期中考试

试卷共 6 页, 共 16 题, 满分 30 分.

判断题, 填空题: 无需写出证明.

1. (1 分) 在命题逻辑中, 对于任意命题, $\vdash \varphi$ 和 $\vdash \neg\varphi$ 有且只有一个成立.

   解 否

2. (1 分) 可以在去掉 RAA 的自然演绎系统中推出 $(((P \to Q) \to P) \to P)$.

   解 否

   作业题.

3. (1 分) 令 $S_0 = \varnothing$, $S_{i+1} = 2^{S_i}$. 那么 $S_0 \cup S_1 \cup \dots$ 是否是一个 ZFC 中的集合.

   解 是

   从 S_i 到 S_{i+1} 使用幂集公理, 再到 $\bigcup_i S_i$ 使用 $\mathbb{N}$ 和替代公理模式.

4. (1 分) a, b, c 是正整数, 那么 $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$.

   解 是

5. (1 分) $\mathrm{Sym}(4)$ 有 9 阶子群.

   解 否

   $|\mathrm{Sym}(4)| = 4!$ 不是 9 的倍数.

6. (1 分) $\mathbb{Z}[x]$ 是一个主理想整环 (PID).

   解 否

   $(x, 2)$ 不是主理想.

7. (1 分) 有限阶循环群的子群一定是循环群.

   解 是

8. (1 分) 如果 R 是一个整环 (含幺交换无零因子), 那么 $R[x]$ 是一个整环.

解 是

含幺和交换显然. 只需注意到对两个非零多项式 $f, g \in R[x]$, fg 的最高项系数等于 f, g 最高项系数的乘积.

9. (1 分) 最小的非交换群是几阶群.

解 $6 = |\mathrm{Sym}(3)|$.

素数阶群一定交换, 所以只需验证 4 阶群是否都交换. 如果其中有 4 阶元一定交换. 如果只含有 2 阶元和 1 阶元, 根据作业也一定交换.

10. (1 分) $\mathbb{F}_2[x]$ 中有几个 (首一的) 10 次不可约多项式.

解 99

$x^{2^{10}} - x$ 是所有次数为 1,2,5,10 的不可约多项式的乘积. $x^{2^5} - x$ 是所有次数为 1,5 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 $(x^{2^{10}} - x)(x^2 - x)/(x^{2^5} - x)(x^{2^2} - x)$ 是所有 10 次不可约多项式的乘积. 说明 10 次不可约多项式的个数为 $(2^{10} - 2^5 - 2^2 + 2)/10$.

解答题: 请选择 4 道作答.

11. (5 分) 令 Γ 表示如下公理集合, 不难看出它们是在 Peano 公理中不涉及乘法的公理.

$$\forall x \neg(0 = S(x))$$
$$\forall xy(S(x) = S(y) \to x = y)$$
$$\forall x(x + 0 = x)$$
$$\forall xy(x + S(y) = S(x + y))$$
$$(\varphi(0) \wedge \forall x(\varphi(x) \to \varphi(S(x))) \to \forall x\varphi(x) \qquad \text{对任意 } \varphi$$

为了简化证明, 我们使用几个稍作修改的相等规则, 不再局限于变量符号. 它们都很容易从原有的相等公理使用一次 $\forall E$ 规则得出.

$$\frac{}{t = t}\ \mathrm{RI}_1^* \qquad \frac{t_1 = t_2}{t_2 = t_1}\ \mathrm{RI}_2^* \qquad \frac{t_1 = t_2 \qquad t_2 = t_3}{t_1 = t_3}\ \mathrm{RI}_3^* \qquad \frac{t_1 = t_2}{t(t_1) = t(t_2)}\ \mathrm{RI}_4^* \qquad \frac{t_1 = t_2}{\varphi(t_1) \to \varphi(t_2)}\ \mathrm{RI}_4^*$$

在作业中, 已经作为例子给出 $\Gamma \vdash \forall x(0 + x = x)$ 和 $\Gamma \vdash \forall xy(S(x) + y = S(x + y))$ 的证明. 请使用自然演绎法, 证明 $\Gamma \vdash \forall xyz((x + y) + z = x + (y + z))$. 可以直接使用例子中已经证明的命题.

解 记 $\varphi(y) := \forall xz((x + y) + z = x + (y + z))$, 也就是要证明 $\forall y\varphi(y)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\forall x(x+0=x)}{x+0=x}\forall\mathrm{E}}{(x+0)+z=x+z}\mathrm{RI}_4^*\quad \dfrac{\dfrac{\dfrac{\forall x(0+x=x)}{0+z=z}\forall\mathrm{E}}{z=0+z}\mathrm{RI}_2^*}{(x+z=x+(0+z)}\mathrm{RI}_4^*}{(x+0)+z=x+(0+z)}\mathrm{RI}_2^*}{\forall xz((x+0)+z=x+(0+z))}\forall\mathrm{I}}{\text{i.e. } \varphi(0)}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\forall xz((x+y)+z=x+(y+z))]\ \text{i.e. } \varphi(y)}{(x+y)+z=x+(y+z)}\forall\mathrm{E}}{S((x+y)+z)=S(x+(y+z))}\mathrm{RI}_4^*\quad \dfrac{\forall xy(S(x)+y=S(x+y))}{S(x+y)+z=S((x+y)+z)}\forall\mathrm{E}}{S(x+y)+z=S(x+(y+z))}\mathrm{RI}_3^*\quad \dfrac{\dfrac{\forall xy(x+S(y)=S(x+y))}{x+S(y)=S(x+y)}\forall\mathrm{E}}{(x+S(y))+z=S(x+y)+z}\mathrm{RI}_4^*}{(x+S(y))+z=S(x+(y+z))}\mathrm{RI}_3^*\quad \dfrac{\dfrac{\dfrac{\forall xy(x+S(y)=S(x+y))}{x+S(y+z)=S(x+(y+z))}\forall\mathrm{E}}{S(x+(y+z))=x+S(y+z)}\mathrm{RI}_2^*}{(x+S(y))+z=x+S(y+z)}\mathrm{RI}_3^*\quad \dfrac{\dfrac{\dfrac{\forall xy(S(x)+y=S(x+y))}{S(y)+z=S(y+z)}\forall\mathrm{E}}{S(y+z)=S(y)+z}\mathrm{RI}_2^*}{x+S(y+z)=x+(S(y)+z)}\mathrm{RI}_4^*}{(x+S(y))+z=x+(S(y)+z)}\mathrm{RI}_3^*}{\varphi(y)\to\varphi(S(y))}\to\mathrm{I}}{\forall y(\varphi(y)\to\varphi(S(y)))}\forall\mathrm{I}\quad \varphi(0)}{\varphi(0)\wedge\forall y(\varphi(y)\to\varphi(S(y))}\wedge I\quad (\varphi(0)\wedge\forall y(\varphi(y)\to\varphi(S(y)))\to\forall y\varphi(y)}{\forall y\varphi(y)}\to E$$

12. (5 分) 在 ZFC 中, 证明或证伪以下命题: 如果 $\in$ 是集合 S 上的 (全) 序关系, 也就是定义 $x<y$ 当且仅当 $x\in y$. 那么也是 S 上的良序关系.

解 是

考虑 S 的任何一个非空子集 T, 需要证明 T 中有最小元. 注意到 T 的性质和 S 相同, 所以只需证明 S 中有最小元.

反证法, 假设 S 中没有最小元, 那么就存在 S 中的无穷下降列 $x_1\ni x_2\ni x_3\ldots$. 根据作业, 我们知道这样的无穷下降列违背了正则公理.

13. (5 分) 用 PA 表示 Peano 公理, 其最自然的模型就是自然数. 在课上, 我们说明了 PA 存在非标准模型, 其步骤如下.

1. 添加常数符号 $\{c_i\}_{i\in\mathcal{I}}$. 这里 $\mathcal{I}$ 是一个不可数集合.
2. 对任意不同的 $i, j \in \mathcal{I}$, 添加公理 $c_i \neq c_j$.
3. 添加的符号和公理后仍然一致, 即 $\mathrm{PA}, \{c_i \neq c_j\}_{i\neq j\in\mathcal{I}} \nvdash \bot$.
4. 由一阶逻辑的完备性, 存在一个模型 $\mathfrak{B}$ 使得 $\mathfrak{B} \vDash \mathrm{PA}, \{c_i \neq c_j\}_{i\neq j}$. 新加入的公理 $\{c_i \neq c_j\}_{i\neq j}$ 保证了 $\mathfrak{B}$ 一定远大于自然数模型.
5. $\mathfrak{B} \vDash \mathrm{PA}$, 即 $\mathfrak{B}$ 也是 Peano 代数的一个（非标准）模型.

请论证其中的第三步, 为何新公理不会破坏一致性?

解 假设新公理破坏了一致性, 也就是 $\mathrm{PA}, \{c_i \neq c_j\}_{i\neq j\in\mathcal{I}} \vdash \bot$. 令 $I \subseteq \mathcal{I}$ 表示推导过程使用的下标集合, 也就是 $\mathrm{PA}, \{c_i \neq c_j\}_{i\neq j\in I} \vdash \bot$. 因为推导过程是有限的, 所以 I 是有限集.

如果自然数是 PA 的模型, 那么只需将 $\{c_i\}_{i\in I}$ 分别赋为不同的自然数, 便得到了 $\mathrm{PA}, \{c_i \neq c_j\}_{i\neq j\in I}$ 的一个模型.

14. (5 分) 设 R 为整环 (含幺交换无零因子), 则 R 中可逆元构成的乘法群的任意有限子群 G 是循环群.

提示: 考虑分式域.

解 考虑 R 的分式域, 记为 $F = \mathrm{Frac}(R)$. 在 R 到 F 的自然环同态下, G 同构于 $F^* = F \setminus \{0\}$ 的一个子群. 不引起误会的前提下, 可以把 G 视为 F^* 的一个子群.

记 $n = |G|$, G 中所有 d 阶元均是 $x^d - 1$ 的根. 因为 F 是域, $x^d - 1$ 的根不超过 d 个, 其中至多 $\varphi(d)$ 个是 d 阶元.

$$n = \sum_{d|n} G \text{ 中 } d \text{ 阶元个数} \leq \sum_{d|n} \varphi(d) = n.$$

所以对 n 的每个因数 d, G 中恰好有 $\varphi(d)$ 个 d 阶元. 特别地, 有 $\varphi(n)$ 个 n 阶元, 所以 G 是循环群.

15. (5 分) 素数 p, q 满足 $p > q > 2$ 且 $q \mid p - 1$.

(1) 证明, 存在阶为 pq 的非循环群.

(2) (额外 2 分) 证明, 在同构意义下, 阶为 pq 的非循环群只有一个.

提示: 需要使用 Sylow 第三定理: 若 $|G| = p^k m$ (p 为素数, $\gcd(p, m) = 1$) , 记 Sylow p-子群的数目为 n_p, 那么 $n_p \mid m$ 且 $n_p \equiv 1 \pmod{p}$.

提示: 对任意有限域 $\mathbb{F}$, $\mathbb{F}^*$ 是循环群.

解 令 G 是一个 pq 阶非循环群.

根据 Sylow 第三定理, $n_p = 1$. 记这个唯一的 p 阶子群为 $P = \langle g \rangle \cong \mathbb{Z}_p$, 它是 G 的一个正规子群.

根据 Sylow 第一定理, 存在 q 阶子群. 记其中一个 q 阶子群为 $Q = \langle h \rangle \cong \mathbb{Z}_q$.

$G = QP$, 因此 G 中所有元素都可以唯一地表示为 $h^i g^j$, 其中 $i \in \mathbb{Z}_q, j \in \mathbb{Z}_p$. 因为 $Gh = hG$, 一定存在 t 使得 $gh = hg^t$. 因为 $x \mapsto h^{-1}xh = x^t$ 是 G 的自同态, 所以 $\gcd(t, \varphi(p)) = 1$, 也可以记为 $t \in \mathbb{Z}_p^*$. 因为 $g = gh^q = h^q g^{t^q} = g^{t^q}$, 所以 $t^q = 1$. 因为 $\mathbb{Z}_p^*$ 是循环群, 其中满足 $x^q = 1$ 的元素构成了一个 q 阶子群, 记为 $Q' \leq \mathbb{Z}_p^*$. 因为 G 是非交换群, 所以 $t \neq 1$.

(1) 对任意 $t \in Q'$, 只需验证乘法定义为 $h^i g^j \cdot h^{i'} g^{j'} = h^{i+i'} g^{j \cdot t^{i'} + j'}$ 确实使得 $\{h^i g^j | i \in \mathbb{Z}_q, j \in \mathbb{Z}_p\}$ 构成一个群.

注. 这里实际是在定义半直积.

为此只需验证存在单位元 $h^0 g^0$, 逆元 $(h^i g^j)^{-1} = h^{-i} g^{-t^{-i} \cdot j}$ 以及结合律

$$h^i g^j \cdot h^{i'} g^{j'} \cdot h^{i''} g^{j''} = h^{i+i'+i''} g^{j \cdot t^{i'+i''} + j' \cdot t^{i''} + j''}.$$

可以自然地定义和计算 t 的 $i \in \mathbb{Z}_q$ 次幂是因为 $t^q = 1$.

当 $t \neq 1$ 时, 这便是一个 pq 阶非循环群.

(2) 对任意 $s \in Q' \backslash \{1\}$, 其对应群 $H = \langle a, b | a^p = b^q = e, b^{-1}ab = a^s \rangle$, 其中的群运算为 $b^i a^j \cdot b^{i'} a^{j'} = b^{i+i'} a^{j \cdot t^{i'} + j'}$. 证明 H 同构于 G.

因为 $Q' \cong \mathbb{Z}_q$ 所以存在 $k, k^{-1} \in \mathbb{Z}_q$ 使得 $t = s^k, s = t^{k^{-1}}$. 考虑同态

$$\begin{aligned} \phi : G &\to H & \qquad \phi^{-1} : H &\to G \\ h^i g^j &\mapsto b^{ki} a^j & \qquad b^i a^j &\mapsto h^{k^{-1} i} g^j \end{aligned}$$

验证其确实为同态

$$\begin{aligned} \phi(h^i g^j \cdot h^{i'} g^{j'}) &= \phi(h^{i+i'} g^{j \cdot t^{i'} + j'}) = \phi(h^{i+i'} g^{j \cdot t^{i'} + j'}) = b^{ki + ki'} a^{j \cdot t^{i'} + j'}, \\ \phi(h^i g^j) \cdot \phi(h^{i'} g^{j'}) &= b^{ki} a^j \cdot b^{ki'} a^{j'} = b^{ki + ki'} a^{j \cdot s^{ki'} + j'} = b^{ki + ki'} a^{j \cdot t^{i'} + j'}. \end{aligned}$$

16. (5 分) 令 $K_1 = \mathbb{F}_{11}[x]/(x^2 + 1)$ 和 $K_2 = \mathbb{F}_{11}[y]/(y^2 + 2y + 2)$.

(1) 证明 K_1, K_2 均是大小为 121 的域.

(2) K_1 中元素可以记为 $ax + b$ 的形式, K_2 中元素可以记为 $ay + b$ 的形式, 其中 $a, b \in \mathbb{F}_{11}$. 在这种表示下, 给出一个 K_1 到 K_2 的域同构.

解

(1) 只需说明 $x^2 + 1$ 是不可约多项式. 对 $y^2 + 2y + 2$ 的验证留到下一问.

- 如果可约则有 1 次因式. $x^{11} - x$ 是 $\mathbb{F}_{11}[x]$ 中所有 1 次多项式的乘积.

$$\gcd(x^2 + 1, x^{11} - x) = \gcd(x^2 + 1, -2x) = \gcd(1, -2x) = 1.$$

- 如果有 1 次因式则有解, 枚举说明 $x^2 + 1$ 没有解.

$$1^2 = (-1)^2 = 1, \quad 2^2 = (-2)^2 = 4, \quad 3^2 = (-3)^2 = 9, \quad 4^2 = (-4)^2 = 5, \quad 5^2 = (-5)^2 = 3.$$

- x^2+1 是否有解等价于 -1 是否式模 11 的二次剩余. 根据二次互反律, -1 不是 11 的二次剩余.

(2) 考虑 $\mathbb{F}_{11}[x]$ 到 $\mathbb{F}_{11}[y]$ 的环同构

$$\begin{aligned} \phi : \mathbb{F}_{11}[x] &\to \mathbb{F}_{11}[y] & \phi^{-1} : \mathbb{F}_{11}[y] &\to \mathbb{F}_{11}[x] \\ f(x) &\mapsto f(y+1) & g(y) &\mapsto g(x-1) \end{aligned}$$

在 ϕ 同构下, (x^2+1) 被映射到 (y^2+2y+2), 所以 $\mathbb{F}_{11}[x]/(x^2+1) \cong \mathbb{F}_{11}[y]/(y^2+2y+2)$. 这个 ϕ 诱导的域同构将 $ax+b$ 映射到 $ay+a+b$.

另一个将 (x^2+1) 被映射到 (y^2+2y+2) 的环同构为 $f(x) \mapsto f(-y-1)$, 其诱导的域同构是 $ax+b \mapsto -ax-a+b$. 不难说明 K_1, K_2 之间只有这两个域同构.

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:

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

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

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

$$\frac{\begin{array}{c}\mathcal{D} \\ \phi(x)\end{array}}{\forall x \phi(x)} \forall I \qquad \frac{\forall x \phi(x)}{\phi(t)} \forall E$$

$\exists x$ 是 $\neg\forall x\neg$ 的缩写. 引入关系符号 $=$ 及对应推导规则或公理.