期中考试

试卷共 5 页，共 16 题，满分 30 分.

判断题，填空题: 无需写出证明.

1. (1 分) 对任意集合 A, B，如果 $|2^A| > |2^B|$，那么 $|A| > |B|$.

   解 是

   考虑逆否命题即可.

2. (1 分) 集合 S 上定义了一个 (全) 序关系 $\leq$. 如果对任意 $x \in S$, 都存在一个后继 $s_x \in S$ 满足 $x \leq s_x$ 且 x, s_x 之间没有其它元素, 那么 $\leq$ 是 S 上的一个良序.

   解 否

   $\mathbb{Z}$ 为一个反例.

3. (1 分) 以下哪个命题可以在去掉 RAA 的自然演绎系统中推出.

   A. $(P \to Q) \to (\neg Q \to \neg P)$ B. $(\neg Q \to \neg P) \to (P \to Q)$

   解 A

   作业题.

4. (1 分) 对公式 φ, ψ, 如果 $\vdash (\neg\varphi) \leftrightarrow \psi$, 那么称 ψ 是 φ 的一个否定. 在一阶自然演绎系统中, x, y, z 是变元，A 是谓词符. 判断 $\forall x \exists y \forall z \exists x A(x, y, z)$ 是否是 $\forall y \exists z \forall x \neg A(x, y, z)$ 的一个否定.

   解 是

   $\forall y \exists z \forall x \neg A(x, y, z)$ 的否定是 $\varphi = \exists y \forall z \exists x A(x, y, z)$. 注意道 φ 中 x 不是自由变量, 因此 φ 和 $\forall x \varphi$ 等价.

5. (1 分) a, b, c 是正整数. 如果 $a|bc$, $b|ac$, $c|ab$, 那么 $\gcd(a, b, c) = \gcd(\frac{ab}{c}, \frac{ac}{b}, \frac{bc}{a})$.

   解 否

   反例为 $2, 2^2, 2^3$.

6. (1 分) Sym(4) 有 6 阶子群.

解 是

考虑所有将 1 映射到 1 的映射. 它们构成 Sym(4) 的一个子群, 同构于 Sym(3).

7. (1 分) 循环群的商群一定是循环群.

解 是

考虑循环群 $\langle g\rangle$ 和它的一个商群 $\langle g\rangle/N$. $\bar{g}$ 是商群的一个生成元.

8. (1 分) 在一个幺环中, 如果元素 x 有两个不同的左逆 u_1, u_2, 那么 x 没有右逆.

解 是

假设有右逆 v, 那么 $u_1 = u_1xv = v = u_2xv = u_2$.

9. (1 分) 设 $\mathbb{F} = \mathbb{F}_q$ 是一个有限域, $\mathbb{E}$ 是 $\mathbb{F}[x]$ 的分式域. 那么 $\mathbb{E}$ 包含至少一个 q^2 阶的子域.

解 否

反证, 假设这样的子域 K 存在. 任选一个 $K\setminus\mathbb{F}$ 中的元素, 可以表示成 $\alpha = \frac{f(x)}{g(x)}$, 其中 $\gcd(f,g) = 1$.
因为 $\alpha \in K\setminus\{0\}$, $\alpha^{q^2-1} = 1$.

因为 $\alpha \notin \mathbb{F}$, 所以 $f \neq 0$ 且 f, g 中至少有一个非常数 (度数 ≥ 1). 所以 $\alpha^{q^2-1} = \frac{f^{q^2-1}(x)}{g^{q^2-1}(x)} \neq 1$.

10. (1 分) $\mathbb{F}_2[x]$ 中有几个 5 次不可约多项式.

解 6

$x^{2^5} - x$ 是所有次数为 1,5 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 $\frac{x^{2^5}-x}{x^2-x}$ 是所有 5 次不可约多项式的乘积. 说明 5 次不可约多项式的个数为 $\frac{2^5-2}{5}$.

解答题: 请选择 4 道作答.

11. (5 分) 设 $k \geq 1$ 是整数, 找到最小的 d, 使得对任意 n, 都存在一个 $\mathbb{F}_2$ 上的次数不超过 d 的多项式 $f(x_1, \ldots, x_n)$

$$\forall x_1, \ldots, x_n \in \{0,1\},\ f(x_1, \ldots, x_n) = \begin{cases} 1, & \text{if } x_1, \ldots, x_n \text{ 中 1 的个数} \equiv -1 \pmod{2^k} \\ 0, & \text{otherwise} \end{cases}$$

提示: 先考虑 $n = 2^k - 1$ 的情况.

解 $d = 2^k - 1$.

因为输入只有 0 或 1, 对任意 $k > 1$ 都有 $x_i^k = x_i$. 所以不妨令 f 对于每位输入的次数都不超过 1.

先考虑 $n = 2^k - 1$ 的情况. 这时唯一满足要求的多项式是 $f = x_1x_2\ldots x_n$.

对一般的情况, 可以知道 f 中没有次数小于 2^k-1 的项, 同时含有所有次数为 2^k-1 的项. 尝试

$$f(x_1,\dots,x_n)=\sum_{\text{size-}(2^k-1)\ S\subseteq[n]}\prod_{i\in S}x_i.$$

当输入中有 m 个 1 时,

$$f(x_1,\dots,x_n)=\binom{m}{2^k-1}\bmod 2=\frac{(m-2^k+2)\cdots(m-1)m}{1\cdot 2\cdot\cdots\cdot(2^k-1)}\bmod 2.$$

我们关心分子分母中 2 的次数.

- 如果 $m=2^kq+2^k-1$, 那么可以将分子分母中的项一一对应, i 与 2^kq+i 对应. 对应的两项中 2 的次数相同, 因此上下次数相同.
- 如果 $m=2^kq+r$ 且 $r\in\{0,\dots,2^k-2\}$, 那么仍然可以分子分母中的项按照 $\bmod 2^k$ 的值一一对应. 只有分子中的 2^kq 和分母中的 $r+1$ 没有对应. 这里 2^kq 中 2 的次数比 $r+1$ 中 2 的次数多.

12. (5 分) 考虑命题逻辑的自然演绎系统, 证明 $r\to p\vdash((p\to q)\to r)\to p$.

解 作业中已经证明 $\vdash((p\to q)\to p)\to p$. 因为增加了 $r\to p$ 的条件, 只需将原证明稍作修改即可推导出 $((p\to q)\to r)\to p$.

$$\dfrac{\dfrac{\dfrac{\dfrac{[p\to\bot]_2\qquad[p]_3}{\bot}(\to E)}{q}(\bot)}{p\to q}(\to I_3)\qquad[(p\to q)\to r]_1}{r}(\to E)\qquad p\to r}{\dfrac{\dfrac{p}{\bot}(\to E,\text{结合}[p\to\bot]_2)}{p}(\mathrm{RAA}_2)}{((p\to q)\to p)\to p}\to I_1$$

13. (5 分) 群 G 是有限生成群 (finitely generated group) 当且仅当存在有限集合 $F\subseteq G$ 使得 $G=\langle F\rangle$. 设 G 是有限生成群, $\{g_1,\dots,g_n\}$ 是 G 的一个生成集. 用 $\mathsf{free}(S)$ 表示由一个给定符号集合 $S=\{s_1,\dots,s_n\}$ 生成的自由群. 证明, 存在 $\mathsf{free}(S)$ 的一个正规子群 H, 满足 $G\cong\mathsf{free}(S)/H$.

解 定义同态 $\varphi:\mathsf{free}(S)\to G$. 对任意符号串 a, 将其中每个 s_i 符号替换为 g_i, 将每个 s_i^{-1} 符号替换为 g_i^{-1}, 替换得到的结果即为 $\varphi(a)$.

首先验证 φ 是映射. 对任意两个等价符号串 $a\sim b$, 一定存在一列有限长的等价符号串

$$a_0=a,\quad a_1,\quad a_2,\quad\dots,\quad a_{t-1},\quad a_t=b.$$

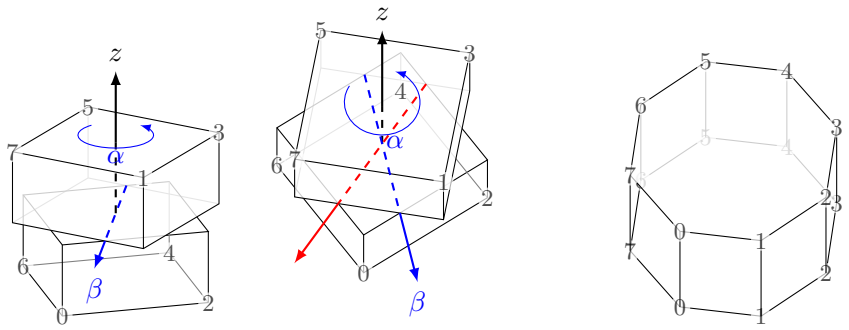
其中任意相邻的两个符号串 a_i,a_{i+1} 都只在某处差一对符号 ss^{-1} 或 $s^{-1}s$. 因此 $\varphi(a_i)=\varphi(a_{i+1})$. 进而 $\varphi(a)=\varphi(b)$. 这说明 φ 在等价类上是良好定义的.

根据 φ 的定义, $\varphi(ab)=\varphi(a)\varphi(b)$. 所以 φ 是同态.

因为 $G=\langle g_1,\dots,g_n\rangle$ 所以 G 用每个元素都等于 $g_1,g_1^{-1},\dots,g_n,g_n^{-1}$ 中有限个元素 (可重复选取) 的乘积. 这对应 $\mathsf{free}(S)$ 中存在原像. 所以 φ 是满同态.

因而 $G=\operatorname{Im}\varphi\cong \mathsf{free}(S)/\operatorname{Ker}\varphi$, 其中 $\operatorname{Ker}\varphi\trianglelefteq\mathsf{free}(S)$.

14. (5 分) 给定一个正方体，垂直于 z 轴将其平分为两半，并将其下半部分绕 z 轴旋转 45 度.



按照某种特定方式对它整体旋转（即特殊正交变换，可以保角度的旋转，但没有镜面操作）的时候，它会与原来的占位重合，尽管点和面可能换了位置. 占位不变的旋转构成一个群 R. 记 α 为逆时针绕着 z 轴转 90 度. 记 β 为绕着图中标出的轴转 180 度. 可以证明，α,β 生成了 R.

(1) 证明：R 同构于 D_8 的一个子群.

提示：对正方体的顶点编号 $0,1,2,3,4,5,6,7$.

(2) 写出 R 的类方程 (class equation), 并解释它的几何意义 (即每个共轭类对应的旋转类型).

解 使用题目中的两个基础旋转 $\alpha=(1357)(0246),\beta=(01)(27)(36)(45)$.

(1) 直接注意到对给定形状占位不变的旋转, 也是 D_8 占位不变的旋转.

也可以注意这个群有 8 个元素 $\{\beta^b\alpha^i\}_{b\in\{0,1\},i\in\{0,1,2,3\}}$, 并且满足 $e=\alpha^4=\beta^2$, $\alpha\beta\alpha=\beta$. 这正是 D_4. 同构于 D_8 的某个子群.

(2) 共有五个共轭等价类, 特别注意到后两个共轭类的手性不同.

共轭类大小	1	1	2	2	2
包含元素	e	α^2	α,α^3	$\beta,\beta\alpha^2$	$\beta\alpha,\beta\alpha^3$
几何含义	不动	z 轴对称	转 90 度	绕蓝色轴的轴对称	绕红色轴的轴对称
中心化子			$\langle\alpha\rangle$	$\langle\alpha^2,\beta\rangle$	$\langle\alpha^2,\beta\alpha\rangle$

15. (5 分) 设素数 $p>2$ 且，我们知道二面体群 D_p 是一个 $2p$ 的非循环群. 证明，在同构意义下，阶为 $2p$ 的非循环群只有 D_p.

解 令 G 是一个大小为 $2p$ 的非循环群. 根据 Sylow 定理, G 存在一个 p 阶子群, 记为 $N = \langle g \rangle$. 因为 $[G : N] = 2$, 所以 $N \trianglelefteq G$.

任取 G/N 中的一个元素 h, 因为 $\bar{h}$ 的阶为 2, 所以 h 的阶一定是 2 的倍数, 只能是 2 或 $2p$. 如果 $\text{order}(h) = 2p$, 那么 $G = \langle h \rangle$ 是循环群, 与假设矛盾. 只能是 $\text{order}(h) = 2$.

G 中任意元素都可以唯一的写成 $h^i g^j$ 的形式, 其中 $i \in \mathbb{Z}_2, j \in \mathbb{Z}_p$.

因为 $hN = Nh$, 一定存在 $k \in \mathbb{Z}_p$ 使得 $hg = g^k h$.

$$e = h^2 = (g^k h g^{-1})^2 = g^k h g^{k-1} h g^{-1} = g^k g^{(k-1)k} h^2 g^{-1} = g^{k^2-1}.$$

因此 $k^2 - 1 = 0 \ (\text{in } \mathbb{Z}_p)$,

- 如果 $k = 1$, 那么 G 是交换群. 大小为 $2p$ 的交换群一定是循环群.
- 如果 $k = -1$, 那么 $hg = g^{-1}h$, 与 D_p 同构.

16. (5 分) 考虑 $\mathbb{F}_{103}[x]$ 中的多项式 $f(x) = x^3 - 2$, $\mathbb{F}_{103}[x]/(f(x))$ 是否是域? 请计算说明.

解 是

只需验证 f 是不可约 3 次多项式. 因为 $\deg f = 3$, 如果 f 可约, 那么一定存在 1 次因式. 我们知道 $x^{103} - x$ 是所有 1 次不可约多项式的乘积. 因此只需验证 $\gcd(f, x^{103} - x) = \gcd(f, x^{102} - 1) = 1$.

$$\gcd(f, x^{102} - 1) = \gcd(f, (x^{102} - 1) \bmod (x^3 - 2)) = \gcd(f, 2^{34} - 1) = \begin{cases} f, & \text{if } 2^{34} - 1 = 0 \\ 1, & \text{otherwise} \end{cases}$$

最终 $2^{34} - 1 = 45 \pmod{103}$.

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:

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

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

附录: 自由群 给定一个符号集合 S. 对每个 $s \in S$, 定义新符号 s^{-1}. 考虑符号串组成的集合 S^*. 对任意两个符号串 a, b, 对任意符号 s, 令 $ass^{-1}b \sim ab \sim as^{-1}sb$ (这里 ab 表示 a, b 的拼接). 考虑满足前述要求的最小等价关系 $\sim$.

自由群 $\mathsf{free}(S) = S^*/\sim$, 群运算为 $\bar{a} \cdot \bar{b} = \overline{ab}$.