x]$ 中不可约多项式. 于是也可以看作 $f(x)$ 在 $F[x]$ 中的分解

$$f(x) = \underbrace{\alpha}_{\alpha_1 \ldots \alpha_s} p_1(x)\ldots p_t(x) = \underbrace{\beta}_{\beta_1 \ldots \beta_u} q_1(x)\ldots q_v(x),$$

F 是域 $\implies$ $F[x]$ 是欧氏整环 $\implies$ $F[x]$ 是 UFD. 所以这两种分解也在 $F[x]$ 中等价.

注意到, p_i, q_j 在 $F[x]$ 中相伴 $\implies$ 存在非零 $\gamma \in F$ $p_i = \alpha q_j$ $\implies$ 存在互素 $\gamma_1, \gamma_2 \in R$ $\gamma_1 p_i = \gamma_2 q_j$ $\implies$ p_i, q_j 在 $R[x]$ 中相伴. 所以这两种分解在 $R[x]$ 中也等价.

14. (5 分) n 是正整数. 令 $N = 2^n - 1$. 考虑 $\mathbb{Z}_N^\times$ 的一个子群 $G = \{1, 2, 2^2, \ldots, 2^{n-1}\}$. 定义群作用

$$G \times \mathbb{Z}_N \to \mathbb{Z}_N$$
$$g \cdot a = ga$$

(1) 假设 n 是素数, G 作用下 $\mathbb{Z}_N$ 有多少个轨道?

(2) G 作用下 $\mathbb{Z}_N$ 有多少个轨道?

解 a 是乘 2^t 的不动点, 等价于 $(2^t - 1)a = 0 \pmod N$, 等价于 a 是 $N/\gcd(2^t - 1, N)$ 的倍数. 所以乘 2^t 的不动点数目为 $\gcd(2^t - 1, N) = \gcd(2^t - 1, 2^n - 1) = 2^{\gcd(t,n)} - 1$.

(1) 如果 n 是素数, 对于任意 $t \neq 0$, 乘 2^t 只有一个不动点 0. 换言之, 除了 0, 所以轨道都恰好有 n 个元素. 总轨道数为 $1 + \frac{2^n-2}{n}$.

(2) 使用 Burnside 引理. 轨道数为

$$\frac{1}{n} \sum_{t \in \mathbb{Z}_n} \left(2^{\gcd(t,n)} - 1\right) = \frac{1}{n} \sum_{d|n} \varphi(n/d) \cdot 2^d - 1.$$

另一种解法: 注意到, 乘 2 等价于循环左移. 对于最高位, 因为我们选取 $2^n - 1$ 作为模数, 最高位会被移到最低位. 因此我们可以考虑如下等价问题: 循环左移可以看作 $\mathbb{Z}_n$ 对 $\{0,1\}^n$ 的群作用, 我们关心这个群作用有多少轨道. 轨道数比原问题多 1, 因为原问题排除了 1^n 的单点轨道.

(1) 当长度 n 为素数时, 除了 $0^n, 1^n$ 之外, 任何轨道都有 n 个元素. 所以轨道数为 $2 + \frac{2^n-2}{n}$.

(2) 使用 Burnside 引理. 对 $g \in \mathbb{Z}_n$, g 作用的不动点数目为 $2^{\gcd(g,n)}$. 所以轨道数为

$$\frac{1}{n} \sum_{g \in \mathbb{Z}_n} 2^{\gcd(g,n)} = \frac{1}{n} \sum_{d|n} \varphi(n/d) \cdot 2^d$$

15. (5 分) $0 = a_0 < a_1 < a_2 < \ldots$ 是一个递增自然数序列, 使得对任意 $n \in \mathbb{N}$, 都存在唯一的解 (i, j, k) 满足 $n = a_i + 2a_j + 4a_k$.

证明这样的序列存在, 并求出 a_{1024}.

解 假设这样的序列存在, 定义生成函数 $G(x) = \sum_{i=0}^{\infty} x^{a_i}$. 那么

$$G(x)G(x^2)G(x^4) = \sum_{i,j,k} x^{a_i + 2a_j + 4a_k} = \sum_{i=0}^{\infty} x^i = \frac{1}{1-x}$$
$$G(x^2)G(x^4)G(x^8) = \frac{1}{1-x^2}.$$

因而 $G(x^8)(1 + x) = G(x)$. 也就是说, $\langle 8a_0, 8a_0 + 1, 8a_1, 8a_1 + 1, \ldots \rangle$ 与 $\langle a_0, a_1, \ldots \rangle$ 是同一个序列. 这样得到递推公式

$$a_{2i} = 8a_i, \qquad a_{2i+1} = 8a_i + 1.$$

所以 $a_{1024} = 8^{10}a_1 = 8^{10}(8a_0 + 1) = 8^{10}$.

最后验证这样的序列的存在性. 前述得到的序列 $0,1,8,9,8^2,8^2+1,8^2+8,8^2+8+1,\ldots$ 由所有 8 进制表示只含有 $0,1$ 的自然数构成. 不难说明, 此序列满足了 $n=a_i+2a_j+4a_k$ 存在唯一解的条件.

16. (5 分) 立方体的顶点可以用 $V=\{-1,1\}^3\subseteq\mathbb{R}^3$ 表示.

(1) 按照某种特定方式对它整体旋转和镜面（即正交变换）的时候, 它会与原来的占位重合, 尽管顶点可能换了位置. 这类变换对应什么样的矩阵?

(2) 占位不变的变换构成一个群 R. 这个群有几个共轭类? 指出每个共轭类的大小, 并举出一个代表元.

(3) 用 C 种颜色对面染色, 有多少种不同的染色方式.

解

(1) 用 $\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3$ 表示 $\mathbb{R}^3$ 上的标准基.

立方体的面的中心是 $\pm\mathbf{e}_1,\pm\mathbf{e}_2,\pm\mathbf{e}_3$. 因此, 其对应矩阵的每个列向量只能是 $\pm\mathbf{e}_1,\pm\mathbf{e}_2,\pm\mathbf{e}_3$ 之一. 又因为是正交变换, 每列对应的标准基向量不同.

$$R=\left\{\left[\begin{array}{ccc}| & | & |\\ a_1\mathbf{e}_{\pi(1)} & a_2\mathbf{e}_{\pi(2)} & a_3\mathbf{e}_{\pi(3)}\\ | & | & |\end{array}\right]\middle|\begin{array}{c}\pi\in\mathrm{Sym}(3),\\ a_1,a_2,a_3\in\{\pm1\}\end{array}\right\}$$

注. 所有 $\pi=e$ 的变换构成 R 的一个正规子群 N, 同构于 $\mathbb{Z}_2^3$. 所有 $a_1=a_2=a_3=1$ 的变换构成 R 的一个子群 H, 同构于 $\mathrm{Sym}(3)$. R 是半直积 $R=N\rtimes H$.

(2) 共轭不变量是: π 的轮换类型 (cycle type), π 的每个轮换中系数 a_i 的乘积.

π 的类型	轮换系数乘积, 用正负号表示	共轭类大小	面染色不动点个数	代表元
$1,1,1$	$1+,1+,1+$	1	C^6	$\begin{bmatrix}1&&\\&1&\\&&1\end{bmatrix}$
	$1+,1+,1-$	$\binom{3}{1}$	C^5	$\begin{bmatrix}1&&\\&1&\\&&-1\end{bmatrix}$
	$1+,1-,1-$	$\binom{3}{2}$	C^4	$\begin{bmatrix}1&&\\&-1&\\&&-1\end{bmatrix}$
	$1-,1-,1-$	1	C^3	$\begin{bmatrix}-1&&\\&-1&\\&&-1\end{bmatrix}$
$2,1$	$2+,1+$	$3\cdot2$	C^4	$\begin{bmatrix}1&&\\&1&\\&&1\end{bmatrix}$
	$2+,1-$	$3\cdot2$	C^3	$\begin{bmatrix}1&&\\&1&\\&&-1\end{bmatrix}$
	$2-,1+$	$3\cdot2$	C^3	$\begin{bmatrix}1-&&\\&1&\\&&1\end{bmatrix}$
	$2-,1-$	$3\cdot2$	C^2	$\begin{bmatrix}1-&&\\&1&\\&&-1\end{bmatrix}$
3	$3+$	$2\cdot2^2$	C^2	$\begin{bmatrix}1&&\\&1&\\&&1\end{bmatrix}$
	$3-$	$2\cdot2^2$	C	$\begin{bmatrix}1&&\\&1&\\&&-1\end{bmatrix}$

(3) 对于每个轮换, 如果轮换系数乘积为 $+1$, 那么对应维度的面有 C^2 种染色方式; 如果轮换系数乘积为 -1, 那么对应维度的面有 C 种染色方式.

面染色方案数为 $\frac{1}{48}(C^6+3C^5+9C^4+13C^3+14C^2+8C)$.

附录: 自然演绎系统推导规则 考虑只包含连接词 $\to$ 和 $\wedge$ 的命题逻辑. 包括永假常元 $\bot$, $\neg\phi$ 是 $\phi \to \bot$ 的缩写. 没有公理. 推导规则如下:

$$\frac{\phi \quad \psi}{\phi \wedge \psi} \wedge I \qquad \frac{\phi \wedge \psi}{\phi} \wedge E_1 \qquad \frac{\phi \wedge \psi}{\psi} \wedge E_2 \qquad \frac{\bot}{\phi} \bot$$

$$\begin{array}{cc} [\phi] & [\neg\phi] \\ \mathcal{D} & \mathcal{D} \\ \dfrac{\psi}{\phi \to \psi} \to I & \dfrac{\phi \quad \phi \to \psi}{\psi} \to E \qquad \dfrac{\bot}{\phi}\text{RAA} \end{array}$$

其中, 横线上面是前提, 下面是推导的结果 (结论), 横线右边是规则的名字 (例如 $\wedge I$). $\mathcal{D}$ 表示省略的推导步骤; 方括号表示假设该公式已经推出, 在此基础上进行推理.

扩展为一阶逻辑后, 引入变量符号、常量符号. 引入量词符号 $\forall$ 及推导规则

$$\begin{array}{cc} \mathcal{D} & \\ \dfrac{\phi(x)}{\forall x \phi(x)} \forall I & \dfrac{\forall x \phi(x)}{\phi(t)} \forall E \end{array}$$

$\exists x$ 是 $\neg\forall x\neg$ 的简写. $\varphi \leftrightarrow \psi$ 是 $(\varphi \to \psi) \wedge (\psi \to \varphi)$ 的简写. 引入关系符号 $=$ 及对应推导规则或公理.