期中考试

试卷共 2 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 $|A| > |B|$.
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.
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. $(\neg Q \to \neg P) \to (P \to Q)$
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.
5. (1 分) a, b, c 是正整数. 如果 $a|bc$, $b|ac$, $c|ab$, 那么 $\gcd(a, b, c) = \gcd(\frac{ab}{c}, \frac{ac}{b}, \frac{bc}{a})$.
6. (1 分) $\mathrm{Sym}(4)$ 有 6 阶子群.
7. (1 分) 循环群的商群一定是循环群.
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.
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.
10. (1 分) $\mathbb{F}_2[x]$ 中有几个 5 次不可约多项式.

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 $f(x_1, \ldots, x_n)$

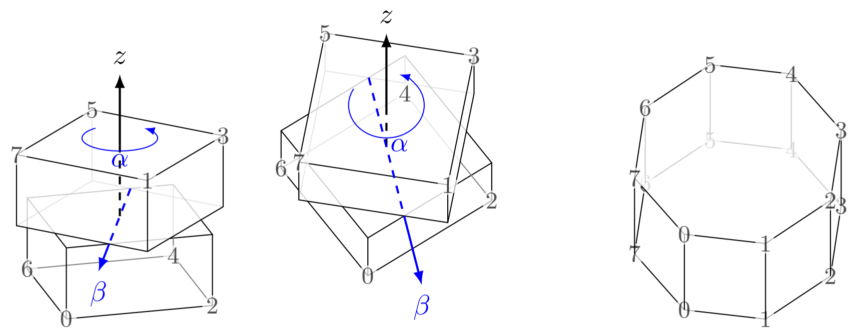
$$\forall x_1, \ldots, x_n \in \{0, 1\},\ f(x_1, \ldots, x_n) = \begin{cases} 1, & \text{if } x_1, \ldots, x_n \text{ 中 } 1 \text{ 的个数} \equiv -1 \pmod{2^k} \\ 0, & \text{otherwise} \end{cases}$$

   提示：先考虑 $n = 2^k - 1$ 的情况.

12. (5 分) 考虑命题逻辑的自然演绎系统，证明 $r \to p \vdash ((p \to q) \to r) \to p$.
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，$\{g_1, \ldots, g_n\}$ 是 G 的一个生成集. 用 $\mathsf{free}(S)$ 表示由一个给定符号集合 $S = \{s_1, \ldots, s_n\}$ 生成的自由群. 证明，存在 $\mathsf{free}(S)$ 的一个正规子群 H，满足 $G \cong \mathsf{free}(S)/H$.

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).

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.

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.

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 $\perp$, $\neg\phi$ 是 $\phi \to \perp$ 的缩写. 没有公理. 推导规则如下：

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

$$\frac{\begin{matrix}[\phi] \\ \mathcal{D} \\ \psi\end{matrix}}{\phi \to \psi} \to I \qquad \frac{\phi \quad \phi \to \psi}{\psi} \to E \qquad \frac{\perp}{\phi} \perp \qquad \frac{\begin{matrix}[\neg\phi] \\ \mathcal{D} \\ \perp\end{matrix}}{\phi} \mathrm{RAA}$$

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 $\bar{a} \cdot \bar{b} = \overline{ab}$.