计算机科学与人工智能的数学基础 I

期末复习资料

作者：2025 级 AI 学组

时间：June 22, 2026

版本：1.0

目录

第一部分

逻辑学初步

第 1 章 命题逻辑

笔者按：逻辑学是整个数学和计算机科学的语言基础。命题逻辑处理的是” 不能再分解的陈述句” 之间的关系。你可以把命题逻辑理解为” 布尔代数的语法层面”——它关注的不是真值本身，而是真值之间的推导规则。这部分内容看似简单，但如果你把底层逻辑真正吃透，后面学谓词逻辑、集合论乃至程序验证都会轻松很多。

1.1 命题——逻辑的原子

1.1.1 定义

命题是能够判断真假的陈述句。

两层核心含义：

- 必须是**陈述句**。疑问句、祈使句、感叹句都不是命题。
- 必须有**唯一确定的真值**——要么真，要么假，不能模糊，不能既真又假（这叫**二值逻辑**）。

很多同学在这里会有一个误解：把” 我是否能判断真假” 和” 命题本身是否有真值” 混为一谈。一个命题客观上非真即假，但我可能不知道——这不妨碍它是个命题。比如” 外星人存在于地球之外”——这显然是个命题，只是我们暂时不知道它是真还是假。

不是命题的例子：

- ” 请勿吸烟”——祈使句，没有真假
- ” 你今天好吗？”——疑问句
- ” 这个小男孩多勇敢啊！”——感叹句
- ” 我正在说谎”——**悖论**。如果它为真，则我在说谎，所以它是假的；如果它为假，则我没说谎，所以它是真的。经典的自指悖论，揭示了自然语言和形式逻辑之间的鸿沟。

简单命题（原子命题）：不能再分解为更简单陈述句的命题。如” 今天下雨”。

复合命题：由若干简单命题通过**联结词**联结而成。如” 今天下雨且气温下降”。

原子命题是逻辑的” 原子”——不可再分的真值载体。复合命题的真值完全由原子命题的真值以及联结词的含义决定。这就是**真值函数性**——逻辑的核心特征之一。

1.2 联结词——逻辑的” 运算”

联结词是命题之间的运算。与代数中的加减乘除不同的是，这里的运算对象是真值（0 或 1），结果也是真值。

1.2.1 五种基本联结词

(1) 否定 ¬（一元联结词）

$\neg P$ 为真当且仅当 P 为假。相当于日常语言中的”非”、”不”、”没有”。

表 1.1:

P	$\neg P$
1	0
0	1

注意：日常语言中”这些都是男同学”的否定不是”这些都不是男同学”，而是**”并非这些都是男同学”**——即其中至少有一个不是男同学。自然语言到逻辑语言的翻译需要精确。

(2) 合取 ∧（二元联结词）

$P \wedge Q$ 为真当且仅当 P 和 Q **同时**为真。相当于”与”、”且”、”并且”、”而且”。

表 1.2:

P	Q	$P \wedge Q$
1	1	1
1	0	0
0	1	0
0	0	0

陷阱：不要见到”与”或”和”就机械地使用 ∧！例如”李文与李武是兄弟”——这不是 $P \wedge Q$，因为”是兄弟”是一个**二元关系谓词**，需要谓词逻辑才能准确表达。命题逻辑处理不了关系。

(3) 析取 ∨（二元联结词）

$P \vee Q$ 为真当且仅当 P 和 Q **至少有一个**为真。相当于”或”。

表 1.3:

P	Q	$P \vee Q$
1	1	1
1	0	1
0	1	1
0	0	0

相容或 vs. 排斥或：逻辑中的 ∨ 是**相容或**（inclusive OR）——允许两者同时为真。日常语言中的”或”很多时候是**排斥或**（exclusive OR）——比如”派小王或小李中的一人去开会”，不可能两人都去。排斥或需要额外表达：$(P \vee Q) \wedge \neg(P \wedge Q)$，或者 $(P \wedge \neg Q) \vee (\neg P \wedge Q)$。

(4) 蕴含 →（二元联结词）

$P \to Q$ 为假当且仅当 P 为真而 Q 为假。其余情况全为真。

这是初学逻辑最大的困惑之一：为什么前件为假时，蕴含式自动为真？

表 1.4:

P	Q	$P \to Q$
1	1	1
1	0	0
0	1	1
0	0	1

理解方式一（承诺模型）：某人承诺”如果明天下雨，我就带伞”。如果明天没下雨（$P = 0$），无论他带不带伞，他都没有违背承诺——所以命题为真。

理解方式二（集合模型）：$P \to Q$ 等价于”P 的集合是 Q 的集合的子集”。当 P 为假时，相当于从空集出发——空集是任何集合的子集。

理解方式三（数学角度）：$P \to Q \equiv \neg P \vee Q$。当 $P = 0$ 时，$\neg P = 1$，析取自然为真。记住这个等价式，一切疑惑迎刃而解。

自然语言到 $\to$ 的翻译技巧：

- ”只要 P，就 Q” $\to P \to Q$
- ”如果 P，那么 Q” $\to P \to Q$
- ”只有 P，才 Q” $\to Q \to P$（注意方向！这和直觉是反的）
- ”除非 P，否则 Q” $\to \neg P \to Q$（等价于 $P \vee Q$）
- ”Q 仅当 P” $\to Q \to P$

”只有”和”除非”是高频易错点。”只有天冷，小王才穿羽绒服”——穿羽绒服蕴含天冷，即 $Q \to P$，不是 $P \to Q$！因为穿羽绒服这个事实可以推导出天冷，但天冷不必然导致穿羽绒服。

(5) 等价 $\leftrightarrow$（二元联结词）

$P \leftrightarrow Q$ 为真当且仅当 P 和 Q 真值**相同**。即 $(P \to Q) \wedge (Q \to P)$。

表 1.5:

P	Q	$P \leftrightarrow Q$
1	1	1
1	0	0
0	1	0
0	0	1

1.2.2 运算优先级

$$\neg \quad > \quad \wedge, \vee \quad > \quad \to \quad > \quad \leftrightarrow$$

实在记不住的话——**加括号**。宁可多写几个括号，也不要在考试中因为优先级搞错丢分。

PPT 例题——联结词的符号化：

1. 合取与析取的区分（PPT 例 1.1.2-1.1.3）：

表 1.6:

原句	符号化（设 p: 李平聪明, q: 李平用功）
李平既聪明又用功	$p \wedge q$
李平虽然聪明，但不用功	$p \wedge \neg q$
李平不但聪明，而且用功	$p \wedge q$
李平不是不聪明，而是不用功	$\neg(\neg p) \wedge \neg q$（即 $p \wedge \neg q$）

”虽然…但…”、”不但…而且…” ——看起来像转折或递进，但在逻辑上都是**合取**！

排斥或 vs 相容或（PPT 例 1.1.3）：

- ”小王爱打球**或**爱跑步” → $p \vee q$（相容或，可以两者都爱）
- ”派小王**或**小李中的**一人**去开会” → $(p \wedge \neg q) \vee (\neg p \wedge q)$（排斥或，两人不能同时去）

2. 蕴涵的翻译——”只要”vs”只有”（PPT 例 1.1.4-1.1.5，设 p: 天冷, q: 小王穿羽绒服）：

表 1.7:

自然语言	符号化	规律
只要天冷，小王就穿羽绒服	$p \to q$	”只要”后面是**前件**
如果天冷，小王**那么**穿羽绒服	$p \to q$	”如果”后面是前件
只有天冷，小王**才**穿羽绒服	$q \to p$	”只有”后面是**后件**！
除非天冷，小王**才**穿羽绒服	$q \to p$	同”只有…才…”
小王穿羽绒服**仅当**天冷	$q \to p$	”仅当”后面是后件
除非小王穿羽绒服，**否则**天不冷	$\neg q \to \neg p$（即 $p \to q$）	”除非 A 否则 B” → $\neg A \to B$

核心易错点：中文的”只有 A 才 B”和”如果 A 就 B”方向相反！”只有”后面跟的是**必要条件**（结论的前件），”如果”后面跟的是**充分条件**（前件）。记法：**”只要”= 充分 =”如果”，”只有”= 必要 =”仅当”**。

3. 等价联结词实例（设 p: 2+2=4 为真, q: 3 是奇数为真）：

- $p \leftrightarrow q$（2+2=4 当且仅当 3 是奇数）→ **真**
- $p \leftrightarrow \neg q$（2+2=4 当且仅当 3 不是奇数）→ **假**

1.3 命题公式——从原子到复合

1.3.1 命题公式的构造（递归定义）

1. 单个命题变项是公式（基础）
2. 若 A 是公式，则 $\neg A$ 是公式（否定）
3. 若 A, B 是公式，则 $A \wedge B$、$A \vee B$、$A \to B$、$A \leftrightarrow B$ 均是公式

这种递归定义在计算机科学中随处可见——编程语言的语法、树结构、归纳证明……本质上都是同一个思路：先定义原子，再定义构造规则。

命题常项 vs 命题变项：

- 常项：真值确定的命题（如”2+2=4”）
- 变项：真值待定的占位符（如 p, q, r），类似于代数中的 x, y

命题变项本身**不是命题**——它没有确定的真值。只有当你把具体的命题代入变项后，才得到一个命题。这和函数 $f(x)$ 在没有代入 x 之前不是一个具体的数值是同样的道理。

1.3.2 公式的赋值与真值表

给公式中所有命题变项指定一组真值，就能按联结词的定义逐层计算出整个公式的真值。对所有可能的赋值形成的表格就是**真值表**。

n 个命题变项有 2^n 种不同的赋值。

真值表法是逻辑中最” 暴力” 但也最可靠的方法——当你不确定两个公式是否等价、不确定推理是否正确时，直接画真值表。虽然笨，但绝对不会错。

例（真值表构造）：构造公式 $\Phi = (p \wedge q) \to (\neg p \vee r)$ 的真值表。

三个变项 p, q, r，共 $2^3 = 8$ 行。按列逐步计算：

表 1.8:

p	q	r	$p \wedge q$	$\neg p$	$\neg p \vee r$	Φ
0	0	0	0	1	1	1
0	0	1	0	1	1	1
0	1	0	0	1	1	1
0	1	1	0	1	1	1
1	0	0	0	0	0	1
1	0	1	0	0	1	1
1	1	0	1	0	0	**0**
1	1	1	1	0	1	1

Φ 只在 $(1, 1, 0)$ 时为假，其他全为真，故 Φ 是一个**可满足式**（不是永真式，因为存在一行使其为假）。

技巧：真值表构造时，按照” 由内向外” 的顺序逐步计算子公式的真值——先算最内层的 $p \wedge q$ 和 $\neg p$，再算 $\neg p \vee r$，最后算 $\to$。这样不容易出错。

1.3.3 公式的三种分类

表 1.9:

类型	定义	例子
永真式（重言式）	所有赋值下均为真	$P \vee \neg P$
永假式（矛盾式）	所有赋值下均为假	$P \wedge \neg P$
可满足式	至少存在一组赋值使其为真	$P \wedge Q$（当 $P = Q = 1$ 时为真）

永真式是逻辑的” 公理”——不依赖于任何具体事实，仅凭逻辑形式就能保证为真。它们是推理的基石。而永假式是所有逻辑错误的终极形态。

PPT 例题——用真值表判断公式类型：

例 1（PPT 例 1.2.2）：判断 $(p \wedge (p \to q)) \to q$ 的类型。

表 1.10:

p	q	$p \to q$	$p \wedge (p \to q)$	$(p \wedge (p \to q)) \to q$
0	0	1	0	1
0	1	1	0	1
1	0	0	0	1
1	1	1	1	1

最后一列全为 1 → **永真式（重言式）**。这就是著名的**假言推理**（Modus Ponens）的逻辑形式。

例 2（PPT 例 1.2.3）：判断 $\neg(p \to q) \wedge q$ 的类型。

表 1.11:

p	q	$p \to q$	$\neg(p \to q)$	$\neg(p \to q) \wedge q$
0	0	1	0	0
0	1	1	0	0
1	0	0	1	0
1	1	1	0	0

最后一列全为 0 → **矛盾式（永假式）**。

例 3（PPT 例 1.2.1）：求 $\neg(p \to (q \vee r))$ 的成真赋值和成假赋值。

表 1.12:

p	q	r	$q \vee r$	$p \to (q \vee r)$	$\neg(p \to (q \vee r))$
0	0	0	0	1	0
0	0	1	1	1	0
0	1	0	1	1	0
0	1	1	1	1	0
1	**0**	**0**	**0**	**0**	**1**
1	0	1	1	1	0
1	1	0	1	1	0
1	1	1	1	1	0

成真赋值：$(1,0,0)$（仅此一组），成假赋值：其余 7 组。该公式为**可满足式**（不是永真也不是永假）。

1.4 【重点】1.4 等值验算/等值运算法则——公式之间的" 相等"

1.4.1 什么是等值

若 $A \leftrightarrow B$ 是永真式，则称 A 与 B **等值**（逻辑等价），记作 $A \Leftrightarrow B$。

注意区分 $\leftrightarrow$ 和 $\Leftrightarrow$：- $\leftrightarrow$ 是**联结词**，属于逻辑语言内部 - $\Leftrightarrow$ 是**元语言符号**，用来描述两个公式之间在逻辑上等价

就好像 $=$ 和 $\equiv$ 的区分——一个在语言内，一个在语言外描述语言。

1.4.2 核心等价公式

以下 24 个等价式是命题逻辑的”乘法口诀”，需要熟练掌握。但更重要的是**理解每个等价式背后的直观含义**，而不是死记硬背。

(1) 双重否定律： $\neg\neg P \Leftrightarrow P$

负负得正。但要注意：有些逻辑系统（如直觉主义逻辑）不承认双重否定律，因为”并非不真”不一定意味着”构造性地证明了真”。不过在本课的二值逻辑中，它成立。

(2) 幂等律： $P \vee P \Leftrightarrow P$，$P \wedge P \Leftrightarrow P$

重复说同一句话不增加信息量。

(3) 交换律： $P \vee Q \Leftrightarrow Q \vee P$，$P \wedge Q \Leftrightarrow Q \wedge P$

(4) 结合律： $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$，$(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$

(5) 分配律：

- $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$
- $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$

注意：逻辑中 $\wedge$ 对 $\vee$ 的分配和 $\vee$ 对 $\wedge$ 的分配**都成立**——这和普通代数不太一样！在代数里 $a + (b \times c) \neq (a + b) \times (a + c)$，但在逻辑里两者都成立。原因是布尔代数的对称性。

(6) 德·摩根律（极其重要！）：

- $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$
- $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$

德摩根律的哲学含义：”所有人都满意”的反面不是”所有人都不满意”，而是”**存在一个人不满意**”。合取的否定变成否定的析取。这在编程中也常用——`!(a && b)` 等价于 `!a || !b`。

(7) 吸收律：

- $P \vee (P \wedge Q) \Leftrightarrow P$
- $P \wedge (P \vee Q) \Leftrightarrow P$

直观理解：$P \wedge Q$ 的条件比 P 更强（要求更多），所以 P 或 $(P \wedge Q)$ 的真值取决于更弱的那一个——P。

(8) 零律： $P \vee 1 \Leftrightarrow 1$，$P \wedge 0 \Leftrightarrow 0$

(9) 同一律： $P \vee 0 \Leftrightarrow P$，$P \wedge 1 \Leftrightarrow P$

(10) 排中律： $P \vee \neg P \Leftrightarrow 1$

一个命题要么为真，要么为假——没有第三种可能。这是二值逻辑的基石。

(11) 矛盾律： $P \wedge \neg P \Leftrightarrow 0$

一个命题不能同时为真且为假。亚里士多德三大逻辑定律之一。

(12) 蕴含等值式： $P \to Q \Leftrightarrow \neg P \vee Q$

这是最重要的等价式。它把蕴含这种” 如果... 那么...” 的语义关系，转化为一个纯粹的布尔表达式。很多公式的化简和证明都从这一步开始。

(13) 等价等值式： $P \leftrightarrow Q \Leftrightarrow (P \to Q) \wedge (Q \to P) \Leftrightarrow (\neg P \vee Q) \wedge (\neg Q \vee P)$

(14) 假言易位（逆否命题）： $P \to Q \Leftrightarrow \neg Q \to \neg P$

” 如果下雨，地就湿” 等价于” 如果地没湿，就没下雨”。这是数学反证法的逻辑基础。

(15) 归谬论： $(P \to Q) \wedge (P \to \neg Q) \Leftrightarrow \neg P$

如果一个命题能推导出矛盾（Q 和 $\neg Q$ 同时成立），那么该命题必假。这就是**反证法**的逻辑形式。

1.4.3 记忆方法总结

这么多等价式，怎么记？抓住三条核心，其余都是推论：

第一核心（蕴涵转析取）： $P \to Q \Leftrightarrow \neg P \vee Q$。一切 $\to$ 都可以消去，这是化简的第一步。

第二核心（德摩根律）： $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$，$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$。” 否定穿进去，$\wedge$ 变 $\vee$，$\vee$ 变 $\wedge$”。

第三核心（分配律）： $\wedge$ 和 $\vee$ 互相分配（两个方向都成立！）。

其余公式分组记忆：

- **类代数组**（和普通代数一样）：交换律、结合律、分配律（$\wedge$ 对 $\vee$）$\to$ 照搬代数直觉
- **布尔特有组**（普通代数没有）：幂等律、吸收律、$\vee$ 对 $\wedge$ 的分配律 $\to$ 用真值表验一次就记住
- **常量组：** 零律（$\vee$ 1 = 1, $\wedge$ 0 = 0）、同一律（$\vee$ 0 = P, $\wedge$ 1 = P）$\to$ 类似算术
- **否定组：** 双重否定、排中律、矛盾律 $\to$ 直觉即可
- **推理工具组：** 蕴涵等值式、假言易位、归谬论 $\to$ 证明题高频使用，必须熟练

实战技巧： 化简时永远优先用蕴涵等值式消去 $\to$ 和 $\leftrightarrow$，然后用德摩根律把否定深入，最后用分配律展开或吸收律合并。

1.4.4 置换定理

若 $A \Leftrightarrow B$，则将公式 Φ 中出现的 A 替换为 B，得到的新公式与原公式等价。

这保证了等价代换的合法性。有了这个定理和上面的等价公式，就可以像代数化简一样化简逻辑表达式。

PPT 例题——等值演算：

例 1（PPT 例 1.3.3）：用等值演算证明 $(p \to r) \wedge (q \to r) \Leftrightarrow (p \vee q) \to r$。

证：

$(p \to r) \wedge (q \to r)$
$\Leftrightarrow (\neg p \vee r) \wedge (\neg q \vee r)$（蕴涵等值式）
$\Leftrightarrow (\neg p \wedge \neg q) \vee r$（分配律：$(\neg p \vee r) \wedge (\neg q \vee r) \Leftrightarrow (\neg p \wedge \neg q) \vee r$）
$\Leftrightarrow \neg(p \vee q) \vee r$（德 • 摩根律）
$\Leftrightarrow (p \vee q) \to r$（蕴涵等值式）□

例 2（PPT 例 1.3.4）：用等值演算判断 $((p \to q) \wedge p) \to q$ 的类型。

解：

$((p \to q) \wedge p) \to q$
$\Leftrightarrow ((\neg p \vee q) \wedge p) \to q$（蕴涵等值式）
$\Leftrightarrow ((\neg p \wedge p) \vee (q \wedge p)) \to q$（分配律）
$\Leftrightarrow (0 \vee (q \wedge p)) \to q$（矛盾律）
$\Leftrightarrow (q \wedge p) \to q$（同一律）
$\Leftrightarrow \neg(q \wedge p) \vee q$（蕴涵等值式）
$\Leftrightarrow (\neg q \vee \neg p) \vee q$（德 • 摩根律）
$\Leftrightarrow \neg p \vee (\neg q \vee q)$（交换律 + 结合律）
$\Leftrightarrow \neg p \vee 1$（排中律）
$\Leftrightarrow 1$（零律）

故该公式为**永真式（重言式）**。

例 3（PPT 例 1.3.6②）：用等值演算判断 $\neg(p \to (p \vee q)) \wedge r$ 的类型。

解：

$\neg(p \to (p \vee q)) \wedge r$
$\Leftrightarrow \neg(\neg p \vee (p \vee q)) \wedge r$（蕴涵等值式）
$\Leftrightarrow \neg((\neg p \vee p) \vee q) \wedge r$（结合律）
$\Leftrightarrow \neg(1 \vee q) \wedge r$（排中律）
$\Leftrightarrow \neg 1 \wedge r$（零律）
$\Leftrightarrow 0 \wedge r$（否定）
$\Leftrightarrow 0$（零律）

故该公式为**矛盾式（永假式）**。注意：不管 r 取什么值，只要前面是 0，整个合取就是 0。

1.5 范式——逻辑表达式的” 标准形”

回顾线性代数：每个向量在不同的基下有不同表示，但标准正交基下的表示最规范。范式就是命题逻辑中的” 标准正交基”——把任意公式化为统一的标准形式，便于比较、分析和应用。

1.5.1 简单析取式与简单合取式

- **简单析取式**：仅由命题变项及其否定通过 $\vee$ 连接。如 $P \vee \neg Q \vee R$
- **简单合取式**：仅由命题变项及其否定通过 $\wedge$ 连接。如 $P \wedge \neg Q \wedge R$

1.5.2 析取范式（DNF）与合取范式（CNF）

- **析取范式**：若干简单合取式的析取 → 形如：(合取项) ∨ (合取项) ∨ · · ·
- **合取范式**：若干简单析取式的合取 → 形如：(析取项) ∧ (析取项) ∧ · · ·

DNF 和 CNF 的应用意义：DNF 自然地对应”使公式为真的所有情况”——每个合取项对应一组条件，只要满足任一组条件公式就为真。CNF 则对应”使公式为假的所有排除条件”。在电路设计中，DNF 对应 AND-OR 两级电路，CNF 对应 OR-AND 两级电路。

1.5.3 极小项与极大项

这是范式中最关键、也是考试最爱考的概念：

极小项（minterm）：包含 n 个命题变项中**每一个**（或其否定）恰好一次的简单合取式。

- n 个变项共有 2^n 个不同的极小项
- 每个极小项只在**一种**赋值下为真——这就是”极小”的含义：它为真的”范围”极小，只有一个点
- 每个极小项对应真值表中的一行（真值为 1 的那一行）

极大项（maxterm）：包含 n 个命题变项中**每一个**（或其否定）恰好一次的简单析取式。

- n 个变项共有 2^n 个不同的极大项
- 每个极大项只在**一种**赋值下为假——”极大”意味着它几乎总是真的，只在一个点处为假
- 每个极大项对应真值表中的一行（真值为 0 的那一行）

极小项和极大项的关系：极小项 m_i 和极大项 M_i 互为否定——$\neg m_i \Leftrightarrow M_i$，$\neg M_i \Leftrightarrow m_i$。这意味着极小项和极大项之间存在精确的一一对应。理解了这个，主析取范式和主合取范式之间的转换就很容易了。

1.5.4 【重点】主析取范式与【不考】主合取范式

- **主析取范式**：由极小项构成的析取范式。每个命题公式有**唯一**的主析取范式。
- **主合取范式**：由极大项构成的合取范式。每个命题公式有**唯一**的主合取范式。

主范式的”唯一性”是它最强大的地方——两个公式逻辑等价当且仅当它们有相同的主析取范式（或主合取范式）。这提供了一个机械化的等价判定方法。

构造方法：

1. 消去 → 和 ↔（用 $\neg P \vee Q$ 和 $(\neg P \vee Q) \wedge (\neg Q \vee P)$）
2. 用德摩根律把否定深入（否定符只出现在变项前）
3. 用分配律展开
4. 补全缺失的变项（用 $P \vee \neg P$ 或 $P \wedge \neg P$）

由真值表直接得到主范式：

- 找所有真值为 1 的行 → 每一行对应一个极小项 → 析取起来 = 主析取范式
- 找所有真值为 0 的行 → 每一行对应一个极大项 → 合取起来 = 主合取范式

这是”偷懒”的方法，也是最不容易出错的方法。如果变项不多（≤4 个），直接用真值表法比代数推导更快更可靠。

例 1（真值表求主范式）：求公式 $(p \to q) \wedge r$ 的主析取范式和主合取范式。

解：三个变项 p, q, r，共 $2^3 = 8$ 种赋值。

表 1.13:

p	q	r	$p \to q$	$(p \to q) \wedge r$
0	0	0	1	0
0	0	1	1	**1**
0	1	0	1	0
0	1	1	1	**1**
1	0	0	0	0
1	0	1	0	0
1	1	0	1	0
1	1	1	1	**1**

真值为 1 的行：$(0,0,1)$、$(0,1,1)$、$(1,1,1)$，分别对应极小项：

- $(0,0,1) \to \neg p \wedge \neg q \wedge r$ (即 m_1)
- $(0,1,1) \to \neg p \wedge q \wedge r$ (即 m_3)
- $(1,1,1) \to p \wedge q \wedge r$ (即 m_7)

主析取范式： $\boxed{(\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge q \wedge r)}$

真值为 0 的行对应极大项，由极大项合取得**主合取范式：**

$$\boxed{(p \vee q \vee r) \wedge (p \vee \neg q \vee r) \wedge (\neg p \vee q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (\neg p \vee \neg q \vee r)}$$

极小项的编码规则：把 p 看作最高位，0 对应 $\neg$，1 对应原变量。$(0,0,1)$ 对应 m_1，$(1,1,1)$ 对应 m_7。

例 2（代数法求主范式）：求公式 $(p \vee q) \to r$ 的主析取范式。

解：

1. 消去 $\to$：$\neg(p \vee q) \vee r$
2. 德摩根律：$(\neg p \wedge \neg q) \vee r$
3. 补全缺失变项：第一个合取项缺 r，第二个合取项缺 p, q
   - $\neg p \wedge \neg q \to (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$
   - $r \to$ 需要展开为包含 p, q 的极小项：$(p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge r)$
1. 合并相同项，得最终主析取范式。

可以验证：代数法和真值表法得到的结果一致——实际上主析取范式是**唯一**的，两种方法殊途同归。

例 3（真值表法求主析取范式）：求公式 $(p \wedge q) \to (\neg q \vee r)$ 的主析取范式。

解：三个变项 p, q, r，共 $2^3 = 8$ 种赋值。

真值为 1 的行共 7 行（除 $(1,1,0)$ 外），分别对应极小项：

- $(0,0,0) \to \neg p \wedge \neg q \wedge \neg r$ (即 m_0)
- $(0,0,1) \to \neg p \wedge \neg q \wedge r$ (即 m_1)
- $(0,1,0) \to \neg p \wedge q \wedge \neg r$ (即 m_2)
- $(0,1,1) \to \neg p \wedge q \wedge r$ (即 m_3)

表 1.14:

p	q	r	$p \wedge q$	$\neg q$	$\neg q \vee r$	Φ
0	0	0	0	1	1	1
0	0	1	0	1	1	1
0	1	0	0	0	0	1
0	1	1	0	0	1	1
1	0	0	0	1	1	1
1	0	1	0	1	1	1
1	1	0	1	0	0	**0**
1	1	1	1	0	1	1

- $(1,0,0) \to p \wedge \neg q \wedge \neg r$ (即 m_4)
- $(1,0,1) \to p \wedge \neg q \wedge r$ (即 m_5)
- $(1,1,1) \to p \wedge q \wedge r$ (即 m_7)

主析取范式： $\boxed{m_0 \vee m_1 \vee m_2 \vee m_3 \vee m_4 \vee m_5 \vee m_7}$，即 $\Sigma(0,1,2,3,4,5,7)$。

这个例子说明：如果真值表中绝大部分行都是 1，主析取范式会很”长”。此时用主合取范式反而更简洁——只有一个极大项 M_6：$(\neg p \vee \neg q \vee r)$。

谓词符号化例题（PPT 例 2.1.1-2.1.4）：

表 1.15:

原句	个体域	符号化
王明是劳动模范	全总个体域	$M(a)$，其中 $M(x)$：x 是劳模，a：王明
小李是小赵的老师	全总个体域	$T(s,t)$，其中 $T(x,y)$：x 是 y 的老师
所有人都是要死的	全总个体域	$\forall x(M(x) \to F(x))$，$M(x)$：x 是人
有的人活百岁以上	全总个体域	$\exists x(M(x) \wedge P(x))$
凡是有理数均可表为分数	实数域	$\forall x(R(x) \to F(x))$
有的有理数是整数	实数域	$\exists x(R(x) \wedge G(x))$

谓词符号化进阶（PPT 例 2.1.4 ）：

- ”任何金属都可以溶解在某种液体中” $\to \forall x(M(x) \to \exists y(L(y) \wedge D(x,y)))$
- ”不管白猫黑猫，抓住老鼠就是好猫” $\to \forall x(C(x) \wedge (W(x) \vee B(x)) \wedge \exists y(M(y) \wedge K(x,y)) \to G(x))$

PPT 例题——谓词逻辑有效性判断（例 2.2.3）：

判断以下公式哪些是逻辑有效式（在任何解释下均为真）：

(1) $\forall x F(x) \to \exists x F(x)$ → **逻辑有效式**（非空域中，全称蕴含存在）

(2) $\forall x F(x) \to (\forall x \exists y G(x,y) \to \forall x F(x))$ → **逻辑有效式**（代入永真式 $p \to (q \to p)$）

(3) $\neg(F(x,y) \to R(x,y)) \wedge R(x,y)$ → **矛盾式**（代入矛盾式 $\neg(p \to q) \wedge q$）

(4) $\forall x \exists y F(x,y) \to \exists x \forall y F(x,y)$ → **不是逻辑有效式**。反例：$F(x,y)$ 为”$x = y$” 在自然数域中，前件真（每人都有一个等于自己的人），后件假（不存在等于所有人的那个人）。

PPT 例题——前束范式（例 2.3.3）：

课上 PPT 大量出现这种”批量求前束范式”的题目，考试很大概率会出类似的。

- 若派甲，则也派丙或丁

表 1.16:

公式	前束范式
$\forall x F(x) \wedge \neg \exists x G(x)$	$\forall x (F(x) \wedge \neg G(x))$
$\forall x F(x) \vee \neg \exists x G(x)$	$\forall x \forall y (F(x) \vee \neg G(y))$
$\forall x F(x) \to \exists x G(x)$	$\exists x (F(x) \to G(x))$
$\exists x F(x) \to \forall x G(x)$	$\forall x \forall y (F(x) \to G(y))$

- 若派乙，则也派甲或丙
- 若派丙，则也派丁
- 甲和丁不能同时派

试用真值表法决定派谁参加比赛。

解：设 p：派甲，q：派乙，r：派丙，s：派丁。

四个条件符号化：

(1) $p \to (r \vee s)$

(2) $q \to (p \vee r)$

(3) $r \to s$

(4) $\neg(p \wedge s)$（甲和丁不能同时派）

总条件：$\Phi = (1) \wedge (2) \wedge (3) \wedge (4)$

列真值表（16 行），找出 $\Phi = 1$ 的行：

- $p = 1, q = 0, r = 0, s = 1$：派甲和丁
- $p = 0, q = 1, r = 1, s = 0$：派乙和丙

故有两种方案：**（甲，丁）或（乙，丙）**。

这个例子展示了真值表法的实际用途：把自然语言约束翻译成逻辑公式，然后机械化地找出所有可行解。在电路设计、调度问题中，这种方法是 SAT 求解器的雏形。

1.6 【不考】1.6 联结词全功能集——逻辑的”最小完备集”

1.6.1 【不考】真值函数

n 个命题变项可以构成 2^{2^n} 个不同的真值函数。

为什么是 2^{2^n}？n 个变项有 2^n 种赋值组合（真值表有 2^n 行），而每一种赋值下函数可以输出 0 或 1，所以共有 2^{2^n} 种可能的函数。当 $n = 1$ 时有 4 种，$n = 2$ 时有 16 种——你列的 5 种联结词只覆盖了其中的一部分。

1.6.2 全功能集

一个联结词集合称为**全功能集**（或称功能完备集），如果任何真值函数都可以仅用该集合中的联结词表达。

常见全功能集：

- $\{\neg, \wedge\}$ ——可以只用” 非” 和” 与” 表达一切
- $\{\neg, \vee\}$ ——” 非” 和” 或”
- $\{\neg, \rightarrow\}$ ——” 非” 和” 蕴含”
- $\{\uparrow\}$ ——与非（Sheffer stroke），单元素全功能集！
- $\{\downarrow\}$ ——或非（Peirce arrow），也是单元素全功能集！

这意味着：理论上，你可以只用一种逻辑门（NAND 或 NOR）搭建出整个计算机。事实上，早期的集成电路确实偏爱 NAND 门，因为它在硅上的实现最简单。这个来自逻辑学的发现，直接影响了半导体工业的设计哲学。

冗余联结词： $\rightarrow$、$\leftrightarrow$、$\wedge$（在有 $\neg$ 和 $\vee$ 时冗余）、$\vee$（在有 $\neg$ 和 $\wedge$ 时冗余）。

1.7 【重点】1.7 推理理论——从前提推导结论

1.7.1 什么是有效推理

推理 $(A_1 \wedge A_2 \wedge \cdots \wedge A_n) \rightarrow B$ 为**永真式**时，称 B 是 $A_1, A_2, \cdots, A_n$ 的**逻辑结论**，推理是**有效的**。

注意：推理有效 $\neq$ 结论为真！推理有效只保证” 如果前提都为真，则结论必然为真”。如果前提中有一个是假的，那结论是真是假就不好说了。

1.7.2 核心推理规则

(1) 附加律： $P \implies P \vee Q$

如果 P 成立，那么 P 或任何其他命题也成立——真理加上任意的” 或” 还是真理。

(2) 化简律： $P \wedge Q \implies P$

合取可以直接拆开使用。但反过来不行——从 P 推不出 $P \wedge Q$。

(3) 假言推理（Modus Ponens）： $P \rightarrow Q, P \implies Q$

这可能是最自然、最常用的推理形式：” 如果下雨地就湿，下雨了，所以地湿。” 三段论的根本。

(4) 拒取式（Modus Tollens）： $P \rightarrow Q, \neg Q \implies \neg P$

” 如果下雨地就湿，地没湿，所以没下雨。”——反证法和故障诊断的逻辑基础。

(5) 析取三段论： $P \vee Q, \neg P \implies Q$

” 要么 A 要么 B，不是 A，所以是 B。”——排除法推理。

(6) 假言三段论： $P \to Q, Q \to R \implies P \to R$

蕴含的传递性。

(7) 等价三段论： $P \leftrightarrow Q, Q \leftrightarrow R \implies P \leftrightarrow R$

等价的传递性。类似代数的 $a = b, b = c \Rightarrow a = c$。

(8) 构造性二难： $(P \to Q) \wedge (R \to S), P \vee R \implies Q \vee S$

两条路，不管你走哪条，都会有对应的后果。

(9) 破坏性二难： $(P \to Q) \wedge (R \to S), \neg Q \vee \neg S \implies \neg P \vee \neg R$

后果没有发生，说明前提不成立——" 顺藤摸瓜的反向"。

记忆口诀： 前 6 条是" 基本款"（考最多），后 3 条是" 进阶款"。等价三段论 = 等价的传递，构造性二难 = 选路都有后果，破坏性二难 = 无果则无因。

1.7.3 证明方法

直接证明： 从前提出发，反复应用推理规则，直至推导出结论。

附加前提证明法（CP 规则）： 如果要证 $A \implies (B \to C)$，可以把 B 作为附加前提加入，转而证明 $A \wedge B \implies C$。这相当于把" 如果 B 则 C" 的 B 暂时" 假设为真"。

CP 规则的本质：$(A \to (B \to C)) \Leftrightarrow ((A \wedge B) \to C)$。这等价于函数的 Currying 化——一个二元函数可以看作每次接受一个参数的一元函数链。

反证法（归谬法）： 要证 $A \implies B$，假设 A 和 $\neg B$ 同时成立，推出矛盾（如 $P \wedge \neg P$），则原推理成立。

反证法的逻辑形式：$(A \wedge \neg B) \to (P \wedge \neg P) \implies A \to B$。

PPT 例题——推理证明：

例 1（直接证明，PPT 例 1.6.2）： 证明" 如果明天是周二或周五，则我有课。如果我有课，则今天必须备课。我今天下午没备课。所以明天不是周二也不是周五。"

设 p：明天周二，q：明天周五，r：有课，s：备课。

前提：$(p \vee q) \to r$, $r \to s$, $\neg s$。结论：$\neg p \wedge \neg q$。

证明：

1. $r \to s$　　前提引入
2. $\neg s$　　前提引入
3. $\neg r$　　1,2 拒取式
4. $(p \vee q) \to r$　　前提引入
5. $\neg(p \vee q)$　　3,4 拒取式
6. $\neg p \wedge \neg q$　　5 德摩根律 □

例 2（CP 规则，PPT 例 1.6.1-CP）：证明 $p \vee q,\ p \to r,\ r \to \neg s \implies s \to q$。

证明（附加前提 s）：

1. $p \to r$ 前提引入
2. $r \to \neg s$ 前提引入
3. $p \to \neg s$ 1,2 假言三段论
4. s 附加前提引入
5. $\neg p$ 3,4 拒取式
6. $p \vee q$ 前提引入
7. q 5,6 析取三段论
8. $s \to q$ CP 规则 □

例 3（反证法，PPT 例 1.6.1-反证）：证明 $\neg(p \wedge q) \vee r,\ r \to s,\ \neg s,\ p \implies \neg q$。

证明（假设 q，推出矛盾）：

1. $r \to s$ 前提引入
2. $\neg s$ 前提引入
3. $\neg r$ 1,2 拒取式
4. $\neg(p \wedge q) \vee r$ 前提引入
5. $\neg(p \wedge q)$ 3,4 析取三段论
6. $\neg p \vee \neg q$ 5 德摩根律
7. q 否定结论引入
8. $\neg p$ 6,7 析取三段论
9. p 前提引入
10. $p \wedge \neg p$ 8,9 合取（**矛盾！**）□

例：用等值演算判断公式 $((p \to q) \wedge p) \to q$ 的类型。

解：

$((p \to q) \wedge p) \to q$

$\Leftrightarrow \neg((\neg p \vee q) \wedge p) \vee q$ （蕴涵等值式）

$\Leftrightarrow (\neg(\neg p \vee q) \vee \neg p) \vee q$ （德摩根律）

$\Leftrightarrow ((p \wedge \neg q) \vee \neg p) \vee q$ （德摩根律）

$\Leftrightarrow ((p \vee \neg p) \wedge (\neg q \vee \neg p)) \vee q$ （分配律）

$\Leftrightarrow (1 \wedge (\neg q \vee \neg p)) \vee q$ （排中律）

$\Leftrightarrow (\neg q \vee \neg p) \vee q$ （同一律）

$\Leftrightarrow \neg p \vee (\neg q \vee q)$ （交换律 + 结合律）

$\Leftrightarrow \neg p \vee 1$ （排中律）

$\Leftrightarrow 1$ （零律）

故该公式为**永真式（重言式）**。

第 2 章 谓词逻辑

命题逻辑有一个根本性的局限：它不能表达” 所有” 和” 存在” 这样的量化关系。命题逻辑处理的是整体命题之间的关系，但不能**看穿命题的内部结构**。谓词逻辑解决了这个问题——它把命题拆解为” 个体” 和” 谓词”，并通过量词来表达普遍性和存在性。

2.1 为什么需要谓词逻辑？

考虑这个经典的三段论推理：

所有人都会死。苏格拉底是人。所以苏格拉底会死。

在命题逻辑中，这三句话只能分别表示为 P、Q、R。而 $(P \land Q) \to R$ **不是永真式**——你无法从 P 和 Q 推导出 R！因为命题逻辑看不到” 人” 和” 会死” 之间的内部联系。

谓词逻辑通过引入**谓词**和**量词**解决了这个问题：

- $\forall x(Human(x) \to Mortal(x))$ ——对任意 x，如果 x 是人则 x 会死
- $Human(Socrates)$ ——苏格拉底是人
- $\therefore Mortal(Socrates)$ ——所以苏格拉底会死

这正是谓词逻辑的力量——它能表达命题内部的逻辑结构，从而使三段论这种最自然的推理形式变得严格可证。

2.2 【重点】2.2 谓词逻辑的基本元素（谓词逻辑符号化）

2.2.1 个体词

表示讨论对象的符号。包括：

- **个体常项**：具体对象，如 a（张三）、b（北京）
- **个体变项**：抽象占位符，如 x, y, z

2.2.2 谓词

表示个体的性质或个体之间关系的符号。

- **一元谓词** $P(x)$：描述单个体的性质。如 $Student(x)$（x 是学生）、$Prime(x)$（x 是质数）
- **二元谓词** $Q(x, y)$：描述两个体之间的关系。如 $Love(x, y)$（x 爱 y）、$Greater(x, y)$（$x > y$）
- n **元谓词**：描述 n 个体之间的关系

注意：0 元谓词（不含个体变项的谓词）退化为命题。在这个意义上，**命题逻辑是谓词逻辑的特例**。

2.2.3 量词

(1) 全称量词 $\forall$

$\forall x P(x)$：对个体域中**所有** x，$P(x)$ 成立。

(2) 存在量词 $\exists$

$\exists x P(x)$：个体域中**存在**（至少一个）x，使 $P(x)$ 成立。

2.2.4 特性谓词——极易混淆的点！

在用全称量词时，通常要加一个**特性谓词**来限制讨论范围：

- 全称量词后跟**蕴含**：$\forall x(Student(x) \to Good(x))$ ——" 所有学生都好"
- 存在量词后跟**合取**：$\exists x(Student(x) \wedge Good(x))$ ——" 存在好学生"

为什么全称用 $\to$ 而存在用 $\wedge$？

全称量词 $\forall x(Student(x) \to Good(x))$ 的意思是：对于每个 x，**如果** x 是学生，**那么** x 好。当 x 不是学生时，前件为假，蕴含式自动为真——这很合理，因为我们只关心学生。

但如果用 $\wedge$：$\forall x(Student(x) \wedge Good(x))$ 的意思是**每个** x 既是学生又好——这意味着世界上所有东西都是学生且都好！这显然是荒谬的。

存在量词反过来：$\exists x(Student(x) \wedge Good(x))$ 表示存在一个 x，它既是学生又好——正确。而 $\exists x(Student(x) \to Good(x))$ 等价于 $\exists x(\neg Student(x) \vee Good(x))$，只要存在一个非学生的东西（比如一块石头），这个公式就为真——完全不是我们想表达的意思。

记法：全称 $\to$ 蕴含，存在 $\to$ 合取。这是谓词逻辑符号化的第一铁律。

2.2.5 【重点】符号化例题（必须使用全总个体域）

考试要求：谓词逻辑符号化时**必须用全总个体域**！这意味着你需要引入**特性谓词**来限定讨论范围，而不是改变个体域本身。

例 1（基本符号化——全总个体域）：将以下语句用谓词逻辑符号化（使用全总个体域）。

表 2.1:

原句	符号化	说明
王明是劳动模范	$M(a)$，$M(x)$：x 是劳模，a：王明	个体常项直接用谓词描述
小李是小赵的老师	$T(s,t)$，$T(x,y)$：x 是 y 的老师	二元谓词表示关系
所有人都是要死的	$\forall x(M(x) \to F(x))$，$M(x)$：x 是人	全称 $\to$ 蕴涵，$M(x)$ 为特性谓词
有的人活百岁以上	$\exists x(M(x) \wedge P(x))$，$P(x)$：$x$ 活百岁以上	存在 $\to$ 合取，$M(x)$ 为特性谓词

注意第一条和第二条：如果原句已经指明了具体个体（王明、小李、小赵），直接用个体常项代入谓词即可，**不需要加量词！**

例 2（多个量词嵌套）：" 任何金属都可以溶解在某种液体中。"

符号化（全总个体域）：

- $M(x)$：x 是金属

- $L(y)$：y 是液体
- $D(x,y)$：x 可以溶解在 y 中

$$\forall x(M(x) \to \exists y(L(y) \wedge D(x,y)))$$

口诀：**全称后面跟 $\to$，存在后面跟 $\wedge$；特性谓词放前件，主谓词放后件。**

例 3（复杂自然语言符号化）：”不管白猫黑猫，抓住老鼠就是好猫。”
符号化（全总个体域）：

- $C(x)$：x 是猫
- $W(x)$：x 是白色的
- $B(x)$：x 是黑色的
- $M(y)$：y 是老鼠
- $K(x,y)$：x 抓住 y
- $G(x)$：x 是好猫

$$\forall x\,(C(x) \wedge (W(x) \vee B(x)) \wedge \exists y(M(y) \wedge K(x,y)) \to G(x))$$

拆解思路：”不管白猫黑猫” = 猫且 (白或黑)；”抓住老鼠” = 存在一个老鼠且猫抓住了它；”就是好猫” = 结论 $G(x)$。中间全部用 $\wedge$ 连接后作为前件，$\to$ 连接结论。

例 4（”只有... 才...” 在谓词中的处理）：”只有考试及格，才能拿到学分。”
符号化：设 $P(x)$：x 考试及格，$Q(x)$：x 能拿到学分。注意”只有 A 才 B” $\to B \to A$！

$$\forall x(Q(x) \to P(x))$$

而非 $\forall x(P(x) \to Q(x))$！后者意思是”所有及格的都能拿到学分”——这两句话含义完全不同。

2.3 谓词公式的构造

2.3.1 项（Term）

项的递归定义：

1. 个体常项和个体变项是项
2. 若 f 是 n 元函数，$t_1, \cdots, t_n$ 是项，则 $f(t_1, \cdots, t_n)$ 是项

函数的引入使谓词逻辑的表达力大幅增强。$father(x)$ 是一个函数项，表示”x 的父亲”——一个确定的个体。而 $Father(x,y)$ 是一个谓词，表示”x 是 y 的父亲”——一个可真可假的判断。函数和谓词的区别就在于此。

2.3.2 合式公式（Well-Formed Formula, WFF）

1. 原子公式（谓词 + 项）是合式公式
2. 联结词规则与命题逻辑相同
3. 若 A 是公式，则 $\forall xA$ 和 $\exists xA$ 也是公式

2.3.3 自由变项与约束变项

- **约束变项**：在量词 $\forall x$ 或 $\exists x$ 辖域内的 x
- **自由变项**：不在任何量词辖域内的变项

自由变项和约束变项的区分极其重要。$\forall xP(x,y)$ 中，x 是约束的（被量词绑定），y 是自由的。自由变项的取值会影响公式的真值，而约束变项只是一个”遍历器”。带自由变项的公式不是命题——它没有确定的真值。

闭式：不含任何自由变项的公式。闭式是真正的命题。

2.3.4 换名规则

为避免变量名冲突，可以对约束变项换名：

- $\forall xP(x) \Leftrightarrow \forall yP(y)$
- 但换名不能改变原有的约束关系

2.4 谓词逻辑的等值式

2.4.1 量词否定律（德摩根律的谓词版本）

$$\neg\forall xP(x) \Leftrightarrow \exists x\neg P(x)$$

$$\neg\exists xP(x) \Leftrightarrow \forall x\neg P(x)$$

”不是所有人都聪明”等价于”存在一个人不聪明”。这是对全体陈述的最简洁反驳方式。

2.4.2 量词辖域收缩与扩张等值式（定理 2.2）

这组定理告诉你：当一个公式中既有量词又有联结词时，量词的”作用范围”可以如何调整。记法核心：**看 B 中有没有 x**——没有就可以自由进出。

设 $A(x)$ 含 x 的自由出现，B 不含 x 的自由出现，则：

最重要的两条（考试常考）：$\forall$ 和 $\exists$ 在 $\rightarrow$ 的**左边**时，移出来会**互换**！$\forall xA \rightarrow B \equiv \exists x(A \rightarrow B)$，$\exists xA \rightarrow B \equiv \forall x(A \rightarrow B)$。这也解释了为什么”化前束范式”时经常出现 $\forall$ 变 $\exists$ 的”反直觉”现象。

表 2.2:

情况	等值式	记忆口诀
$\forall$ 与 $\vee$	$\forall x A(x) \vee B \Leftrightarrow \forall x(A(x) \vee B)$	$\forall$ 可以” 吞” 旁边的 B
$\forall$ 与 $\wedge$	$\forall x A(x) \wedge B \Leftrightarrow \forall x(A(x) \wedge B)$	同上
$\exists$ 与 $\vee$	$\exists x A(x) \vee B \Leftrightarrow \exists x(A(x) \vee B)$	$\exists$ 也可以” 吞”
$\exists$ 与 $\wedge$	$\exists x A(x) \wedge B \Leftrightarrow \exists x(A(x) \wedge B)$	同上
$\forall$ 与 $\rightarrow$（左）	$\forall x A(x) \rightarrow B \Leftrightarrow \exists x(A(x) \rightarrow B)$	$\forall$ **变** $\exists$!
$\exists$ 与 $\rightarrow$（左）	$\exists x A(x) \rightarrow B \Leftrightarrow \forall x(A(x) \rightarrow B)$	$\exists$ **变** $\forall$!
B 与 $\rightarrow$（右）	$B \rightarrow \forall x A(x) \Leftrightarrow \forall x(B \rightarrow A(x))$	$\forall$ 不变
B 与 $\rightarrow$（右）	$B \rightarrow \exists x A(x) \Leftrightarrow \exists x(B \rightarrow A(x))$	$\exists$ 不变

2.4.3 量词分配（定理 2.3）

- $\forall x(P(x) \wedge Q(x)) \Leftrightarrow \forall x P(x) \wedge \forall x Q(x)$ ——$\forall$ 对 $\wedge$ 可分配
- $\exists x(P(x) \vee Q(x)) \Leftrightarrow \exists x P(x) \vee \exists x Q(x)$ ——$\exists$ 对 $\vee$ 可分配

但注意！以下两个方向不能分配（高频考点）：

- $\forall x(P(x) \vee Q(x)) \not\Leftrightarrow \forall x P(x) \vee \forall x Q(x)$
- $\exists x(P(x) \wedge Q(x)) \not\Leftrightarrow \exists x P(x) \wedge \exists x Q(x)$

但小心：

- $\forall x(P(x) \vee Q(x)) \not\Leftrightarrow \forall x P(x) \vee \forall x Q(x)$ ——全称对 $\vee$ 不能分配！
- $\exists x(P(x) \wedge Q(x)) \not\Leftrightarrow \exists x P(x) \wedge \exists x Q(x)$ ——存在对 $\wedge$ 不能分配！

” 每个人都有手机或电脑” $\neq$ ” 每个人都有手机或每个人都有电脑”。前者只要求每个人至少有一个设备，后者要求所有人统一使用同一种设备——条件强得多。

2.4.4 量词顺序

关键规则：同种量词可以交换顺序；不同种量词**一般**不可交换。

- $\forall x \forall y P(x, y) \Leftrightarrow \forall y \forall x P(x, y)$
- $\exists x \exists y P(x, y) \Leftrightarrow \exists y \exists x P(x, y)$
- $\forall x \exists y P(x, y) \not\Leftrightarrow \exists y \forall x P(x, y)$

$\forall x \exists y\ Loves(x, y)$：” 每个人都有一个爱的人”——你爱的人可以不同。$\exists y \forall x\ Loves(x, y)$：” 有一个人，所有人都爱 ta”——一个万人迷。前者 $\not\Leftrightarrow$ 后者。这两个公式表达的意思天差地别。

2.5 【重点】2.5 解释（Interpretation）——给公式赋予意义

命题逻辑中，只要给命题变项赋值（0 或 1），公式的真值就确定了。但在谓词逻辑中，公式含有谓词、函数、量词——真值取决于我们如何” 解释” 这些符号。同一个谓词公式在不同解释下可以有完全不同的真值。

2.5.1 什么是解释

谓词逻辑中的一个**解释**（Interpretation）I 由以下四部分组成：

1. **非空个体域** D：讨论对象的全体（必须非空！）
2. **个体常项的指派**：对每个个体常项 a，指定 D 中的一个元素 $\bar{a} \in D$
3. **函数符号的指派**：对每个 n 元函数符号 f，指定一个映射 $\bar{f} : D^n \to D$
4. **谓词符号的指派**：对每个 n 元谓词符号 P，指定一个映射 $\bar{P} : D^n \to \{0, 1\}$（即 D 上的一个 n 元关系）

核心理解：公式本身只是一串符号——它没有" 绝对" 的真值。真值是**相对于解释**而言的。说一个公式是" 真" 的，一定是在某个具体的解释下。

2.5.2 公式在解释下的真值

给定解释 I 后：

- 原子公式 $P(t_1, \cdots, t_n)$ 的真值 = $\bar{P}(\bar{t_1}, \cdots, \bar{t_n})$
- $\forall x A(x)$ 为真 $\iff$ 对 D 中**每一个**元素 d，$A(d)$ 均为真
- $\exists x A(x)$ 为真 $\iff$ 在 D 中**存在**（至少一个）元素 d，使 $A(d)$ 为真
- 联结词的真值规则与命题逻辑完全相同

2.5.3 谓词公式的三种分类（相对于解释）

表 2.3:

类型	定义
逻辑有效式（永真式）	在**任何**解释下均为真
矛盾式（永假式）	在**任何**解释下均为假
可满足式	存在至少一个解释使其为真

注意与命题逻辑的区别：命题逻辑中判断永真式只需验算有限行真值表；谓词逻辑中" 任何解释" 有无穷多种——判断逻辑有效式要困难得多（Church 定理：一阶逻辑的有效性是不可判定的）。

2.5.4 PPT 例题——解释与公式真值判断

例 1（给定解释，求公式真值）：设解释 I 为：$D = \{1, 2\}$，谓词 $P(x)$ 解释为"$x = 1$"（即 $P(1) = 1, P(2) = 0$），判断以下公式在 I 下的真值：

(1) $\forall x P(x)$ → **假**。因为 $P(2) = 0$，并非所有元素都满足 P。

(2) $\exists x P(x)$ → **真**。因为存在 $x = 1$ 使 $P(1) = 1$。

(3) $\forall x(P(x) \vee \neg P(x))$ → **真**。排中律在任何个体上恒真，故全称也为真。

(4) $\exists x(P(x) \wedge \neg P(x))$ → **假**。矛盾式不可能被任何个体满足。

例 2（判断逻辑有效式）：判断 $\forall x F(x) \to \exists x F(x)$ 是否为逻辑有效式。

解：任取解释 I（非空域 D），前件 $\forall x F(x)$ 为真意味着 D 中所有元素都满足 F。由于 D 非空，至少存在一个元素 $d \in D$，$F(d)$ 为真，故后件 $\exists x F(x)$ 为真。因此蕴涵式恒真 → **逻辑有效式**。

但如果允许空域，则前件 $\forall x F(x)$ 空真为真，后件 $\exists x F(x)$ 为假——整个蕴涵式变假。所以在大多数逻辑教材中，规定个体域非空。

例 3（构造反例，证明非逻辑有效式）：证明 $\exists x F(x) \to \forall x F(x)$ 不是逻辑有效式。
解：构造解释 I：$D = \{1, 2\}$，$F(x)$ 解释为"$x = 1$"（即 $F(1) = 1, F(2) = 0$）。
前件 $\exists x F(x)$：存在 $x = 1$ 使 $F(1) = 1$，故前件为**真**。
后件 $\forall x F(x)$：$F(2) = 0$，故后件为**假**。
蕴涵式"真 $\to$ 假" = **假**。
存在一个解释使公式为假 $\to$ 该公式**不是**逻辑有效式。

构造反例的关键：让前件的"存在一个"和后件的"所有"满足不同的个体。

例 4（同一公式在不同解释下的真值）：考虑公式 $\forall x \exists y R(x, y)$。

- 解释 I_1：$D = \mathbb{N}$（自然数），$R(x, y)$ 为"$x \leq y$" $\to$ **真**（对任意自然数，总有比它大的自然数）。
- 解释 I_2：$D = \mathbb{N}$，$R(x, y)$ 为"$x > y$" $\to$ **假**（取 $x = 0$，没有任何 y 使 $0 > y$，因为自然数从 0 开始）。
- 解释 I_3：$D = \{1, 2\}$，R 为 $\{(1, 1), (1, 2), (2, 2)\}$ $\to$ **真**（$x = 1$ 时有 $y = 1$ 或 $y = 2$；$x = 2$ 时有 $y = 2$）。

同一个公式，三种解释三种结果——这说明**公式的真值完全依赖于解释**。

2.6 【重点】2.6 前束范式及运算法则

2.6.1 定义

形如 $Q_1 x_1 Q_2 x_2 \cdots Q_n x_n A$ 的公式称为**前束范式**，其中：

- 每个 Q_i 是 $\forall$ 或 $\exists$
- A 是不含量词的公式（称为**母式**）

前束范式把所有的量词都"提前"到公式的最外层。这和主析取范式一样，是一种标准形——便于分析公式的结构和性质。

2.6.2 化前束范式的步骤

第一步：消去 $\to$ 和 $\leftrightarrow$（用蕴含等值式和等价等值式）
第二步：否定深入（用德摩根律和量词否定律，使 $\neg$ 只出现在原子公式前）
第三步：变量改名（用换名规则避免量词辖域中的变量名冲突——这是最容易出错的步骤）
第四步：量词前移（将所有量词依次提到公式最前面）

致命陷阱：当量词前移时，如果一个量词的辖域既包含约束变项也包含自由变项，必须非常小心。例如，将 $\forall x P(x) \to Q(y)$ 化为前束范式时，结果是 $\exists x(P(x) \to Q(y))$，而不是 $\forall x(P(x) \to Q(y))$。因为 $\forall x P(x) \to Q(y) \equiv \neg\forall x P(x) \vee Q(y) \equiv \exists x \neg P(x) \vee Q(y) \equiv \exists x(\neg P(x) \vee Q(y)) \equiv \exists x(P(x) \to Q(y))$。全称变成了存在！这就是为什么必须严格按照步骤来，不要凭直觉跳步。

例：求 $\exists x F(x,y) \to (H(x) \to \neg\forall y G(y))$ 的前束范式。

解：

第一步（消去蕴涵）：

原式 $\Leftrightarrow \neg\exists x F(x,y) \vee (H(x) \to \neg\forall y G(y))$

$\Leftrightarrow \neg\exists x F(x,y) \vee (\neg H(x) \vee \neg\forall y G(y))$

第二步（否定深入，量词否定转换）：

$\Leftrightarrow \forall x \neg F(x,y) \vee (\neg H(x) \vee \exists y \neg G(y))$

第三步（变量改名——避免 x 和 y 的冲突）：

将 $\exists x$ 改名为 $\exists u$：前面已有 $\forall x$，改用新变量 u

$\Leftrightarrow \forall x \neg F(x,y) \vee (\neg H(x) \vee \exists v \neg G(v))$ （y 也改名 v）

第四步（量词前移——注意：全称 $\forall$ 在析取 $\vee$ 后变为存在 $\exists!$）：

$\Leftrightarrow \forall x \exists v(\neg F(x,y) \vee \neg H(x) \vee \neg G(v))$

$\Leftrightarrow \forall x \exists v(F(x,y) \to (H(x) \to \neg G(v)))$

关键提醒：量词前移时，$\forall$ 如果在 $\vee$ 的左边，移出来会变成 $\exists!$（因为 $\forall x A \vee B \equiv \exists x(A \vee B)$，而非 $\forall x(A \vee B)$。这和量词辖域扩张等值式有关。）

例 2（两变项前束范式）：求 $\forall x P(x) \to \exists y Q(y)$ 的前束范式。

解：

第一步（消去 $\to$）：

原式 $\Leftrightarrow \neg\forall x P(x) \vee \exists y Q(y)$

第二步（量词否定转换）：

$\Leftrightarrow \exists x \neg P(x) \vee \exists y Q(y)$

第三步（变量改名——x 和 y 不同，无冲突，无需改名）

第四步（量词前移——两个 $\exists$ 均可提出）：

$\Leftrightarrow \exists x \exists y(\neg P(x) \vee Q(y))$

最终前束范式：$\boxed{\exists x \exists y(P(x) \to Q(y))}$

注意：本题无变量冲突，步骤简单。关键是第一步用 $\neg\forall x P(x) \equiv \exists x \neg P(x)$ 将全称变为存在。

例 3（否定在前束化中的处理）：求 $\neg\exists x(P(x) \wedge \forall y Q(y))$ 的前束范式。

解：

第一步（无 $\to$ 和 $\leftrightarrow$，跳过）

第二步（否定深入）：

$\neg\exists x(P(x) \wedge \forall y Q(y))$

$\Leftrightarrow \forall x\neg(P(x)\wedge\forall yQ(y))$（量词否定律：$\neg\exists xA\equiv\forall x\neg A$）
$\Leftrightarrow \forall x(\neg P(x)\vee\neg\forall yQ(y))$（德摩根律）
$\Leftrightarrow \forall x(\neg P(x)\vee\exists y\neg Q(y))$（量词否定律：$\neg\forall yQ(y)\equiv\exists y\neg Q(y)$）
第三步（变量改名——x 和 y 不同，无冲突，无需改名）
第四步（量词前移——$\exists y$ 在 $\vee$ 右侧，可直接提出）：
$\Leftrightarrow \forall x\exists y(\neg P(x)\vee\neg Q(y))$
最终前束范式： $\boxed{\forall x\exists y(\neg P(x)\vee\neg Q(y))}$

这个例子展示了”否定深入”的关键作用——从最外层 $\neg$ 一步步向内推进，每一步都精确应用量词否定律和德摩根律。特别注意：$\neg\exists xA\equiv\forall x\neg A$ 和 $\neg\forall xA\equiv\exists x\neg A$，方向不要搞反。

2.7 谓词逻辑推理

谓词逻辑的推理规则在命题逻辑的基础上增加了四条：
(1) 全称例化（UI）：$\forall xP(x)\implies P(c)$（其中 c 是个体域中任意个体）
(2) 全称泛化（UG）：如果 $P(c)$ 对任意 c 成立，则 $\forall xP(x)$
(3) 存在例化（EI）：$\exists xP(x)\implies P(c)$（$c$ 是某个特定个体，需确保 c 是新引入的符号）
(4) 存在泛化（EG）：$P(c)\implies\exists xP(x)$

EI 规则有一个重要的使用限制：引入的 c 必须是一个”全新”的符号，不能和已有的个体符号重名，也不能带有任何额外的假设。如果你在一个证明中多次用 EI，每次都要用不同的新符号。这保证了”存在”仅仅意味着”至少有一个”，而不是”恰好是你上次引入的那个”。

写到这里，笔者觉得有必要说一句：谓词逻辑的推理证明是本课中比较”机械化”的部分——你只需要按部就班地用量词规则消去量词，用命题逻辑推理得到结论，再用量词规则把量词加回去。难的不是单步推导，而是**保持思路清晰**——尤其当量词嵌套、变量名冲突时。建议在草稿纸上明确标注每一步使用了什么规则、对哪个公式操作的，这样复查时不会混乱。

2.8 章末附：逻辑学与计算机科学

学完这部分之后，你可能会问：这些逻辑推理在 CS 中有什么用？举几个例子：

- **程序验证**：用谓词逻辑精确描述前置条件和后置条件，自动证明程序正确性（Hoare 逻辑）
- **数据库查询**：SQL 本质上是谓词逻辑的一种语法糖——`SELECT * FROM students WHERE`

`score > 90` 对应的就是 $\{x \mid Student(x) \land Score(x) > 90\}$ - **类型系统：**函数式编程中的类型推导（如 Hindley-Milner 系统）建立在谓词逻辑的合一算法之上 - **AI 推理：**知识表示和自动定理证明直接依赖于一阶谓词逻辑 - **SAT 求解器：**命题逻辑的可满足性问题是 NP 完全的，现代 SAT 求解器却能高效处理百万级变量——这是逻辑学和算法工程的完美结合

逻辑学不仅是你理解这些技术的基础，更重要的是它训练了一种**精确思考**的能力——把模糊的直觉转化为严格的形式推导。这种能力，无论你将来做算法、做系统还是做 AI，都是最核心的竞争力。

第二部分

集合论与组合分析

第 3 章 集合论基础

笔者按：集合论是整个现代数学的”操作系统”。从幼儿园起我们就知道”一堆东西”叫集合，但朴素直观的集合概念在 20 世纪初引发了罗素悖论等危机，最终催生了公理化集合论。本课讲的是朴素集合论——不做公理化的形式推导，而是建立一套精确的语言来描述集合之间的关系、运算和规模。如果你把这部分和前面的谓词逻辑结合起来看，会发现集合运算本质上就是谓词逻辑的”另一张脸”：$\cap$ 就是 $\wedge$，$\cup$ 就是 $\vee$，补集就是 $\neg$。

3.1 集合的基本概念

3.1.1 什么是集合？

集合就是一些确定事物的整体，且任一事物是否属于该集合是完全确定的——要么属于，要么不属于。构成集合的事物称为**元素**。

”完全确定”是这里最关键的词。高数成绩好的同学 是集合吗？不是——因为”好”没有明确的判定标准。但高数成绩 $\geq$ 线数成绩的同学 是集合——判定规则是精确的。

元素与集合的关系：

- $a \in A$：a 属于 A
- $a \notin A$：a 不属于 A

3.1.2 集合的表示法

(1) 列举法（花名册法）：把元素写在花括号里。

- $A = \{\text{红}, \text{黄}, \text{蓝}\}$
- $B = \{0, 1, 4, 9, 16, 25, \cdots\}$（列出足够多元素以反映规律）

(2) 谓词表示法（集合构造器）：$S = \{x \mid P(x)\}$ ——由满足性质 P 的所有元素组成。

集合构造器 $\{x \mid P(x)\}$ 完美地对应了谓词逻辑中的特性谓词：$x \in S \leftrightarrow P(x)$。这也是为什么这门课把集合预备知识放在逻辑学之后——集合就是逻辑的”外延化”。逻辑关心的是谓词的真假，集合关心的是满足谓词的元素全体。

3.1.3 常见集合

3.1.4 集合元素的三个特性

1. **确定性**：x 是否属于 A 是确定的（不能既属于又不属于）
2. **互异性**：集合中元素互不相同（$\{1, 1, 2\} = \{1, 2\}$）
3. **无序性**：元素之间没有顺序（$\{1, 2\} = \{2, 1\}$）

表 3.1:

符号	含义
$\emptyset$	空集，不含任何元素
$\mathbb{N}$	自然数集 $\{0,1,2,3,\cdots\}$
$\mathbb{Z}$	整数集
$\mathbb{Z}^+$	正整数集 $\{1,2,3,\cdots\}$
$\mathbb{Q}$	有理数集
$\mathbb{R}$	实数集
$\mathbb{C}$	复数集

3.2 集合之间的关系

3.2.1 子集与相等

- **子集**：$A \subseteq B \iff \forall x(x \in A \to x \in B)$
- **真子集**：$A \subset B \iff A \subseteq B \wedge A \neq B$
- **相等**：$A = B \iff A \subseteq B \wedge B \subseteq A$

  证明两集合相等的最标准方法就是**双向包含**——先证 $A \subseteq B$ 再证 $B \subseteq A$。这个方法看似笨拙，但极其可靠，在集合论的证明中反复使用。

- **不包含**：$A \nsubseteq B \iff \exists x(x \in A \wedge x \notin B)$

空集的性质：对任意集合 A，有 $\emptyset \subseteq A$。

为什么空集是任何集合的子集？用逻辑角度理解：$\forall x(x \in \emptyset \to x \in A)$ 的前件 $x \in \emptyset$ 永远为假，蕴含式自动为真。空集是" 什么都不包含"，所以它满足任何子集定义——这是一种**虚真**（vacuous truth）。

3.2.2 基数

有限集 S 中元素的个数称为**基数**，记作 $|S|$。n 元集：$|S| = n$。

3.2.3 幂集【重点】

定义：$\mathcal{P}(A) = \{X \mid X \subseteq A\}$ ——A 的所有子集构成的集合。
核心性质：若 $|A| = n$，则 $|\mathcal{P}(A)| = 2^n$。

为什么是 2^n？对 A 中的每个元素，在构造子集时有两种选择。

PPT 例题——幂集计算（例 1.1.2）：

- $P(\emptyset) = \{\emptyset\}$
- $P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$
- $P(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$

- $P(\{1,\{2,3\}\}) = \{\emptyset, \{1\}, \{\{2,3\}\}, \{1,\{2,3\}\}\}$

幂集还有一个深刻的性质：对于任何集合 A，$|\mathcal{P}(A)| > |A|$（康托尔定理）。这意味着**永远存在比当前集合更大的集合**——不存在”最大”的集合。

例 2——枚举三元集的幂集：设 $A = \{a, b, c\}$，求 $\mathcal{P}(A)$ 并验证 $|\mathcal{P}(A)| = 2^3$。

解：按子集元素个数分类枚举：

表 3.2:

元素个数	子集	个数
0	$\emptyset$	$C(3,0) = 1$
1	$\{a\}, \{b\}, \{c\}$	$C(3,1) = 3$
2	$\{a,b\}, \{a,c\}, \{b,c\}$	$C(3,2) = 3$
3	$\{a,b,c\}$	$C(3,3) = 1$

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$$

验证：$|\mathcal{P}(A)| = 1 + 3 + 3 + 1 = 8 = 2^3$。□

这个枚举揭示了幂集和组合数之间的深层联系：$|\mathcal{P}(A)| = \sum_{k=0}^{n} \binom{n}{k} = 2^n$。二项式定理给出了这个等式的代数证明：$(1+1)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot 1^k \cdot 1^{n-k}$。

例 3——嵌套幂集的基数验证：验证 $|\mathcal{P}(\mathcal{P}(\emptyset))| = 2$ 和 $|\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))| = 4$。

解：

$\mathcal{P}(\emptyset) = \{\emptyset\}$，基数 $1 = 2^0$。

$\mathcal{P}(\mathcal{P}(\emptyset)) = \mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$，基数 $2 = 2^1$。

$\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \mathcal{P}(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$，基数 $4 = 2^2$。

一般地，$|\mathcal{P}^{k+1}(\emptyset)| = 2^{|\mathcal{P}^k(\emptyset)|}$，每取一次幂集，基数按 $0 \to 1 \to 2 \to 4 \to 16 \to 65536 \to \cdots$ 爆炸增长。□

注意区分 $\emptyset$ 和 $\{\emptyset\}$：前者是空集（0 个元素），后者是以空集为唯一元素的集合（1 个元素）。$P(\emptyset) = \{\emptyset\}$ 不是空集——它有一个元素（就是空集本身）。考试中 $P(\emptyset) = \{\emptyset\}$ 是最常考的一个特例。

3.3 集合的基本运算

3.3.1 五种基本运算

从这里可以清晰地看到：**集合运算就是谓词逻辑运算的”集合化”**。并集对应析取——元素只要在 A 或 B 中即可。交集对应合取——元素必须同时在两者中。补集对应否定——元素不能在其中。这个对应关系是理解集合运算律的最佳途径——每一个集合律都可以还原为对应的逻辑等价式。

表 3.3:

运算	定义	逻辑对应
并集	$A \cup B = \{x \mid x \in A \vee x \in B\}$	$\vee$
交集	$A \cap B = \{x \mid x \in A \wedge x \in B\}$	$\wedge$
相对补	$A - B = \{x \mid x \in A \wedge x \notin B\}$	$\wedge\neg$
绝对补	$\overline{A} = E - A$（E 为全集）	$\neg$
对称差	$A \oplus B = (A - B) \cup (B - A)$	XOR

3.3.2 集合运算律

下面的运算律和命题逻辑的等价公式一一对应。把它们并列起来看，就会发现大自然的对称之美：

表 3.4:

名称	集合形式	逻辑对应
幂等律	$A \cup A = A$，$A \cap A = A$	$P \vee P \Leftrightarrow P$
交换律	$A \cup B = B \cup A$	$P \vee Q \Leftrightarrow Q \vee P$
结合律	$(A \cup B) \cup C = A \cup (B \cup C)$	同理
分配律	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$
同一律	$A \cup \emptyset = A$，$A \cap E = A$	$P \vee 0 \Leftrightarrow P$
零律	$A \cup E = E$，$A \cap \emptyset = \emptyset$	$P \vee 1 \Leftrightarrow 1$
互补律	$A \cup \overline{A} = E$，$A \cap \overline{A} = \emptyset$	$P \vee \neg P \Leftrightarrow 1$
吸收律	$A \cup (A \cap B) = A$	$P \vee (P \wedge Q) \Leftrightarrow P$
双重否定	$\overline{\overline{A}} = A$	$\neg\neg P \Leftrightarrow P$

注意：分配律的两个方向在集合论中都成立（$\cup$ 对 $\cap$ 可分配，$\cap$ 对 $\cup$ 也可分配），这和普通代数中 $a + (b \times c) \neq (a + b) \times (a + c)$ 完全不同。集合运算的对称性比数的运算更完美。

3.3.3 德 · 摩根律（De Morgan's Laws）

绝对补集版本：

$$\overline{A \cup B} = \overline{A} \cap \overline{B}, \quad \overline{A \cap B} = \overline{A} \cup \overline{B}$$

相对补集版本：

$$A - (B \cup C) = (A - B) \cap (A - C), \quad A - (B \cap C) = (A - B) \cup (A - C)$$

德摩根律在集合论中有一个非常直观的" 翻译"：不属于并集 = 两者都不属于；不属于交集 = 至少有一个不属于。画个 Venn 图一目了然，但从逻辑等价式的角度推导出来才是最严格的方式。

例：证明 $A - (B \cap C) = (A - B) \cup (A - C)$。
证（双向包含法）：
( ) 任取 $x \in A - (B \cap C)$，则 $x \in A$ 且 $x \notin B \cap C$。

- $x \notin B \cap C$ 意味着 $\neg(x \in B \wedge x \in C) \equiv x \notin B \vee x \notin C$
- 若 $x \notin B$，则 $x \in A - B$；若 $x \notin C$，则 $x \in A - C$
- 无论哪种情况，$x \in (A - B) \cup (A - C)$

( ) 任取 $x \in (A - B) \cup (A - C)$。

- 若 $x \in A - B$，则 $x \in A$ 且 $x \notin B$，从而 $x \notin B \cap C$，故 $x \in A - (B \cap C)$
- 若 $x \in A - C$，同理可得 $x \in A - (B \cap C)$

综上，$A - (B \cap C) = (A - B) \cup (A - C)$。□

注：这实际上是命题逻辑中 $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$（德摩根律）的集合版本。把集合语言翻译成逻辑语言：$x \notin B \cap C \iff \neg(x \in B \wedge x \in C) \iff x \notin B \vee x \notin C$。集合论的每一道证明题，本质上都是在练习谓词逻辑推理。

3.3.4 对称差的性质

对称差 $A \oplus B$ 是集合论中的"XOR 运算"——属于 A 或 B 但不同时属于两者。

基本性质：

- $A \oplus A = \emptyset$（自己和自己差，什么都没剩下）
- $A \oplus \emptyset = A$（和空集差还是自己）
- $A \oplus E = \overline{A}$（和全集差就是补集）
- $A \oplus B = B \oplus A$（交换律成立）
- $(A \oplus B) \oplus C = A \oplus (B \oplus C)$（结合律成立！证明时推荐用特征函数法）

结合律的成立意味着 $\oplus$ 构成了集合上的一个群运算——集合在对称差下构成一个 Abel 群（零元是 $\emptyset$，每个元素的逆元就是它自己，因为 $A \oplus A = \emptyset$）。

- $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$（$\cap$ 对 $\oplus$ 的分配律）
- $A \oplus B = A \oplus C \Rightarrow B = C$（消去律）

3.4 容斥原理【重点】

容斥原理是计数问题中的核心工具。它的基本思想是：在计数并集时，直接加会重复计入交集部分，所以需要减回去；但减多了又需要加回来……如此交替。

3.4.1 两个集合的简单情况

$$|A \cup B| = |A| + |B| - |A \cap B|$$

3.4.2 一般形式

设 A_i 是 S 中具有性质 P_i 的元素构成的子集：

至少具有一条性质的元素个数：

$$|A_1 \cup A_2 \cup \cdots \cup A_m| = \sum |A_i| - \sum_{i<j} |A_i \cap A_j| + \cdots + (-1)^{m-1} |A_1 \cap \cdots \cap A_m|$$

不具有任何性质的元素个数（从总数中排除）：

$$|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_m}| = |S| - \sum |A_i| + \sum_{i<j} |A_i \cap A_j| - \cdots + (-1)^m |A_1 \cap \cdots \cap A_m|$$

PPT 例题——容斥原理经典题（例 3.3.1）：求 1 到 1000 中不能被 5、6、8 中任何一个整除的整数个数。

设 A, B, C 分别为能被 5、6、8 整除的集合。$|S| = 1000$。

- $|A| = 200, |B| = 166, |C| = 125$
- $|A \cap B| = 33$（被 30 整除）, $|A \cap C| = 25$（被 40 整除）, $|B \cap C| = 41$（被 24 整除）
- $|A \cap B \cap C| = 8$（被 120 整除）

故 $|\overline{A} \cap \overline{B} \cap \overline{C}| = 1000 - (200 + 166 + 125) + (33 + 25 + 41) - 8 = \boxed{600}$。

> 容斥原理的" 加减交替" 模式来源于二项式定理——$(1-1)^m = \sum_{k=0}^{m} (-1)^k \binom{m}{k} = 0$。当 m 很大时手工计算不现实，但在 $m = 2$ 或 $m = 3$ 时非常实用。考试基本集中在 $m = 2$ 或 $m = 3$ 的情况。

例：某班 24 人，13 人会英语，10 人会德语，9 人会法语，5 人会日语。已知：4 人既会英语又会法语，4 人既会英语又会德语，4 人既会德语又会法语，3 人既会日语又会英语。会日语的人不会法语和德语。问：有多少人会三门语言（英、德、法）?

解：

设 A：会英语，B：会德语，C：会法语，D：会日语。

分析日语（D）的特殊性：由于会日语的人不会法语和德语，所以日语只可能与英语有交集。从总人数去掉日语的" 纯增量"：

- 5 人会日语，其中 3 人也只会英语而不涉及德和法
- 其余 $24 - (5 - 3) = 22$ 人不涉及日语，构成一个标准的三集容斥问题

对 A, B, C 三集合应用容斥原理：

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

$$22 = 13 + 10 + 9 - 4 - 4 - 4 + x$$

$$22 = 20 + x \quad \Rightarrow \quad x = 2$$

故：**2 人会三门语言（英、德、法）**。

技巧总结：遇到特殊约束时先隔离，再用标准容斥。

PPT 例题——欧拉函数（例 3.3.3）：$\varphi(n)$ 表示 1 到 n 中与 n 互质的数的个数。若 $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$，则 $\varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k})$。

例：$\varphi(12) = 12 \times \frac{1}{2} \times \frac{2}{3} = 4$（1,5,7,11 与 12 互质）。$\varphi(60) = 60 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 16$。这比直接在 4 集合上做容斥更简洁且不易出错。

第 4 章 组合分析初步【不考】

组合分析回答的是一个朴素的问题：**有多少种**？从密码的排列数到算法的复杂度分析，从统计组合数到信息论中的编码数——计数问题遍布 CS 的每一个角落。而所有复杂计数的根基，就是下面几个最简单的法则和公式。

4.1 加法法则与乘法法则【不考】

组合计数的两个” 元法则”：

加法法则：事件 A 有 p 种方式，事件 B 有 q 种方式，且二者**互斥**（不能同时发生），则”A 或 B” 有 $p+q$ 种方式。

乘法法则：事件 A 有 p 种方式，事件 B 有 q 种方式，且二者**独立**（B 的选择不依赖于 A 的选择），则”A 且 B” 有 $p\cdot q$ 种方式。

这两个法则简单到几乎不值一提——但 90

PPT 例题——加法/乘法法则（例 4.1.1）：从 1,2,3,4,5 中选数字构成 3 位数：

- (1) 各位不同：$5\times4\times3=60$
- (2) 偶数：个位为 2 或 4（2 种），$2\times5\times5=50$
- (3) 被 5 整除：个位必为 5，$1\times5\times5=25$
- (4) 大于 300：百位为 3,4,5（3 种），$3\times5\times5=75$

PPT 例题——排列（例 4.2.1-4.2.2）：

- 5 天安排 3 门考试（每天最多一门）：$P(5,3)=60$；不限制：$5^3=125$
- 10 男 5 女站一排，女生互不相邻：男生先排 10!，11 个空隙选 5 个放女生 $P(11,5)$，共 $10!\times P(11,5)$
- 圆排列版本：$(10-1)!\times P(10,5)$（男生先围圈）

PPT 例题——组合（例 4.2.3-4.2.4）：

- 25 个点（无三点共线）可连 $C(25,2)=300$ 条直线，$C(25,3)=2300$ 个三角形
- 1 300 中选 3 个数使和为 3 的倍数：按 mod 3 分三类各 100 个，同组取 3 个 $3\times C(100,3)$ + 每组各取 1 个 100^3 = **1,485,100**

PPT 例题——多重集（例 4.2.7-4.2.8）：

- r 个相同球放入 n 个不同盒子：$C(n+r-1,r)$（隔板法）
- 5 天共学 15 小时，每天至少 1 小时：先每天给 1 小时，剩 10 小时自由分配 $\to C(10+5-1,10)=C(14,4)$ 关键是判断：两个子任务的关系是” 或”（加法）还是” 且”（乘法），是” 互斥” 还是” 独立”。

4.2 排列与组合【不考】

排列和组合的核心区别只有两个字：**顺序**。有序是排列，无序是组合。把这两个概念区分清楚，整个组合分析就入门了。

4.2.1 排列（有序选取）

从 n 个不同元素中选 r 个并**按顺序排列**的方式数：

$$P_n^r = P(n,r) = \frac{n!}{(n-r)!} = n \cdot (n-1) \cdot (n-2) \cdots (n-r+1)$$

直观推导：第一个位置有 n 种选择，第二个有 $n-1$ 种，……第 r 个有 $n-r+1$ 种。由乘法法则得乘积。

当 $r = n$ 时即为**全排列**：$P_n^n = n!$

4.2.2 环排列

n 个元素排成一圈，旋转重合视为相同。环排列数：$(n-1)!$

为什么是 $(n-1)!$ 而不是 $n!/n$？因为圆排列中，所有 n 个旋转等价（同一圆排列可以旋转 n 次得到 n 个不同的线排列）。但这里有个微妙之处：如果环还可以翻转（手镯排列而不是圆桌排列），那还要再除以 2——翻转对称意味着 $n!/2n = (n-1)!/2$。考试时看清楚题意是否允许翻转。

4.2.3 组合（无序选取）

从 n 个不同元素中选 r 个（**不考虑顺序**）的方式数：

$$C_n^r = C(n,r) = \binom{n}{r} = \frac{n!}{r!(n-r)!} = \frac{P_n^r}{r!}$$

$\binom{n}{r} = \frac{P_n^r}{r!}$ 的解释：先从 n 个元素中有序选出 r 个（P_n^r 种），但因为组合不关心顺序，每个 r 元子集被重复计数了 $r!$ 次（r 个元素的所有排列）。除以 $r!$ 即可。

组合的核心性质：

- $\binom{n}{r} = \binom{n}{n-r}$ ——选哪些进去 = 选哪些出去。对称美。
- $\sum_{r=0}^{n} \binom{n}{r} = 2^n$ ——n 元集的子集总数（这就是幂集大小为 2^n 的组合证明）
- $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$ ——帕斯卡恒等式（杨辉三角的递推基础）

帕斯卡恒等式的直观理解：从 n 个元素中选 r 个，分两种情况——选入第一个元素（则需要从剩余 $n-1$ 个中选 $r-1$ 个），或者不选第一个元素（则需要从剩余 $n-1$ 个中选 r 个）。

4.3 多重集的排列与组合【不考】

经典排列组合假设”每个元素至多取一次”。但在实际问题中，元素经常可以重复选取——比如密码的每个位置可以选重复的数字，货架上同一种商品可以拿多个。多重集就是为这类情景设计的工具。

4.3.1 多重集的排列

无限重复：多重集 $S = \{\infty \cdot a_1, \infty \cdot a_2, \cdots, \infty \cdot a_k\}$ 的 r 排列数为：

$$k^r$$

每个位置独立地从 k 种中选，r 个位置共 k^r 种。100 个字符的密码（允许重复），每位 26 个字母 +10 个数字 = 36^{100} 种。这就是为什么密码要长——指数增长是暴力的。

有限重复（元素有重复次数限制）：
设 $S = \{n_1 \cdot a_1, n_2 \cdot a_2, \cdots, n_k \cdot a_k\}$，$n = n_1 + n_2 + \cdots + n_k$，则 S 的全排列数为：

$$\frac{n!}{n_1!\, n_2! \cdots n_k!}$$

这是组合数学中最重要的公式之一。它的直观理解：先把所有 n 个元素当做不同的（有 $n!$ 种排列），但 n_1 个 a_1 是一模一样的——它们之间的 $n_1!$ 种排列不用区分，所以要除以 $n_1!$。以此类推。

一个经典应用：单词”MISSISSIPPI” 的字母重排数 = $\frac{11!}{4!4!2!1!}$（4 个 I，4 个 S，2 个 P，1 个 M）。

4.3.2 多重集的组合

无限重复：$S = \{\infty \cdot a_1, \infty \cdot a_2, \cdots, \infty \cdot a_k\}$ 的 r 组合数为：

$$\binom{k+r-1}{r}$$

这个公式的推导极其巧妙——用**隔板法**。你有 r 个球要分到 k 个盒子里（允许空盒）。想象 r 个球排成一行，插入 $k-1$ 个隔板来分隔不同盒子。总共 $r+k-1$ 个位置，选 r 个放球（或选 $k-1$ 个放隔板）：$\binom{r+k-1}{r} = \binom{r+k-1}{k-1}$。

若要求每个元素至少取一个（$r \geq k$）：
先给每个盒子放一个球（保证非空），剩下 $r-k$ 个球自由分配：

$$\binom{r-1}{k-1}$$

4.4 递推方程【不考】

递推是算法分析的灵魂。许多经典算法的时间复杂度分析最终都归结为求解递推方程。本课只介绍几个经典案例，但思维方法适用范围远不止于此。

4.4.1 Hanoi 塔问题

传说中世界末日的预言：64 个盘子从 A 柱移到 C 柱，每次只能移一个，大盘不能压小盘。

$$T(n) = 2T(n-1) + 1, \quad T(1) = 1$$

求解得：$T(n) = 2^n - 1$

64 个盘子需要 $2^{64} - 1 \approx 1.8 \times 10^{19}$ 步，约 5800 亿年。

PPT 例题——汉诺塔推导（例 4.3.1）：
递推：$T(n) = 2T(n-1) + 1, T(1) = 1$
迭代求解：$T(n) = 2^n - 1$（数学归纳法可验证）

4.4.2 二分归并排序

$$W(n) = 2W(n/2) + n - 1, \quad W(1) = 0$$

求解得：$W(n) = n\log_2 n - n + 1 = O(n \log n)$

这是分治算法的经典复杂度。$n \log n$ 是基于比较的排序算法的理论下界——你不可能比这更优太多。

4.4.3 分治算法的一般递推

$$T(n) = a \cdot T(n/b) + d(n), \quad T(1) = 1$$

主定理（简化版）：

表 4.1:

$d(n)$	条件	$T(n)$
常数 c	$a = 1$	$O(\log n)$
常数 c	$a > 1$	$O(n^{\log_b a})$
cn	$a < b$	$O(n)$
cn	$a = b$	$O(n \log n)$
cn	$a > b$	$O(n^{\log_b a})$

主定理的本质是**比较分与合的工作量**。a 是子问题数量，n/b 是子问题规模，$d(n)$ 是合并成本。当合的工作量主导时（$a < b$），总复杂度就是合的量级；当分的工作量主导时（$a > b$），总复杂度由子问题数量决定；两者平衡时（$a = b$），多出一个 $\log n$ 因子。

第 5 章 可数集、不可数集与 Cantor 集

这是集合论中最颠覆直觉的部分。你会看到：有些无穷比另一些无穷” 更大”。整数有无穷多个，实数也有无穷多个——但康托尔证明了实数的无穷比整数的无穷大得多。这彻底改变了数学家对” 无穷” 的理解。

5.1 势——衡量无穷的” 大小” 【重点】

5.1.1 映射类型复习

- **单射**：不同原像映射到不同像（$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$）
- **满射**：像集等于整个目标集合（$f(A) = B$）
- **双射**：既单又满——一一对应

5.1.2 对等与势

若存在 A 到 B 的**双射**，则称 A 与 B **对等**，记作 $A \sim B$。

- 对等是一种**等价关系**（自反、对称、传递）
- 对等的集合具有相同的**势**（基数），记作 $\overline{\overline{A}}$

势是” 元素个数” 这个概念在无穷集上的推广。对于有限集，势就是元素个数；对于无穷集，势衡量的是无穷的” 层次”。

5.2 可数集——” 最小的” 无穷【重点】

定义：与正整数集 $\mathbb{Z}^+$ 对等的集合称为**可数集**（或称可列集），其势记为 $\aleph_0$（阿列夫零）。

通俗地说，可数集就是” 可以一个一个列出来” 的集合——虽然有无穷多个元素，但你可以把它们排成一列，给定任意一个元素，你能说出它是第几个。

可数集的关键性质：

1. **任意无限集都包含一个可数子集**。这是选择公理的等价形式之一。
1. **可数集的子集要么有限，要么可数**。可数的” 子子孙孙” 不会出现第三种无穷。
1. **可数个可数集的并集仍是可数集**（Cantor 对角线法）。这意味着：

- $\mathbb{Z}$ 是可数集（正负整数交替排列：$0, 1, -1, 2, -2, \cdots$）
- $\mathbb{Q}$ 是可数集（将分数按分子 + 分母之和排列）

$\mathbb{Q}$ 是可数集这一事实非常反直觉——有理数在实数线上是稠密的（任意两个实数之间都有有理数），但有理数的”数量”竟然和整数一样多！这说明无穷集合的”大小”和我们直觉中的”密度”是完全不同的概念。

1. **部分可以和整体对等**——这是无穷集区别于有限集的最根本特征。例如，正偶数集 $\{2,4,6,\cdots\}$ 和全体正整数 $\{1,2,3,\cdots\}$ 对等（映射：$n \mapsto 2n$），尽管前者是后者的真子集。

   伽利略注意到平方数和正整数一样多，但放弃了。直到康托尔才有了精确语言。

PPT 例题——可数集证明（例 5.1.3-5.1.4）：

- 平面上整数格点集可数：固定 n，$A_n = \{(n,m) \mid m \in \mathbb{Z}\}$ 可数，所有 A_n 的可数并仍可数
- $\mathbb{Q}$ 可数：将既约分数 p/q 映到格点 (p,q)，这是单射到可数集，故 $\mathbb{Q}$ 至多可数；又 $\mathbb{Q}$ 无穷，故可数

PPT 例题——不可数集证明（定理 5.4）：

$[0,1]$ 不可数的康托尔闭区间套证法：假设 $[0,1]$ 可数 $\{a_1,a_2,\cdots\}$。三等分 $[0,1]$，至少有一个闭子区间不含 a_1，记为 I_1；三等分 I_1，有一个不含 a_2……得闭区间套 $I_1 \supset I_2 \supset \cdots$，$|I_n| = 1/3^n \to 0$。由闭区间套定理，存在 $\xi \in \bigcap I_n$，但 $a_n \notin I_n$ 对所有 n 成立，故 ξ 不在序列中，矛盾！

这个证明是康托尔对角线法的几何版本——和大一高数学的闭区间套定理完美结合。

例：试建立 $[0,1]$ 与 $(-2,3)$ 之间的一一对应。

分析：两个区间都是不可数集（势为 $\aleph$），由伯恩斯坦定理知它们等势。但本题要求**显式构造**双射。

解（分段构造法）：

核心思路：用线性映射处理”大多数”实数（无理数），用数列移位处理可数的有理端点。

令 $S = \{0, 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \cdots\}$（0、1 和所有 $\frac{1}{n}$ 构成的可数集）

定义 $f : [0,1] \to (-2,3)$：

$$f(x) = \begin{cases} 5x - 2, & x \notin S\text{（无理数和大多数有理数用线性映射）} \\ -2, & x = 0 \\ 3, & x = 1 \\ \frac{5}{n} - 2, & \end{cases}$$

验证要点：- $x \notin S$ 时：线性映射 $y = 5x - 2$ 把 $[0,1]$ 映到 $[-2,3]$，去掉 S 中可数个点后，端点问题通过 S 的特殊处理解决 - S 中的点被”移位”以腾出端点 -2 和 3 的位置 - 该映射是双射（可逆），故 $[0,1] \sim (-2,3)$

这种”线性映射 + 可数集移位”的技术是证明区间等势的经典手法。关键洞察：**可数集足够小**，可以用移位来处理边界问题而不影响总体的势。

例 2——两端均为无理数的闭区间 $\sim [0,1]$：试建立 $[\sqrt{2},\sqrt{3}]$ 与 $[0,1]$ 之间的一一对应。

分析：区间端点 $\sqrt{2}$ 和 $\sqrt{3}$ 都是无理数。题目要求显式构造双射。

解（两段构造法）：

第一步：线性映射。令 $g(x) = \frac{x-\sqrt{2}}{\sqrt{3}-\sqrt{2}}$，则 g 将 $[\sqrt{2},\sqrt{3}]$ 双射到 $[0,1]$。

$$g(\sqrt{2})=0,\quad g(\sqrt{3})=1,\quad g\text{ 在无理点上仍是双射}$$

验证：g 是严格单调递增的线性函数，其逆为 $g^{-1}(y)=\sqrt{2}+(\sqrt{3}-\sqrt{2})y$，定义在整个 $[0,1]$ 上。
第二步：结论。g 已经是 $[\sqrt{2},\sqrt{3}]\to[0,1]$ 的双射，无需额外处理。

关键对比：当区间端点是无理数时，线性映射直接给出双射——因为无理数不在我们用于” 移位” 的可数集中被重复使用。这和有理端点的情况（需要” 线性映射 + 可数集移位” 两步处理）形成对比。但考试中也可能出现端点一有理一无理的情况，此时仍需要移位技术。

例 3——无理端点的开区间与闭区间对等：试建立 $(0,\sqrt{2})$ 与 $[0,\sqrt{2}]$ 之间的一一对应。
分析：左端点 0 是有理数，右端点 $\sqrt{2}$ 是无理数。目标是让开区间” 补上” 两个边界点。
解（可数子集移位法）：
令 $A=\{\frac{\sqrt{2}}{n}\mid n\in\mathbb{Z}^+\}\cup\{0\}=\{0,\sqrt{2},\frac{\sqrt{2}}{2},\frac{\sqrt{2}}{3},\frac{\sqrt{2}}{4},\cdots\}$（所有 $\frac{\sqrt{2}}{n}$ 和 0 构成的可数集）。
其中 $0\notin(0,\sqrt{2})$（需补入），$\sqrt{2}\notin(0,\sqrt{2})$（需补入），而 $\frac{\sqrt{2}}{n}\in(0,\sqrt{2})$ 对所有 $n\geq 2$ 成立。
定义 $f:[0,\sqrt{2}]\to(0,\sqrt{2})$：

$$f(x)=\begin{cases}\frac{\sqrt{2}}{2}, & x=0\\ \frac{\sqrt{2}}{3}, & x=\sqrt{2}\\ \frac{\sqrt{2}}{n+2}, & x=\frac{\sqrt{2}}{n},\ n\geq 1\\ x, & \end{cases}$$

技巧说明：$A\cap[0,\sqrt{2}]$ 的序列为 $0,\sqrt{2},\frac{\sqrt{2}}{2},\frac{\sqrt{2}}{3},\frac{\sqrt{2}}{4},\cdots$。其中 0 和 $\sqrt{2}$ 不在 $(0,\sqrt{2})$ 内，其余都在。让 $0\mapsto\frac{\sqrt{2}}{2}$，$\sqrt{2}\mapsto\frac{\sqrt{2}}{3}$，$\frac{\sqrt{2}}{n}\mapsto\frac{\sqrt{2}}{n+2}$（$n\geq 1$），其余点不动。这就把序列” 往后挤了两个位置”，腾出空间让 0 和 $\sqrt{2}$ 的像落入 $(0,\sqrt{2})$ 中。

核心思想：无论区间端点是有理数还是无理数，处理手法完全一致——识别一个包含端点（如果端点不在目标区间内）的可数子集，做序列移位，其余点线性映射（或恒等映射）。有理/无理的区别只在于：线性映射的系数是整数/分数还是带根号的表达式——构造逻辑不变。

5.3 不可数集——更” 大” 的无穷【重点】

5.3.1 康托尔对角线法

定理：区间 $[0,1]$ 中的点构成**不可数集**。
证明思路（对角线法）：
假设 $[0,1]$ 中的所有实数可以排成一列 $x_1,x_2,x_3,\cdots$。把每个实数写成无穷小数形式：

$$x_1=0.a_{11}a_{12}a_{13}\cdots$$

$$x_2 = 0.a_{21}a_{22}a_{23}\cdots$$

$$x_3 = 0.a_{31}a_{32}a_{33}\cdots$$

现在构造一个新实数 $y = 0.b_1b_2b_3\cdots$，其中 $b_i \neq a_{ii}$（比如如果 $a_{ii} = 5$ 则 $b_i = 6$，否则 $b_i = 5$）。那么 y 不在上述列表的任何一行中——因为它与第 i 个数在第 i 位不同。但这与” 列出了所有实数” 矛盾。所以 $[0, 1]$ 不可数。

> 对角线法的精妙之处在于：你不需要” 找” 一个漏掉的数，你只需要**构造**一个必然漏掉的数。这是一种构造性的反证法，和图灵停机问题的证明在精神上一脉相承——实际上，哥德尔不完备定理和图灵机停机问题的证明都受到了康托尔对角线法的启发。

5.3.2 连续统的势

实数集 $\mathbb{R}$ 的势记为 $\aleph$（阿列夫），也称为**连续统的势**。

- 无理数集的势也是 $\aleph$（虽然有理数可数，但” 实数 = 有理数 + 无理数”，去掉可数多的有理数，剩下的无理数仍然是不可数的）
- $[0, 1]$ 的势 = $\mathbb{R}$ 的势 = $\aleph$（存在双射，如 tan 函数将 $(0, 1)$ 映射到 $\mathbb{R}$）

5.3.3 伯恩斯坦定理

若 $A \sim B_0 \subseteq B$ 且 $B \sim A_0 \subseteq A$，则 $A \sim B$。

> 伯恩斯坦定理提供了一个” 非构造性” 的等势证明方法——你不需要显式写出双射，只需证明双方都能单射到对方中。这在处理复杂的无穷集时非常方便。在集合论中，伯恩斯坦定理等价于” 势的偏序是反对称的”。

5.3.4 康托尔定理

定理：对任意非空集合 A，$|\mathcal{P}(A)| > |A|$。即**幂集的势严格大于原集合的势**。

证明思路（又是对角线法）：

假设存在 A 到 $\mathcal{P}(A)$ 的双射 f。考虑集合 $B = \{x \in A \mid x \notin f(x)\}$。由于 f 是满射，存在 $y \in A$ 使 $f(y) = B$。那么 $y \in B$ 吗？

- 若 $y \in B$，则由 B 的定义，$y \notin f(y) = B$，矛盾。
- 若 $y \notin B$，则 $y \notin f(y)$，由 B 的定义，$y \in B$，矛盾。

因此这样的双射不可能存在。

> 这个证明和罗素悖论（” 所有不包含自身的集合的集合”）的结构完全一样——都是某种自指构造导致的矛盾。事实上，康托尔定理可以看作是罗素悖论的” 正面” 版本：罗素悖论显示了朴素集合论的矛盾，而康托尔定理将这个矛盾转化为了一个关于势的正面结论。

5.3.5 连续统假设

在 $\aleph_0$（可数无穷）与 $\aleph$（连续统）之间，是否存在其他势？

连续统假设断言：**不存在**。即 $\aleph$ 是 $\aleph_0$ 之后的” 下一个” 势。

哥德尔（1940 年）证明了连续统假设与 ZFC 公理系统不矛盾（不能被证伪）。科恩（1963 年）证明了连续统假设独立于 ZFC（不能被证明）。这意味着：在标准的集合论公理体系下，连续统假设**既不能被证明也不能被证伪**——它是一个不可判定的命题。你可以把它当作” 真”，得到一种集合论；也可以当作” 假”，得到另一种集合论。这是数学基础中最深刻的发现之一——连” 有多少个无穷” 这个问题都没有唯一答案。

5.4 Cantor 集——不可数但” 长度为 0” 【不考】

5.4.1 构造方法

从区间 $[0,1]$ 开始：

1. 三等分，去掉中间的开区间 $(\frac{1}{3},\frac{2}{3})$
2. 对剩下的两个闭区间 $[0,\frac{1}{3}]$ 和 $[\frac{2}{3},1]$ 各自重复此操作
3. 无限次迭代后，剩下的点集就是 **Cantor 集**

5.4.2 Cantor 集的反直觉性质

表 5.1:

性质	含义
闭集	每次去掉的是开区间，剩下的闭区间取交集仍是闭集
没有内点	任何一点附近都有被挖掉的部分——Cantor 集” 处处是洞”
测度为 0	挖掉的总长度 $= 1/3 + 2/9 + 4/27 + \cdots = 1$，所以” 长度” 为零
不可数	势为 $\aleph$，和整个 $[0,1]$ 等势！
自相似	任意小的一段放大后，结构和大尺度完全一样（分形）

长度为 0 但不可数——这是 Cantor 集最令人震撼的性质。你挖掉了几何意义下的” 几乎所有东西”（总长度 1，什么都没剩下），但从集合论角度看，剩下的事物的” 个数” 和原来一样多！这说明**测度**和**势**是完全独立的概念——一个大势的集合可以有零测度，一个正测度的集合也可以有零势的子集。

Cantor 集还是一类最重要的**分形**——它是最早被发现的严格定义的分形结构。在计算机图形学、信号处理和多分辨率分析中都有直接应用。

为什么 Cantor 集的势是 $\aleph$？

Cantor 集中的每个点可以唯一地用一个无穷三进制小数表示，其中每一位只取 0 或 2（因为每次三等分去掉中间那段，留下的两端对应 0 和 2）。于是 Cantor 集与 $\{0,2\}^{\mathbb{N}}$（所有 0-2 无穷序列）之间存

在一一对应。而 $\{0,2\}^{\mathbb{N}}$ 的势恰好是 $2^{\aleph_0}=\aleph$（与 $[0,1]$ 的二进制表示同理）。这就是为什么 Cantor 集” 长度为零但不可数”——它只有 $[0,1]$ 中三进制展开不含 1 的那些点，但这样的点仍然和整个 $[0,1]$ 一样多。

推广：如果不是三等分？

如果我们每次挖掉的不一定是 $\frac{1}{3}$，而是比例 α（$0<\alpha<1$），则：

- **测度**：挖掉的总长度 = $\alpha+(1-\alpha)\alpha+(1-\alpha)^2\alpha+\cdots=1$（只要每次都按相同比例挖）。但如果比例逐层变化（如第一层挖 α_1，第二层挖 α_2……），总长度 = $\alpha_1+(1-\alpha_1)\alpha_2+\cdots$，可能小于 1。此时可以构造出测度大于 0 的 Cantor 型集——称为**胖康托集**。
- **势**：只要每次至少保留两个闭区间（即不把所有子区间都挖光），总可以用某种进制编码剩余的点，证明势仍为 $\aleph$。关键在于：每一步至少有两个选择（左或右），所以本质上是 $2^{\aleph_0}$ 的结构。
- **关键结论**：测度和势是**独立**的——你可以构造出测度任意大（甚至接近 1）但仍不可数的 Cantor 型集；也可以构造出测度为 0 的不可数集（经典 Cantor 集）。

这个推广告诉我们：**势 $\aleph$ 只依赖于” 每一步至少有两个选择” 这个组合事实，与挖掉多少长度无关**。这就是为什么” 看起来几乎什么都没剩” 的经典 Cantor 集，在集合论意义上仍然和整个 $[0,1]$ 一样大。

学完这部分，如果你觉得” 无穷” 这个概念变得既清晰又模糊了——恭喜你，这就是集合论带给人的典型感受。康托尔说：” 我看到了它，但我简直无法相信它。” 人类花了上千年才学会精确地谈论无穷，而康托尔的对角线法不过一百多年历史。无穷的层次、不可判定性、分形结构——这些概念至今仍在挑战人类直觉的边界。而这，正是数学最迷人的地方。

第三部分

图论

第 6 章 图的基本概念

图论是离散数学中最直观、也最”看得见”的分支。它用点和线来描述事物之间的二元关系——社交网络、电路连接、交通路线、依赖关系……莫不如此。本章从最基本的定义出发，逐步建立图的精确语言。欧拉在 1736 年解决哥尼斯堡七桥问题时创立了图论，距今已近三百年。

6.1 无向图与有向图

6.1.1 无向图

无向图 G 是一个二元组 $G = (V, E)$，其中：

1. 顶点集 V 是非空有穷集合，其元素称为**顶点**（或节点）。
2. 边集 E 为 $V \times V$ 的多重子集，其元素称为**无向边**，简称边。

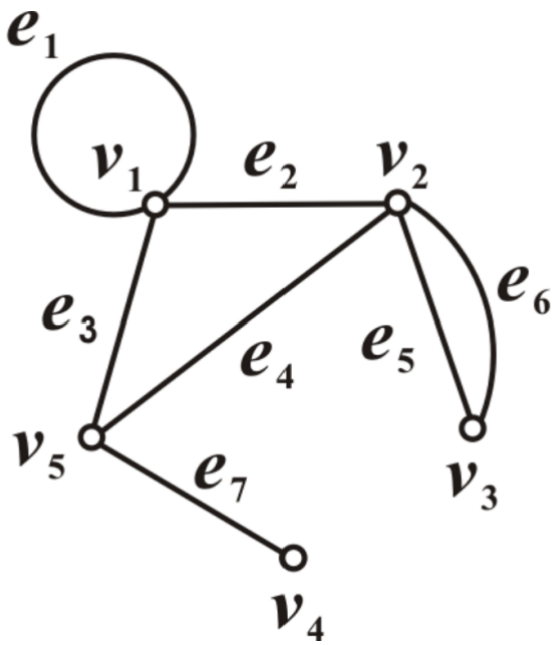


图 6.1: 无向图示例

6.1.2 有向图

有向图 D 是一个二元组 $D = (V, E)$，其中：

1. 顶点集 V 是非空有穷集合。
2. 边集 E 为卡氏积 $V \times V$ 的多重子集，其元素称为**有向边**。
3. D 的**基图**：用无向边代替有向边得到的无向图。

记号约定：G 常表示无向图，D 表示有向图；G 也可泛指无向或有向图。

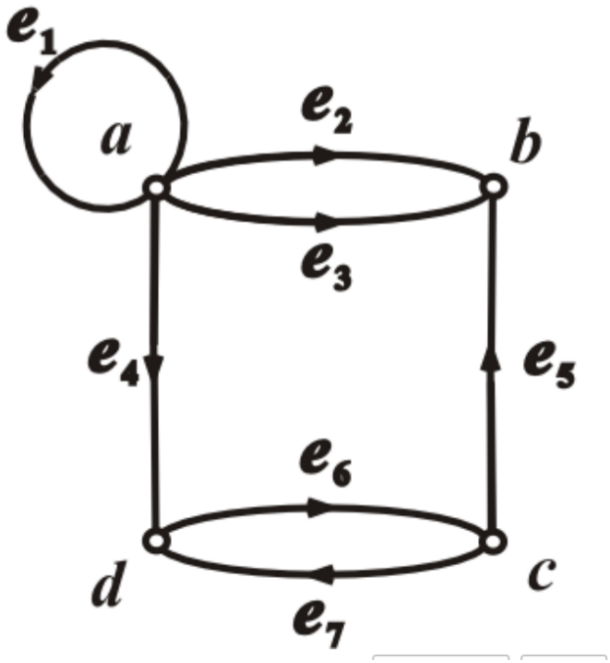


图 6.2: 有向图示例

基本术语：

- n **阶图**：n 个顶点的图
- **零图**：$E = \emptyset$（无边）
- **平凡图**：1 阶零图
- **空图**：$V = \emptyset$

6.1.3 顶点和边的关联

设 $e = (v_i, v_j)$ 是无向图 G 的一条边：

- 称 v_i, v_j 为 e 的**端点**，e 与 v_i, v_j **关联**
- 若 $v_i \neq v_j$，e 与 v_i, v_j 的**关联次数**为 1
- 若 $v_i = v_j$，e 为**环**，关联次数为 2
- 与边无关联的顶点称为**孤立点**

设有向边 $e = (v_i, v_j)$（v_i 为**始点**，v_j 为**终点**），同样称 e 与 v_i, v_j 关联。

6.1.4 顶点的度数

无向图 $G = (V, E)$，$v \in V$：

- **度** $d_G(v)$：v 作为边的端点的次数之和
- **悬挂顶点**：度数为 1；**悬挂边**：与悬挂顶点关联的边
- **最大度** $\Delta(G) = \max\{d(v) \mid v \in V\}$
- **最小度** $\delta(G) = \min\{d(v) \mid v \in V\}$

有向图 $D = (V, E)$，$v \in V$：

- **出度** $d_D^+(v)$：v 作为始点的次数
- **入度** $d_D^-(v)$：v 作为终点的次数
- **度** $d_D(v) = d_D^+(v) + d_D^-(v)$
- 类似定义 $\Delta^+(D), \delta^+(D), \Delta^-(D), \delta^-(D)$

例： 下图度数序列为 5, 3, 3, 3；出度序列 4, 0, 2, 1；入度序列 1, 3, 1, 2。

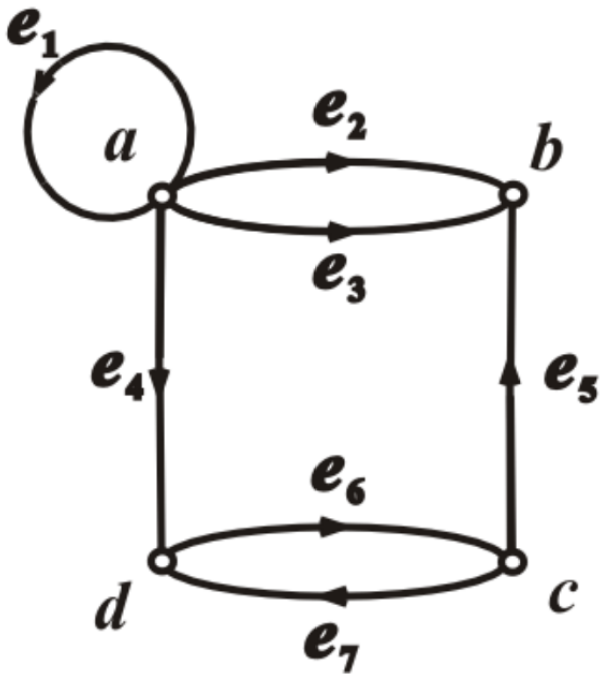


图 6.3: 度数示例

6.1.5 握手定理【重点】

这是图论中第一个”不显然但正确”的定理。它说：你把所有人的朋友数加起来，结果一定是偶数。为什么？因为每次握手都涉及两个人。

设图 $G = (V, E)$，$V = \{v_1, \ldots, v_n\}$，$|E| = m$，则：

$$\sum_{i=1}^{n} d(v_i) = 2m$$

推论： 任何图中，度数为奇数的顶点个数是偶数。

设有向图 D，$|E| = m$，则：

$$\sum_{i=1}^{n} d^+(v_i) = \sum_{i=1}^{n} d^-(v_i) = m$$

考试常考： 已知某些顶点的度数，利用握手定理求边数或未知顶点的度。关键是记住 $2m$ = 总度数。

例 1（由度数求边数）：已知无向图 G 有 6 个顶点，度数分别为 $3,3,2,2,4,4$，求 G 的边数。

解：所有顶点度数之和 $\sum d(v_i) = 3+3+2+2+4+4 = 18$。由握手定理 $2m = 18$，得 $m = 9$。即图 G 有 9 条边。

例 2（由边数求未知度数）：已知无向图 G 有 7 条边，其中 4 个顶点的度数分别为 $1,2,3,4$。若 G 共有 5 个顶点，求第 5 个顶点的度数。

解：由握手定理，所有顶点度数之和 $= 2\times 7 = 14$。已知 4 个顶点度数和 $= 1+2+3+4 = 10$。设第 5 个顶点度数为 x，则 $10 + x = 14$，得 $x = 4$。

例 3（奇度顶点个数）：证明任意无向图中，度数为奇数的顶点个数必为偶数。

证明：设 V_1 为奇度顶点集，V_2 为偶度顶点集。由握手定理：

$$\sum_{v\in V_1} d(v) + \sum_{v\in V_2} d(v) = 2m$$

右端 $2m$ 为偶数；$\sum_{v\in V_2} d(v)$ 为偶数（偶度之和为偶）。因此 $\sum_{v\in V_1} d(v)$ 必为偶数。而 V_1 中每个顶点的度数均为奇数，奇数之和为偶数 $\Longleftrightarrow$ 奇数个数为偶数。故 $|V_1|$ 为偶数。□

例 4（有向图握手定理）：有向图 D 有 5 个顶点，出度分别为 $2,1,3,0,2$，求边数 m。

解：$\sum d^+(v_i) = 2+1+3+0+2 = 8$。由有向图握手定理 $m = \sum d^+(v_i) = 8$。验证入度：若入度分别为 $1,2,1,4,0$，则 $\sum d^-(v_i) = 8 = m$，一致。

6.2 多重图、简单图、完全图、子图、补图、同构

6.2.1 多重图与简单图

- **平行边**：关联同一对顶点的多条边（无向）或同始点同终点的多条边（有向），条数称为**重数**
- **多重图**：含平行边的图
- **简单图**：既无平行边也无环的图

例：e_5 和 e_6 是平行边，重数为 2，这不是简单图。

简单图是本课的主要研究对象——没有环、没有平行边，每个顶点之间最多一条边。

6.2.2 完全图

1. n 阶无向简单图中，若任何顶点都与其余 $n-1$ 个顶点相邻，称为 n 阶**无向完全图**，记作 K_n。
2. n 阶有向简单图中，若任意 u,v 之间既有 $\langle u,v\rangle$ 又有 $\langle v,u\rangle$，称为 n 阶**有向完全图**。

K_n 有 $C(n,2) = n(n-1)/2$ 条边。K_5 有 10 条边，$K_{3,3}$ 是特殊的完全二部图——它们都是著名的非平面图。

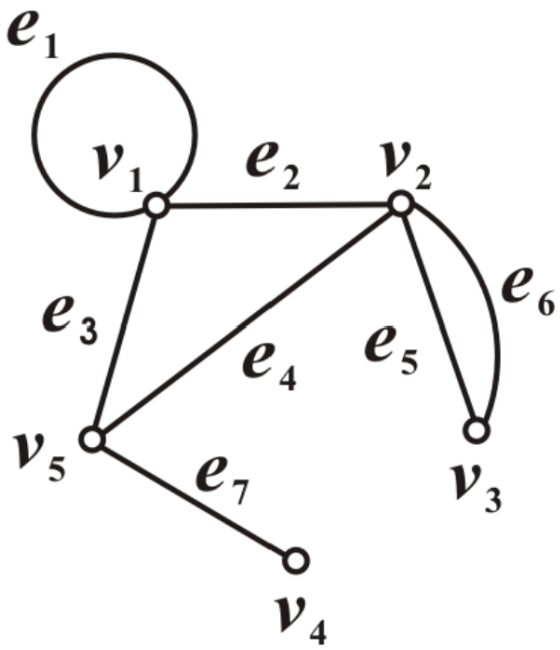


图 6.4: 平行边示例

6.2.3 子图

设 $G=(V,E)$，$G'=(V',E')$：

- $V'\subseteq V$ 且 $E'\subseteq E \to G'$ 是 G 的**子图**，G 是 G' 的**母图**
- $V'=V$ 且 $E'\subseteq E \to$ **生成子图**
- $V'\subset V$ 且 $E'\subset E \to$ **真子图**
- 以 V' 为顶点集、两端点都在 V' 中的边为边集 $\to V'$ 的**导出子图** $G[V']$
- 以 E' 为边集、E' 中边关联的顶点为顶点集 $\to E'$ 的**导出子图** $G[E']$

例：b,c 都是 a 的子图，c 为生成子图。b 是 $\{v_1,v_2\}$ 的导出子图，c 是 $\{e_1,e_3,e_4\}$ 的导出子图。

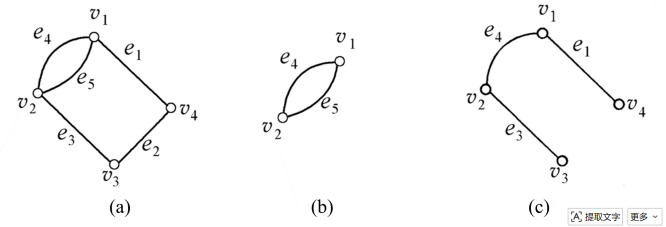


图 6.5: 子图示例

6.2.4 补图

设 G 为 n 阶无向简单图，$\overline{G}$ 的定义：$V(\overline{G})=V(G)$，且

$$E(\overline{G})=\{\{u,v\}\mid u,v\in V,u\neq v,\{u,v\}\notin E(G)\}$$

补图就是”把原来有边的删掉，原来没边的补上”。G 与 $\overline{G}$ 的边数之和 = K_n 的边数 = $n(n-1)/2$。

6.2.5 同构

设两个无向图 G_1 和 G_2，如果存在双射 $\theta : V_1 \to V_2$，使得 $\{u, v\} \in E_1 \iff \{\theta(u), \theta(v)\} \in E_2$，且重数相同，则称 $G_1 \cong G_2$。

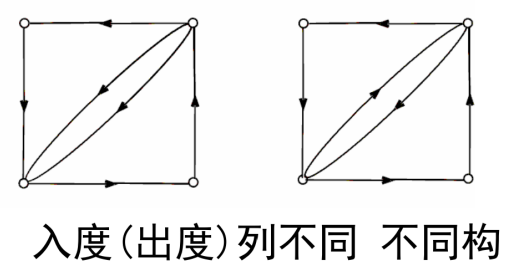


图 6.6: 同构示例 1

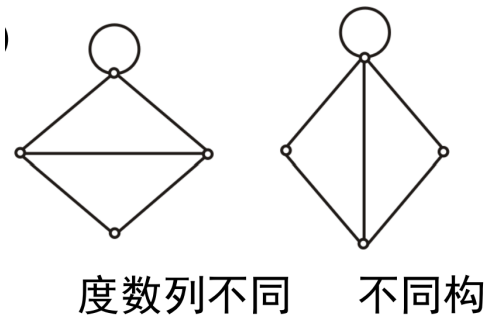


图 6.7: 同构示例 2

没有判定同构的充分必要条件（这是一个著名的开放问题）。但必要条件可用来排除不同构：1. 边数和顶点数相同 2. 度数列相同（不计顺序）3. 对应顶点的关联集及邻域的元素个数相同

破坏任何一条即可断定两图不同构。但满足所有必要条件也不保证同构——这恰是图同构问题的困难所在。

6.3 通路与回路

设 $\Gamma = v_0 e_1 v_1 e_2 \cdots e_l v_l$ 为顶点与边的交替序列，若 v_{i-1} 和 v_i 是 e_i 的端点，则称 Γ 为 v_0 到 v_l 的**通路**，l 为**长度**。若 $v_0 = v_l$，则称 Γ 为**回路**。

分类：

- 所有边互不相同 → **简单通路 / 简单回路**
- 除 $v_0 = v_l$ 外所有顶点互不相同 → **初级通路（路径） / 初级回路（圈）**
- 有边重复 → **复杂通路 / 复杂回路**

表示方法：

- 顶点边交替：$\Gamma = v_0 e_1 v_1 e_2 \cdots e_l v_l$

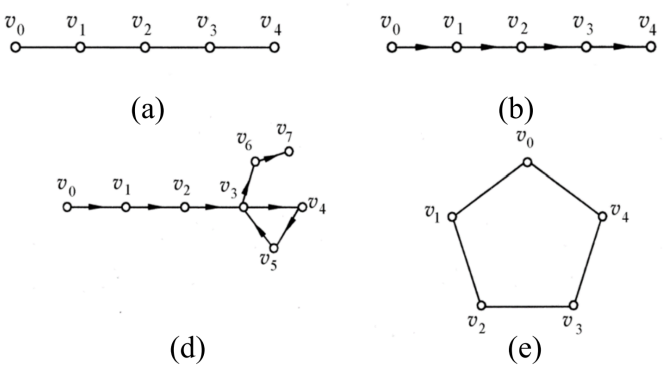


图 6.8: 通路与回路示例

- 只用边序列：$\Gamma = e_1 e_2 \cdots e_l$
- 简单图中用顶点序列：$\Gamma = v_0 v_1 \cdots v_l$

圈的计数注意：

- 定义意义下：无向图中长度为 l ($l \geq 3$) 的圈看作 $2l$ 个
- 同构意义下：长度相同的圈视为 1 个

定理： n 阶图 G 中，若存在 v_i 到 v_j 的通路，则存在长度 $\leq n-1$ 的初级通路。若存在 v_i 到自身的回路，则存在长度 $\leq n$ 的初级回路。

6.4 连通性

1. 无向图 G 中，若 u 到 v 存在通路，则称 u 与 v **连通**（规定每个顶点与自身连通）。
2. 有向图 D 中，若 u 到 v 存在通路，称 u **可达** v。
3. G 是平凡图或任意两顶点连通 $\rightarrow$ **连通图**；否则**非连通图**。

6.4.1 连通分支

顶点间的连通关系是**等价关系**。按此关系将 $V(G)$ 划分成等价类 $V_1, \ldots, V_k$，则导出子图 $G[V_1], \ldots, G[V_k]$ 称为**连通分支**，个数记为 $p(G)$。

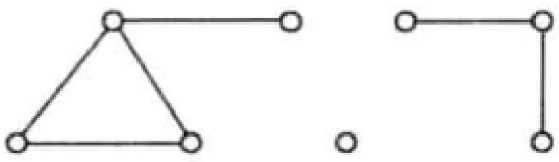
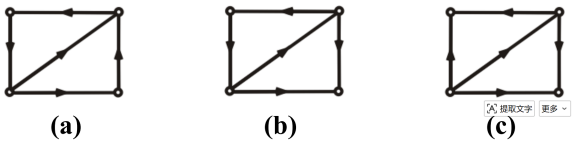


图 6.9: 连通分支

6.4.2 有向图的连通

- **弱连通**：略去方向后连通



(a)为强连通图，(b)为单向连通图，(c)是(弱)连通图

图 6.10: 连通图

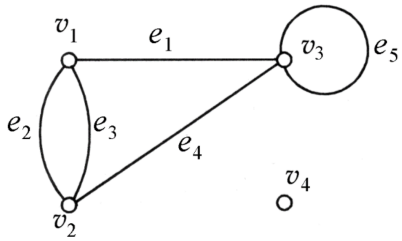
- **单向连通**：任意两顶点至少一个可达另一个
- **强连通**：任何一对顶点相互可达

强连通 ⇒ 单向连通 ⇒ 弱连通，反过来都不成立。

6.5 图的矩阵表示

6.5.1 关联矩阵

无向图：$M(G)=(m_{ij})_{n\times m}$，$m_{ij}$ 为 v_i 与 e_j 的关联次数。



关联矩阵$M(G)=\begin{bmatrix}1&1&1&0&0\\0&1&1&1&0\\1&0&0&1&2\\0&0&0&0&0\end{bmatrix}$

图 6.11: 关联矩阵

性质：

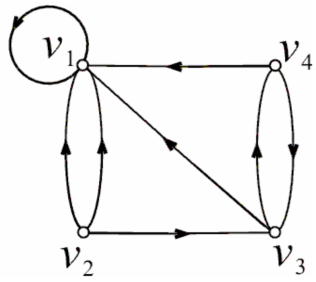
1. 每列恰有两个 1 或一个 2（环）
2. 第 i 行和 = $d(v_i)$
3. 所有元素和 = $2m$
4. v_i 是孤立点 $\iff$ 第 i 行全 0
5. e_j 与 e_k 平行 $\iff$ 第 j 列与第 k 列相同

6.5.2 邻接矩阵（有向图）

$A(D)=(a_{ij})_{n\times n}$，$a_{ij}$ 为 v_i 邻接到 v_j 的边数。

性质：

1. 第 i 行和 = $d^+(v_i)$，第 j 列和 = $d^-(v_j)$



$$A(D)=\begin{bmatrix}1&0&0&0\\2&0&1&0\\1&0&0&1\\1&0&1&0\end{bmatrix}$$

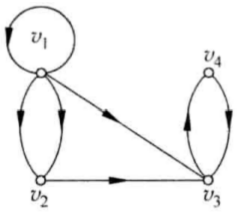
图 6.12: 邻接矩阵

2. 所有元素和 = m
3. A^l 中 (i,j) 元 = v_i 到 v_j 长度为 l 的通路数
4. A^l 中 (i,i) 元 = 长度为 l 的回路数

邻接矩阵的幂次与通路数的关系是图论最漂亮的应用之一。它把图的结构问题转化成了矩阵运算。

6.5.3 可达矩阵

$P(D)=(p_{ij})_{n\times n}$，$p_{ij}=1$ 若 v_i 可达 v_j，否则 0。



$$P(D)=\begin{bmatrix}1&1&1&1\\0&1&1&1\\0&0&1&1\\0&0&1&1\end{bmatrix}$$

图 6.13: 可达矩阵

性质：主对角线恒为 1；D 强连通 $\iff$ $P(D)$ 全为 1。

6.6 割集

设无向图 $G=(V,E)$：

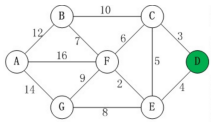
- $V'\subset V$，若 $G-V'$ 不连通，且对 V' 的任何真子集 V''，$G-V''$ 连通 $\to V'$ 为**点割集**。单点割集称为**割点**。
- $E'\subseteq E$，类似定义 $\to E'$ 为**边割集**（简称**割集**）。单边割集称为**割边**或**桥**。

6.7 最短路径、关键路径与着色

6.7.1 Dijkstra 最短路径算法【不考】

求从 D 到 A 的最短路径：

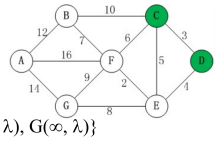
选取顶点D，
默认起点D的距离为0，
且上一个顶点为空，记为λ
此时P={D(0, λ)}
剩余顶点集为
T={A(∞, λ), B(∞, λ), C(∞, λ), E(∞, λ), F(∞, λ), G(∞, λ)}



更新T：T={A(∞, λ), B(∞, λ), C(3, D), E(4, D), F(∞, λ), G(∞, λ)}

图 6.14: Dijkstra 1

步骤二：
选取顶点C，
此时P={D(0, λ), C(3,D)}
剩余顶点集为
T={A(∞, λ), B(∞, λ), E(4, D), F(∞, λ), G(∞, λ)}



更新T：T={A(∞, λ), B(13, C), E(4, D), F(9, C), G(∞, λ)}

步骤三：
选取顶点E，
此时P={D(0, λ), C(3,D), E(4,D)}
剩余顶点集为
T={A(∞, λ), B(13, C), F(9, C), G(∞, λ)}

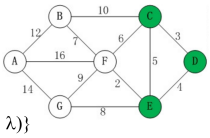
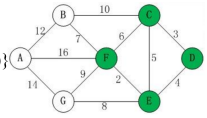


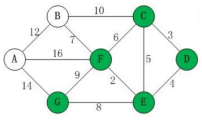
图 6.15: Dijkstra 2

步骤四：
选取顶点F，
此时P={D(0, λ), C(3,D), E(4,D), F(6,E)}
剩余顶点集为
T={A(∞, λ), B(13, C), G(12, E)}



更新T： T={A(22, F), B(13, C或F), G(12, E)}

步骤五：
选取顶点G，
此时P={D(0, λ), C(3,D), E(4,D),
F(6,E), G(12, E)}
剩余顶点集为
T={A(22, F), B(13, C或F)}



更新T： T={A(22, F), B(13, C或F)}

图 6.16: Dijkstra 3

Dijkstra 算法是贪心策略的典范——每次选择当前距离最小的未确定顶点。时间复杂度 $O(n^2)$，用优先队列可优化到 $O(m \log n)$。

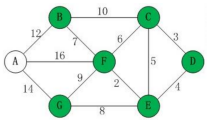
6.7.2 关键路径【不考】

在项目管理（PERT 图）中，**关键路径**是从开始到结束的最长路径——它决定了整个项目的最短完成时间。关键路径上的任何延误都会拖慢整个项目。

6.7.3 着色问题【重点】

定义：对无向图 G 的每个顶点涂一种颜色，使相邻顶点颜色不同，所需的最少颜色数称为 G 的**色数** $\chi(G)$。

步骤六：
选取顶点B，
此时P={D(0, λ), C(3,D), E(4,D), F(6,E), G(12, E), B(13, C或F)}
剩余顶点集为
T={A(22, F)}



更新T： T={A(22, F)}
最终P={D(0, λ), C(3,D), E(4,D), F(6,E), G(12, E), B(13, C或F), A(22, F)}

最短路径：
向前追溯：D、E、F、A

图 6.17: Dijkstra 4

四色定理：任何平面图都可以用至多 4 种颜色着色。这是第一个由计算机辅助证明的重要数学定理（1976 年），至今没有纯人力的证明。

考试核心区分：- 点着色（图着色）：给**顶点**涂色，使相邻顶点颜色不同。色数记作 $\chi(G)$。- **面着色（地图着色）：**给平面图的**面**涂色，使有公共边界的面颜色不同。色数记作 $\chi^*(G)$。- **关键关系：**地图着色（面着色）等价于其对偶图的点着色。即 $\chi^*(G) = \chi(G^*)$。- 四色定理的原意是**面着色**——任何地图只需 4 种颜色就能区分所有相邻区域。转化为图论语言：任何平面图的对偶图，其点色数 ≤ 4。

例 1（点着色—基本图）：求下列各图的色数 $\chi(G)$。

(a) **完全图** K_n：每个顶点与其余 $n-1$ 个顶点相邻，需 n 种颜色，$\chi(K_n) = n$。

(b) **偶圈** C_{2k}（长度为偶数的圈）：可用 2 种颜色交替涂色，$\chi(C_{2k}) = 2$。

(c) **奇圈** C_{2k+1}（长度为奇数的圈）：首尾顶点相邻、颜色冲突，需 3 种颜色，$\chi(C_{2k+1}) = 3$。

(d) **二部图**（无奇圈）：可用 2 种颜色（两部各一色），$\chi = 2$。

(e) **树**：无回路，可用 2 种颜色从根向叶交替涂，$\chi = 2$（$n \geq 2$）。

例 2（面着色—四色定理的直接体现）：给定一个平面图 G 的平面嵌入如下（文字描述：一个三角形内部有两个内点，分别与三角形三个顶点相连），请对面进行着色，并求 $\chi^*(G)$。

分析：画出平面嵌入后，此图共有 4 个面（含外部无限面）。先列出面之间的相邻关系（共享边界的面对）：外部面与 3 个内部面均相邻；3 个内部面两两相邻（通过内部边）。因此需要 4 种颜色——正符合四色定理的上界。

结论：$\chi^*(G) = 4$。此图的对偶图即 K_4（完全图），故 $\chi(G^*) = 4$，验证了面着色 = 对偶图点着色。

例 3（区分面着色与点着色）：对正四面体的平面嵌入（即 K_4 的平面嵌入），分别求：

(a) 点着色色数 $\chi(G)$ (b) 面着色色数 $\chi^*(G)$

解：(a) K_4 中每对顶点均相邻，需 4 种颜色。$\chi(K_4) = 4$。(b) 平面嵌入有 4 个面（3 个内部三角形面 + 1 个外部面），每个面都与其余 3 个面相邻。需 4 种颜色。$\chi^*(K_4) = 4$。

注意此处 $\chi = \chi^* = 4$，是因为 K_4 的平面嵌入是自对偶的。但一般情况下 $\chi(G)$ 与 $\chi^*(G)$ 未必相等。

例 4（用色数判定非平面图—间接应用）：若图 G 的色数 $\chi(G) > 4$，能否断定 G 是非平面图？

解：能。因为若 G 是平面图，则由四色定理，其点色数 $\chi(G) \leq 4$（注意：四色定理原意是面着色 ≤ 4，但其对偶形式即点着色 ≤ 4）。因此若 $\chi(G) \geq 5$，G 必为非平面图。例如 K_5 的色数为 5，故 K_5 非平面。

第 7 章 特殊的图

7.1 二部图与匹配

7.1.1 二部图

若能将无向图 G 的顶点集 V 划分成两个不相交的非空子集 V_1 和 V_2，使得每条边的两端点分别属于 V_1 和 V_2，则称 G 为**二部图**（偶图），记作 $G=(V_1,V_2,E)$。

若 V_1 中每个顶点与 V_2 中每个顶点均有且仅有一条边，称为**完全二部图** $K_{r,s}$（$r=|V_1|,s=|V_2|$）。

判定定理： G 是二部图 $\Longleftrightarrow$ G 中没有长度为奇数的回路。

7.1.2 匹配

设 $M\subseteq E$，若 M 中任意两条边均不相邻 → **匹配**。再加任一条边就不再是匹配 → **极大匹配**。边数最多 → **最大匹配**。匹配边数记作 $\nu(G)$。

v 是某条匹配边的端点 → **饱和点**。所有顶点都是饱和点 → **完美匹配**。

$|M|=|V_1|$（$|V_1|\le|V_2|$）→ V_1 到 V_2 的**完备匹配**。

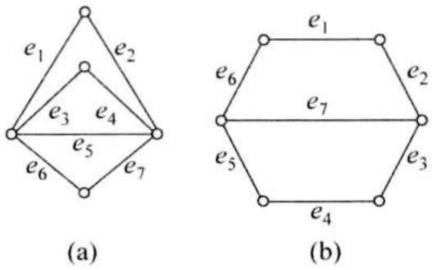


图 7.1: 匹配示例 1

图(a)中$\{e_1\}$、$\{e_1,e_7\}$、$\{e_5\}$、$\{e_4,e_6\}$等都是图中的匹配，其中$\{e_1,e_7\}$、$\{e_5\}$、$\{e_4,e_6\}$是极大匹配，$\{e_1,e_7\}$、$\{e_4,e_6\}$是最大匹配，匹配数是β_1 =2，图中有奇数个顶点显然不存在完美匹配。
图(b)中，$\{e_2,e_5\}$、$\{e_3,e_6\}$、$\{e_1,e_7,e_4\}$、$\{e_2,e_4,e_6\}$都是极大匹配，其中$\{e_1,e_7,e_4\}$、$\{e_2,e_4,e_6\}$是最大匹配。同时也是完美匹配，匹配数为3.

图 7.2: 匹配示例 2

7.1.3 Hall 定理（婚姻定理）

二部图 $G=(V_1,V_2,E)$（$|V_1|\le|V_2|$）存在 V_1 到 V_2 的完备匹配 $\Longleftrightarrow$ V_1 中任意 k 个顶点至少邻接 V_2 中的 k 个顶点。

> Hall 定理的直观含义：n 个男生要配 m 个女生（$n\le m$），每人有一些心仪对象。存在完美配对方案当且仅当——任何一组 k 个男生，他们合起来心仪的对象数 $\ge k$。如果某个” 男生小团体” 的心仪范围太小，就注定有人找不到对象。

相异性条件（充分条件）：$\exists t > 0$，使 V_1 每点至少关联 t 条边，V_2 每点至多关联 t 条边 $\rightarrow$ 存在完备匹配。

7.2 欧拉图

哥尼斯堡七桥问题（1736 年）：能否不重复地走完七座桥回到起点？欧拉把这个问题抽象为图论模型，由此开创了图论。

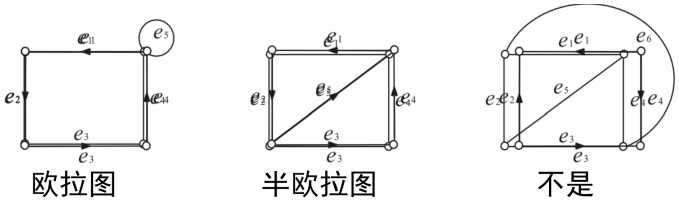


图 7.3: 欧拉图

经过图中每条边**一次且仅一次**并行遍每个顶点的回路/通路称为**欧拉回路/欧拉通路**。存在欧拉回路的图称为**欧拉图**。

判定（无向图）：

- 有欧拉回路 $\iff$ 连通且无奇度顶点
- 有欧拉通路但无欧拉回路 $\iff$ 连通且恰有两个奇度顶点（它们是通路的端点）

判定（有向图）：

- 有欧拉回路 $\iff$ 连通且每个顶点的入度 = 出度
- 有欧拉通路但无欧拉回路 $\iff$ 连通且除两个顶点外入度 = 出度，其中一个入度比出度大 1（终点），另一个出度比入度大 1（始点）

记法：欧拉关心的是**边**（每条边走一次）。判定只看度数的奇偶。

7.3 哈密顿图

哈密顿关心的是**顶点**（每个顶点访问一次）。与欧拉图的判定（充要条件）不同，哈密顿图至今没有简洁的充要条件。

经过图中每个顶点**一次且仅一次**的通路/回路称为**哈密顿通路/哈密顿回路**。存在哈密顿回路的图称为**哈密顿图**。

必要条件：G 为哈密顿图，则对任意非空 $V' \subset V$，有 $p(G - V') \leq |V'|$。

充分条件（无向简单图）：n 阶图 G 中，任何一对不相邻顶点的度数之和 $\geq n-1$ $\rightarrow$ 存在哈密顿通路；$\geq n$ $\rightarrow$ 存在哈密顿回路。

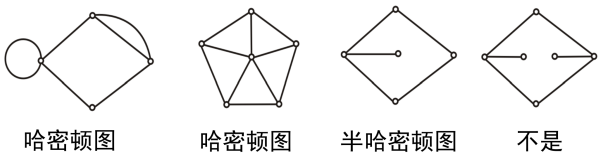


图 7.4: 哈密顿图

考试技巧：判断一个图不是哈密顿图，通常用必要条件（找一个 V' 使 $p(G-V')>|V'|$）。判断是哈密顿图，直接画出一条哈密顿回路即可。

7.4 平面图

图 G 能画在平面上使除顶点外无边交叉 → **平面图**。这种画法称为**平面嵌入**。否则**非平面图**。

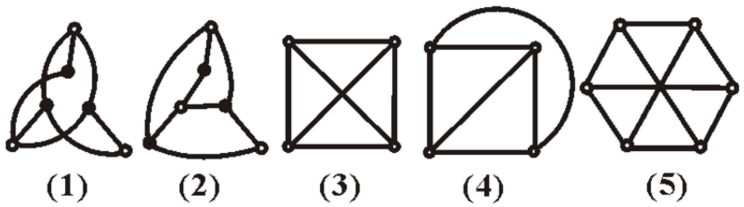


图 7.5: 平面图示例

7.4.1 面与次数

平面嵌入被边分割成的每个区域称为**面**。无限面记作 R_0，有限面记作 $R_1,\ldots,R_k$。

面的**边界**：包围该面的所有边构成的回路组。面的**次数** $\deg(R_i)$：边界长度。

性质：所有面的次数之和 = $2m$（每条边在计算中被使用两次）。

7.4.2 极大平面图与极小非平面图

在平面图中再加任一条边就变非平面 → **极大平面图**。从非平面图中删任一条边就变平面 → **极小非平面图**。

n 阶简单平面图是极大平面图 $\iff$ 连通且每个面的次数均为 3。

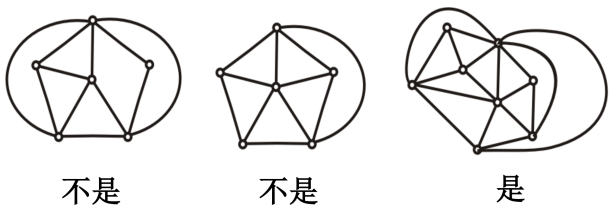


图 7.6: 极大平面图

7.4.3 欧拉公式【重点】

设 G 为 n 阶 m 条边 r 个面的连通平面图：

$$n-m+r=2$$

若 G 有 k 个连通分支：$n-m+r=k+1$。

推论：若每个面的次数 $\geq l$ $(l\geq 3)$，则 $m\leq \frac{l}{l-2}(n-2)$。

应用：K_5 和 $K_{3,3}$ 不是平面图。

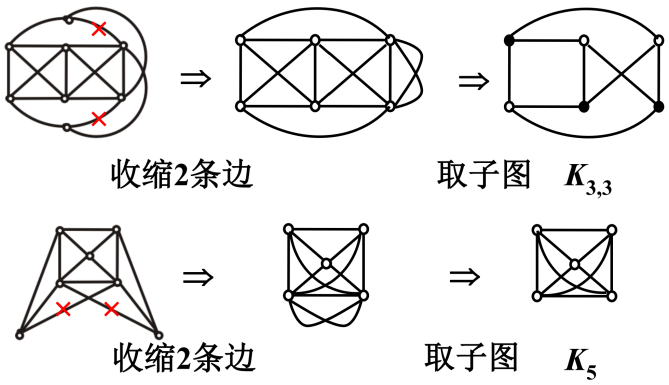


图 7.7: 证明非平面图

证明 K_5 非平面：$n=5, m=10$，若平面则每个面 ≥ 3，$m\leq \frac{3}{1}(5-2)=9$，但 $10>9$，矛盾。

证明 $K_{3,3}$ 非平面：$n=6, m=9$，二部图中无奇圈，每个面 ≥ 4，$m\leq \frac{4}{2}(6-2)=8$，但 $9>8$，矛盾。

库拉图斯基定理：一个图是平面图 $\Longleftrightarrow$ 它不含与 K_5 或 $K_{3,3}$ 同胚的子图。

例 1（公式直接应用）：已知连通平面图 G 有 $n=5$ 个顶点，$m=7$ 条边，求面数 r 及所有面的次数之和。

解：由欧拉公式 $n-m+r=2$，代入得 $5-7+r=2$，故 $r=4$（含外部无限面）。所有面的次数之和 $=2m=14$（每条边恰被两个面各计一次）。

例 2（欧拉公式的证明—对边数归纳）：证明连通平面图满足 $n-m+r=2$。

证：对边数 m 作数学归纳。**基始**：$m=0$（零图）。此时只有 1 个顶点和 1 个面（无边界），$1-0+1=2$，成立。**归纳步**：设边数 $<m$ 时命题成立，考虑边数 $=m$ 的连通平面图 G。- 若 G 是树，则 $m=n-1$，$r=1$，$n-(n-1)+1=2$，成立。- 若 G 含初级回路，取回路上任一边 e。删去 e 得 $G'=G-e$：G' 仍连通，$n'=n$，$m'=m-1$。由于 e 原属两个不同面的边界（或同一面的两侧边界），删去后这两个面合并，故 $r'=r-1$。由归纳假设 $n'-m'+r'=2$，代入得 $n-(m-1)+(r-1)=n-m+r=2$。□

例 3（多连通分支情形）：平面图 G 有 $k=3$ 个连通分支，$n=10$ 个顶点，$m=12$ 条边。求面数 r。

解：多分支欧拉公式 $n-m+r=k+1$。代入：$10-12+r=3+1=4$，得 $r=6$。

例 4（最大边数推论）：证明 $n\geq 3$ 的简单连通平面图中，$m\leq 3n-6$。

证：简单图中无环无平行边，每个面的次数 ≥ 3。所有面次数之和 $=2m\geq 3r$，故 $r\leq \frac{2m}{3}$。代入欧拉公式：

$$n-m+r=2\ \Rightarrow\ n-m+\frac{2m}{3}\geq 2\ \Rightarrow\ n-\frac{m}{3}\geq 2\ \Rightarrow\ m\leq 3n-6$$

此推论是证明 K_5 非平面的关键（$n=5$ 时 $3n-6=9$，而 K_5 有 10 条边）。

例 5（利用欧拉公式证明五色定理的引理）：证明任何简单连通平面图 G 中必存在度数 ≤ 5 的顶点。

证：反设所有顶点度数 ≥ 6。则 $2m=\sum d(v_i)\geq 6n$，即 $m\geq 3n$。但由欧拉公式的推论 $m\leq 3n-6$。两者矛盾。故必存在度数 ≤ 5 的顶点。□

7.4.4 对偶图【重点】

在平面图 G 的每个面中取一点作为新顶点，穿过每条边作新边连接相邻面的顶点——得到 G 的**对偶图** G^*。

对偶图在电路理论（电流图-电压图对偶）和地图着色中有重要应用。

对偶图画法口诀：面中取点 → 穿边连线。具体步骤：

1. 在 G 的**每个面**（含外部无限面）内部各取一个点，作为 G^* 的顶点。2. 对 G 的**每条边** e，若 e 分隔面 R_i 与 R_j，则在 G^* 中作一条边连接 R_i 与 R_j 内对应的顶点。3. 所有新边与 G 的边仅相交一次（交叉即穿过）。得到的图即 G^*。

例 1（三角形—最简单的情形）：画出 3 阶圈 C_3（三角形）的对偶图。

解：C_3 的平面嵌入有两个面：一个有限面（三角形内部 R_1）和一个外部无限面 R_0。在 R_0 和 R_1 中各取一点。C_3 有三条边，每条边分隔 R_0 与 R_1，故作三条新边连接两顶点。结果：C_3^* 是含 2 个顶点、3 条平行边的多重图（两端点间有 3 条平行边）。

注意 C_3^* 不是简单图——这提醒我们对偶图可能含平行边。

例 2（四边形加一条对角线）：画出以下平面图的对偶图：4 个顶点构成四边形，加上一条对角线将一个有限面切成两个三角形面。

解：此平面图共有 3 个面：- R_0：外部无限面，边界为四边形的 3 条外侧边。- R_1：上三角形面，边界为对角线和两条边。- R_2：下三角形面，边界为对角线和另两条边。

在 R_0, R_1, R_2 中各取顶点 v_0^*, v_1^*, v_2^*。- 对角线分隔 R_1 和 R_2 → 作边 $v_1^*v_2^*$ - 四边形的两条边各分隔 R_0 与 R_1 → 作两条平行边 $v_0^*v_1^*$ - 四边形的另两条边各分隔 R_0 与 R_2 → 作两条平行边 $v_0^*v_2^*$

G^* 为 3 顶点图：v_0^* 分别与 v_1^*, v_2^* 各有 2 条平行边，v_1^* 与 v_2^* 有 1 条边。

例 3（正四面体——自对偶图）：画出 K_4 的平面嵌入（正四面体展平）的对偶图。

解：K_4 的平面嵌入有 4 个面（3 个三角形内部面 + 1 个三角形外部面）。在每个面内取一点得 G^* 的 4 个顶点。每条边分隔两个面，故 G^* 有 6 条边。并且 G^* 中每对顶点之间也恰好有一条边相连（因为 K_4 的每对面都共享一条边）。因此 $G^* \cong K_4$——K_4 的平面嵌入是**自对偶图**。

自对偶图的性质：$n^* = r$，$m^* = m$，$r^* = n$。

例 4（对偶图与面着色的关系）：简述为什么” 地图的面着色” 等价于” 对偶图的点着色”。

解：在地图（平面图）中，要求相邻区域（共享边界的面）颜色不同。作对偶图后：- 每个面对应 G^* 的一个顶点 - 两个面相邻（共享边） $\Longleftrightarrow$ G^* 中对应两顶点之间有边相连

因此，对地图面着色（面相邻 $\rightarrow$ 不同色）完全等价于对 G^* 做点着色（点相邻 $\rightarrow$ 不同色）。这就是四色定理从面着色语言翻译为点着色语言的桥梁。

第 8 章 树

树是最简单的连通图——连通且无回路。它是计算机科学中最无处不在的数据结构：文件系统、HTML DOM、表达式树、路由表……当你理解了树的图论定义和性质，再看那些数据结构，会发现它们不过是同一朵花的不同瓣。

8.1 无向树与生成树【不考】

8.1.1 树的定义与等价条件

不含回路的连通无向图称为**无向树**，简称**树**。每个连通分支都是树的非连通图称为**森林**。

设 G 是 n 阶 m 条边的无向图，以下命题**等价**：

1. G 连通且不含回路
2. G 每对顶点间有唯一路径
3. G 连通且 $m = n - 1$
4. G 无回路且 $m = n - 1$
5. G 无回路，但在任意不相邻顶点间加一条边就产生唯一的初级回路
6. G 连通且每条边都是桥

树的本质：n 个顶点的树恰好有 $n - 1$ 条边，多一条就出回路，少一条就不连通。它是”刚好能连通的极小边集”。

树叶：度数为 1 的顶点。**分支点**：度数 ≥ 2 的顶点。

注意区分：图论中树的”度”指一个顶点关联的边数，这与数据结构课程中树的”度”（一个节点的子节点数）是**不同**的定义，考试时注意按图论定义作答。

定理：n 阶非平凡树至少有 2 片树叶。

8.1.2 生成树

设 T 是 G 的生成子图且是树 $\rightarrow T$ 为 G 的**生成树**。

- **树枝**：G 在 T 中的边（$n - 1$ 条）
- **弦**：G 不在 T 中的边（$m - n + 1$ 条）
- **余树**：所有弦的导出子图

定理：任何无向连通图都有生成树。$\Rightarrow m \geq n - 1$。

8.1.3 最小生成树

求带权图中权值最小的生成树。常用算法：**Kruskal**（按边权从小到大贪心选取，不形成回路则选入）和 **Prim**（从一点开始，每次选与已选集合连接的最小权边）。

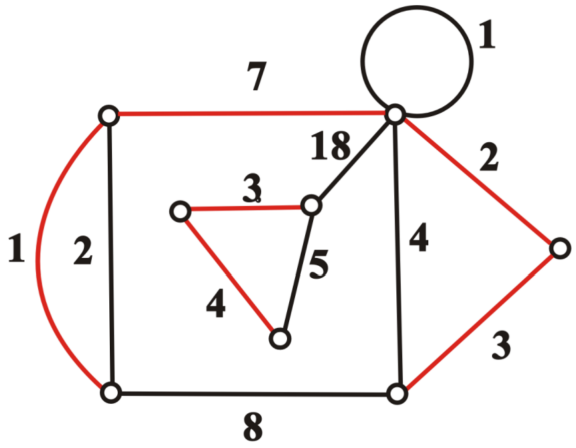


图 8.1: 最小生成树

8.1.4 基本回路与基本割集【不考】

给定生成树 T：

- 加一条弦 → 唯一初级回路 → **基本回路**
- 删一条树枝 → 图不连通 → **基本割集**

基本回路和基本割集提供了分析图结构的" 基"——类似线性代数中的基向量，所有回路都可以用基本回路线性组合（在 $\mathbb{Z}_2$ 上）来表示。

8.2 根树及其应用

8.2.1 根树

略去方向后为无向树的有向图称为**有向树**。有一个顶点入度为 0、其余入度均为 1 的非平凡有向树称为**根树**。

- **树根**：入度为 0 的顶点
- **树叶**：入度为 1、出度为 0
- **内点**：入度为 1、出度 > 0
- **层数**：从根到该顶点的通路长度；**树高**：最大层数

8.2.2 有序树与 m 叉树

如果对根树每层上的顶点规定次序 → **有序树**。每个分支点至多有 m 个儿子 → m **叉树**；每个分支点恰有 m 个儿子 → **正则** m **叉树**。所有树叶层数相同 → **完全** m **叉树**。

右图所示
*a*是树根
*b,e,f,h,i*是树叶
*c,d,g*是内点
*a,c,d,g*是分支点
*a*为0层;1层有*b,c*; 2层有*d,e,f*;
3层有*g,h*; 4层有*i*.
树高为4

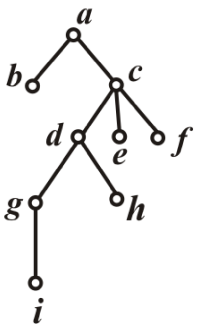


图 8.2: 根树

8.2.3 最优二叉树（Huffman 树）【重点】

设二叉树 T 有 t 片树叶，权分别为 $w_1, \ldots, w_t$，**权** $w(T) = \sum_{i=1}^{t} w_i \cdot l(v_i)$（$l(v_i)$ 为树叶 v_i 的层数）。使 $w(T)$ 最小的二叉树称为**最优二叉树**或 **Huffman 树**。

Huffman 编码是数据压缩的经典算法——频率高的字符用短编码，频率低的用长编码，从而使平均编码长度最小化。它在 ZIP、JPEG、MP3 等格式中无处不在。

Huffman 算法步骤：

1. 将所有树叶权值 $w_1, \ldots, w_t$ 放入集合 F（每片树叶是一棵单结点树）。2. 从 F 中选出两棵权最小的树 T_1, T_2（权分别为 w_{T_1}, w_{T_2}）。3. 构造新二叉树：以新结点为根，T_1, T_2 为左右子树（次序任意），新树的权 $= w_{T_1} + w_{T_2}$。将此新树放回 F。4. 重复步骤 2—3，直到 F 中只剩一棵树。这棵树即最优二叉树。

考试常考：给定权值，画出 Huffman 树的构造过程（合并森林图）并计算 $W(T)$。

例 1（基本构造）：给定权值 $\{2, 3, 4, 7, 8, 9\}$，构造 Huffman 树并求 $W(T)$。

解：逐步合并过程（每次合并两个最小权）：

初始：$\{2, 3, 4, 7, 8, 9\}$ - 第 1 步：合并 2 和 3，得子树权 5。集合变为 $\{4, 5, 7, 8, 9\}$ - 第 2 步：合并 4 和 5，得子树权 9。集合变为 $\{7, 8, 9, 9\}$ - 第 3 步：合并 7 和 8，得子树权 15。集合变为 $\{9, 9, 15\}$ - 第 4 步：合并 9 和 9，得子树权 18。集合变为 $\{15, 18\}$ - 第 5 步：合并 15 和 18，得树根权 33。完成。

计算 $W(T)$——每片树叶的权 × 层数：- 权 2：层数 4（从根往下数，根为第 0 层则层数 = 4）- 权 3：层数 4 - 权 4：层数 3 - 权 7：层数 3 - 权 8：层数 3 - 权 9：层数 2

$$W(T) = 2 \times 4 + 3 \times 4 + 4 \times 3 + 7 \times 3 + 8 \times 3 + 9 \times 2 \quad = 8 + 12 + 12 + 21 + 24 + 18 = 95$$

例 2（不等概率的 Huffman 编码）：某报文中 5 个字符出现频率为 $a: 0.4,\ b: 0.25,\ c: 0.2,\ d: 0.1,\ e: 0.05$。构造 Huffman 树并为每个字符分配编码。

解：用频率（或乘以 100 化为整数权 $\{40, 25, 20, 10, 5\}$）：- 合并 5 和 10 → 子树权 15。集合 $\{40, 25, 20, 15\}$ - 合并 15 和 20 → 子树权 35。集合 $\{40, 25, 35\}$ - 合并 25 和 35 → 子树权 60。集合 $\{40, 60\}$ - 合并 40 和 60 → 根权 100。

编码分配（约定左 0 右 1，或反过来均可）：- $a(40)$：0 - $b(25)$：10 - $c(20)$：110 - $d(10)$：1110 - $e(5)$：1111

高频字符 a 用最短码（1 位），低频 d, e 用长码（4 位）——这正是 Huffman 编码压缩数据的核心思想。

例 3（已知 Huffman 树反推权值关系）：一棵 Huffman 树有 4 片树叶，权分别为 w_1, w_2, w_3, w_4（$w_1 \le w_2 \le w_3 \le w_4$）。若 $w_4 < w_1 + w_2$，这棵 Huffman 树的形状是怎样的？

解：Huffman 算法优先合并最小两权。若 $w_4 < w_1 + w_2$，说明在第二次合并时，w_4 权值仍小于 $w_1 + w_2$，因此：- 第 1 步：合并 $w_1, w_2 \to$ 权 $w_1 + w_2$。集合 $\{w_1 + w_2, w_3, w_4\}$ - 此时最小的两个权是 w_3 和 w_4（因为 $w_3 \le w_4 < w_1 + w_2$）- 第 2 步：合并 $w_3, w_4 \to$ 权 $w_3 + w_4$。集合 $\{w_1 + w_2, w_3 + w_4\}$ - 第 3 步：合并这两棵子树。

最终树形：左右各一对树叶（w_1 与 w_2 同层，w_3 与 w_4 同层），四片树叶均在倒数第二层。$W(T) = 2(w_1 + w_2 + w_3 + w_4)$。

例 4（验证最优性）：权值 $\{1, 3, 5, 7\}$，验证 Huffman 树确实使 $W(T)$ 最小。

解：Huffman 算法产出：合并 $1 + 3 = 4$，再合并 $4 + 5 = 9$，再合并 $9 + 7 = 16$。权 1、3 深度为 3，权 5 深度为 2，权 7 深度为 1。

$$W(T) = 1 \times 3 + 3 \times 3 + 5 \times 2 + 7 \times 1 = 29$$

若尝试其他合并次序（如先合并 5 和 7 得 12，再与 3 合并得 15，最后与 1 合并）：

$$W' = 1 \times 3 + 3 \times 2 + 5 \times 2 + 7 \times 2 = 3 + 6 + 10 + 14 = 33 > 29$$

Huffman 算法得到的 $W(T) = 29$ 确实是最小的。**核心直觉**：权越小的树叶离根越远（深度越大），权越大的离根越近（深度越小），加权和自然最小。Huffman 算法的贪心合并策略正是实现了这一目标。

8.2.4 前缀码【不考】

设 $\beta = \alpha_1\alpha_2\cdots\alpha_n$ 是长度为 n 的符号串，其子串 $\alpha_1\alpha_2\cdots\alpha_k$（$k \le n$）称为 β 的**前缀**。若码中任何符号串都不是其他符号串的前缀，称为**前缀码**。

前缀码保证了解码的唯一性——读到任何一个码字的前缀时，不需要”往后看”就能确定这是一个完整的码字。最优二叉树恰好产生最优前缀码。

第四部分

矩阵论初步

第 9 章 矩阵基础及应用

本章序言：笔者在编写资料时对课程顺序和知识点的安排进行了一些小小的修改，会在节标题中给出对应

9.1 线代基础

下面我们给出一些基本知识，一些东西在 PPT 和课上是没有讲过的，大家可以重点复习一下这一部分：

(1) 特征值和特征向量：设 A 是 n 阶方阵，如果存在常数 λ 和 n 维非零列向量 u 满足关系式：

$$Au = \lambda u \tag{9.1}$$

则称 为 A 的**特征值**，u 为 A 的属于 λ 的一个**特征向量**。特征向量不唯一，可有无穷多个。

矩阵 IA 称为 A 的特征矩阵，其行列式

$$p(\lambda) = |\lambda \boldsymbol{I} - A| =$$

$$\begin{vmatrix} \lambda - \alpha_{11} & -\alpha_{12} & \dots & -\alpha_{1n} \\ -\alpha_{21} & \lambda - \alpha_{22} & \dots & -\alpha_{2n} \\ \dots & \dots & \dots & -\alpha_{3n} \\ -\alpha_{n1} & -\alpha_{n2} & \dots & \end{vmatrix}$$

$$= \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0$$

这里就涉及到一个不是很起眼的**小定理**：任一多项式 $p(\lambda)$ 都能被写成 n 阶方阵

$$A = \begin{bmatrix} -a_{n-1} & a_{n-2} & \cdots & (-1)^{n-1}a_1 & (-1)^n a_0 \\ -1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & \end{bmatrix}$$

的特征多项式。

此定理有一些深刻的意义：它证明了多项式空间和某种矩阵空间的同构性。同时，高次多项式求根（牛顿法）就可以转化为对矩阵 QR 分解求特征值，解决牛顿法的数值稳定性问题。

---

(2) 特征值分解（Eigenvalue Decomposition, EVD）：

特征值分解是线性代数中对方阵进行因子分解的核心方法。其物理意义是将一个线性变换分解为**方向不发生改变的拉伸/压缩运动**。

对于一个 $n \times n$ 的方阵 A，如果存在一个非零向量 u 和标量 λ，满足：

$$Au = \lambda u$$

如果矩阵 A 拥有 n 个线性无关的特征向量，将它们作为列向量排成一个矩阵 $U = [u_1, u_2, \cdots, u_n]$，并将对应的特征值排成对角矩阵 $\Lambda = \text{diag}(\lambda_1, \lambda_2, \cdots, \lambda_n)$，则上述关系可以写成矩阵形式：

$$AU = U\Lambda$$

因为 U 的列向量线性无关，所以 U 可逆。两边同时右乘 U^{-1} 即可得到 **EVD 的标准形式**：

$$A = U\Lambda U^{-1}$$

可对角化条件：

一个矩阵能够进行 EVD 的充要条件是它**拥有 n 个线性无关的特征向量**（此时称矩阵 A **可对角化**）。具体来说，可以通过以下几点来判断：

1. **必要前提：方阵：**只有 $n \times n$ 的方阵才有特征值分解。非方阵（如 $m \times n$）只能使用 * 奇异值分解（SVD）*。
1. **充分条件：**
- **互异特征值：**如果 A 有 n 个**互不相同**的特征值，那么它一定能进行 EVD。
- **实对称矩阵：**如果 A 是**实对称矩阵**（$A = A^T$），它不仅一定能分解，而且其特征向量还可以选为正交的，即 $UU^T = I$。
1. **充要条件：**

当矩阵存在重特征值（即某个特征值求出来是双重或多重根）时，需要看它的**几何重数**是否等于**代数重数**：

- **代数重数（Algebraic Multiplicity）：**特征多项式中该特征根的重数。
- **几何重数（Geometric Multiplicity）：**该特征值对应的特征空间 $\text{null}(\lambda I - A)$ 的维数（即独立特征向量的个数）。
- **结论：**当且仅当**每一个**特征值的几何重数都等于代数重数时，矩阵才能进行 EVD。如果几何重数小于代数重数，该矩阵被称为**缺陷矩阵（Defective Matrix）**，无法进行特征值分解（只能求若尔当标准型 Jordan Form）。

EVD 与行列式：

$$\det(A) = \prod_{i=1}^{n} \lambda_i$$

（3）若尔当形：

前文提到，当一个矩阵有重特征值，且特征向量不够用时（缺陷矩阵），它就无法进行特征值分解（EVD）。这时候，虽然没办法把矩阵变成完美的**对角阵**，但退而求其次，可以把它化简成结构最接近

对角阵的形状——这就是**若尔当形**。

任意一个复数域上的 $n \times n$ 方阵 A，都可以通过相似变换化为若尔当形 J：

$$A = PJP^{-1}$$

其中，若尔当形 J 是一个**分块对角矩阵**，主对角线上是一个个小的**若尔当块（Jordan Block）**：

$$J = \begin{bmatrix} J_1 & & \\ & J_2 & \\ & & \ddots \\ & & \end{bmatrix}$$

每一个具体的若尔当块 J_i 的内部结构高度固定：

- **主对角线**上全是某一个特征值 λ。
- 主对角线上方（次对角线）全是 1。
- 其余位置全是 0。

例如，一个 3×3 的若尔当块长这样：

$$J_i = \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \end{bmatrix}$$

> **直观理解**：次对角线上的那些 1，就是由于特征向量不够用而被迫留下的“胶水”。如果所有若尔当块的大小都是 1×1，那么 J 就退化成了普通的对角矩阵，此时就是标准的特征值分解。

那么若尔当形如何补齐不够的特征向量？

在 EVD 中，我们求解 $Au = \lambda u$。如果某个特征值 λ 只有 1 个特征向量 u_1，而我们实际需要 3 个向量来撑起空间。

若尔当形引入了广义特征向量（Generalized Eigenvectors）的概念。我们不强求后面的向量满足 $Au = \lambda u$，而是让它们满足一个递推链（**若尔当链**）：

1. **常规特征向量**：$(A - \lambda I)u_1 = 0$
2. **第一级广义特征向量**：$(A - \lambda I)u_2 = u_1 \implies Au_2 = \lambda u_2 + u_1$
3. **第二级广义特征向量**：$(A - \lambda I)u_3 = u_2 \implies Au_3 = \lambda u_3 + u_2$

如果把这些向量作为列拼成变换矩阵 $P = [u_1, u_2, u_3]$，去计算 AP：

$$AP = [Au_1, Au_2, Au_3] = [\lambda u_1, \lambda u_2 + u_1, \lambda u_3 + u_2] = [u_1, u_2, u_3] \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix} = PJ_i$$

这就解释了为什么若尔当块的对角线上方会出现 1。

(4) 矩阵多项式

考虑矩阵 A 的 n 次多项式

$$\mathrm{f(A)} = \mathrm{A}^n + c_1 A^{n-1} + \cdots + c_{n-1} A + c_n I$$

若矩阵 A 有特征对 $(\lambda, \boldsymbol{u})$，即 $A\boldsymbol{u} = \lambda \boldsymbol{u}$，则

$$\begin{aligned}\mathrm{f(A)}\boldsymbol{u} &= (\boldsymbol{A}^n + \boldsymbol{c_1 A}^{n-1} + \cdots + \boldsymbol{c_{n-1} A} + \boldsymbol{c_n I})\boldsymbol{u} \\ &= (\boldsymbol{\lambda}^n + \boldsymbol{c_1 \lambda}^{n-1} + \cdots + \boldsymbol{c_{n-1} \lambda} + \boldsymbol{c_n})\boldsymbol{u}\end{aligned}$$

令矩阵多项式 $f(A)$ 的特征值为 $f(\lambda)$，即 $f(A)\boldsymbol{u} = f(\lambda)\boldsymbol{u}$。将这一关系式带入上式，易知

$$\mathrm{f}(\lambda) = \lambda^n + c_1 \lambda^{n-1} + \cdots + c_{n-1}\lambda + c_n$$

是矩阵多项式 $f(A)$ 的特征值。

---

(5) 迹（trace）

符号为 $tr()$，这一部分在课上被轻描淡写的略过了，但实际上**迹**有非常重要的性质，能够帮助大幅简化矩阵求导的推导。这里进行比较系统的介绍：

1. **定义**：对于一个**方阵** $A \in \mathbb{F}^{n \times n}$，其迹为其主对角线上所有元素的代数和，即：

$$tr(A) = \sum_{i=1}^{n} a_{ii}$$

1. **线性性质（Linearity）**

迹是线性变换。对任意方阵 $A, B \in \mathbb{F}^{n \times n}$ 及标量 $c \in \mathbb{F}$，满足：

$$\mathrm{tr}(A + B) = \mathrm{tr}(A) + \mathrm{tr}(B)$$

$$\text{tr}(cA) = c \cdot \text{tr}(A)$$

1. **转置不变性（Invariance under Transposition）**

矩阵转置不改变主对角线上的元素：

$$\text{tr}(A) = \text{tr}(A^T)$$

1. **循环移位不变性（Cyclic Property）**

非常重要

这是迹最重要的代数性质。若 $A \in \mathbb{F}^{m\times n}$ 且 $B \in \mathbb{F}^{n\times m}$（注意：$A, B$ **不一定**是方阵，但乘积必须是方阵），则：

$$\text{tr}(AB) = \text{tr}(BA)$$

该性质可以推广到多个矩阵的乘积，只要满足循环移位（Cyclic Permutation）即可：

$$\text{tr}(ABC) = \text{tr}(CAB) = \text{tr}(BCA)$$

注意：迹对任意排列**不**保持不变，例如通常 $\text{tr}(ABC) \neq \text{tr}(BAC)$。

1. **相似不变性（Similarity Invariance）**

若方阵 A 与 B 相似，即存在可逆矩阵 P 使得 $B = P^{-1}AP$，则它们的迹相等：

$$\text{tr}(B) = \text{tr}(P^{-1}AP) = \text{tr}(APP^{-1}) = \text{tr}(A \cdot I) = \text{tr}(A)$$

这意味着迹是矩阵的一种**拓扑不变量**（不依赖于基底的选择）。

1. **特征值之和（Connection to Eigenvalues）**

根据相似不变性，若矩阵 A 在复数域内的特征值为 $\lambda_1, \lambda_2, \cdots, \lambda_n$（计入代数重数），则 A 相似于其若尔当标准形（或对角阵），因此：

$$\text{tr}(A) = \sum_{i=1}^{n} \lambda_i$$

同时，迹对应于特征多项式 $p(\lambda) = \det(\lambda I - A) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0$ 中 λ^{n-1} 项系数的相反数，即 $a_{n-1} = -\text{tr}(A)$。

1. **Frobenius 内积（Frobenius Inner Product）**

非常重要

在矩阵空间 $\mathbb{R}^{m\times n}$ 中，利用迹可以定义标准的 Frobenius 内积（两个同形矩阵，其对应位置元素乘积之和）：

$$\langle A, B\rangle_{\mathrm{F}} = \mathrm{tr}(A^T B) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij} b_{ij}$$

由此诱导出的矩阵范数即为 Frobenius 范数（根号下矩阵中所有元素的平方和，是向量 L2 范数的推广）：$\|A\|_{\mathrm{F}} = \sqrt{\mathrm{tr}(A^T A)}$。

证明如下：

$$A^T = \begin{bmatrix} a_1^T \\ a_2^T \\ \vdots \\ a_n^T \end{bmatrix} \quad B = \begin{bmatrix} \beta_1 & \beta_2 & \cdots & \beta_m \end{bmatrix}$$

现在我们计算方阵 $A^T B \in \mathbb{R}^{n\times n}$。根据矩阵乘法（左矩阵的行乘以右矩阵的列），$A^T B$ 的第 j 行、第 j 列的对角线元素 $(A^T B)_{jj}$，刚好由 A^T 的第 j 行（即 a_j^T）与 B 的第 j 列（即 b_j）相乘得到：

$$(A^T B)_{jj} = a_j^T b_j$$

这里的 $a_j^T b_j$ 正好是两个列向量在传统欧几里得空间里的标准内积 $\langle a_j, b_j\rangle$。求迹：根据迹的定义，将 $A^T B$ 的所有对角线元素沿指标 j 求和：

$$\mathrm{tr}(A^T B) = \sum_{j=1}^{n} (A^T B)_{jj} = \sum_{j=1}^{n} a_j^T b_j$$

当 $B = A$ 时，有 $\mathrm{tr}(A^T A) = \sum_{j=1}^{n} (A^T A)_{jj} = \sum_{j=1}^{n} a_j^T a_j = \sum_{j=1}^{n}\sum_{i=1}^{n} a_{ij}^2$

1. **迹的导数（Matrix Calculus）**

在矩阵微积分中，迹常用于简化微分表达。几个经典性质包括：

$$\frac{\partial}{\partial A}\mathrm{tr}(A) = I$$

$$\frac{\partial}{\partial A}\mathrm{tr}(AB) = B^T$$

$$\frac{\partial}{\partial A}\mathrm{tr}(A^T B A) = (B + B^T)A$$

这一部分将在 **矩阵求导**一节进行系统介绍。

---

(9) **矩阵幂级数：**

标量 x 的幂级数定义为

$$\mathrm{e}^x = 1 + x + \tfrac{1}{2!}x^2 + \tfrac{1}{3!}x^3 + \cdots$$

类似地，矩阵 A 的幂级数定义为

$$\mathrm{e}^{A} = I + A + \frac{1}{2!}A^2 + \frac{1}{3!}A^3 + \cdots = \sum_{i=0}^{\infty} \frac{1}{i!}A^n$$

假定级数收敛。若矩阵 A 的特征值为 λ，则由矩阵多项式的特征值表示式，立即知矩阵的指数函数 e^A 的特征值为

$$\mathrm{f}(\lambda) = \sum_{i=0}^{\infty} \frac{1}{i!}\lambda^n = e^{\lambda}$$

笔者在看到这里到时候对为什么要定义这个东西心存疑惑，但实际上在微分方程

$$\frac{d}{dt}x(t) = Ax(t)$$

中，引入 e^{At} 可以非常方便的表示出这个方程的解：

$$x(t) = e^{At}x(0)$$

其中 $\mathrm{e}^{At}\mathrm{t}{=}0 Rodrigues' formula \mathrm{e}^{At}$，将在后文进行重点介绍

9.2 主成分分析

基础知识：

1. 内积与范数

对于实向量 $\mathbf{x}$ 和向量 $\mathbf{y}$

1. 向量 $\mathbf{x}$ 和向量 $\mathbf{y}$ 的内积

$$\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^T\mathbf{y} = \sum_{i=1}^{n} x_i y_i$$

向量 $\mathbf{x}$ 的**范数**

- L_0 范数 (也称 0 范数)

$\|\mathbf{x}\|_0$ 定义为 $\mathbf{x}$ 中非零元的个数 L_0 范数是稀疏性的最直接优化目标，但是由于其不可导，工程上一般选用 L_1 范数作为替代。

- L_1 范数 (也称和范数或 1 范数)

$$\|\mathbf{x}\|_1 = \sum_{i=1}^{n} |x_i|$$

- L_2 范数 (也称欧氏范数或 2 范数)

$\|\mathbf{x}\|_2 = \left(\sum_{i=1}^{n} |x_i|^2\right)^{1/2}$

- L_∞ 范数 (也称无穷范数)

$\|\mathbf{x}\|_\infty = \max\{|x_1|, |x_2|, \ldots, |x_n|\}$

- L_p 范数 (也称 Hölder 范数)

$\|\mathbf{x}\|_p = \left(\sum_{i=1}^{n} |x_i|^p\right)^{1/p}, \quad p \geq 1$

---

1. 协方差和协方差矩阵

   注意：此处的样本 $\mathbf{X}$ 和样本 $\mathbf{Y}$，向量中每一个维度事实上都是对同一个随机变量的采样，而不是多个随机变量的向量化书写。（关于随机变量的内容，请参考概率论资料）。这个区分是十分重要的，且十分容易混淆。这关乎到

对于样本 $\mathbf{X} = [x_1, x_2, \ldots, x_n]^T$ 和样本 $\mathbf{Y} = [y_1, y_2, \ldots, y_n]^T$：

- **1. 样本均值**

$$\bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i$$

- **2. 样本方差**

$$S^2 = \frac{1}{n-1} \sum_{i=1}^{n} (x_i - \bar{x})^2$$

- **3. 样本 X 和 Y 的协方差**

$$\mathrm{Cov}(X,Y)=\frac{1}{n-1}\sum_{i=1}^{n-1}(x_i-\bar{x})(y_i-\bar{y})$$

- **4. 协方差矩阵**

设共有 p 个特征（随机变量），每个特征有 n 个观测样本。若 $\mathbf{x}_i$ 与 $\mathbf{x}_j$ 的协方差为：

$$s_{ij}=\mathrm{Cov}(\mathbf{x}_i,\mathbf{x}_j)=\frac{1}{n}\sum_{k=1}^{n}(x_{ik}-\bar{x}_i)(x_{jk}-\bar{x}_j)$$

则其**协方差矩阵**定义为：

$$\mathbf{S}=(s_{ij})_{p\times p}=$$

$$\begin{bmatrix} s_{11} & s_{12} & \cdots & s_{1p} \\ s_{21} & s_{22} & \cdots & s_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ s_{p1} & s_{p2} & \cdots & \end{bmatrix}$$

根据上述定义，有

$$\begin{aligned}\mathbf{S}=&\frac{1}{n-1}\left(\mathbf{x}_1-\mu_1\mathbf{1},\mathbf{x}_2-\mu_2\mathbf{1},\ldots,\mathbf{x}_p-\mu_p\mathbf{1}\right)^T\\&\times\left(\mathbf{x}_1-\mu_1\mathbf{1},\mathbf{x}_2-\mu_2\mathbf{1},\ldots,\mathbf{x}_p-\mu_p\mathbf{1}\right)\end{aligned}$$

在本课中记 $\mathbf{X}_0=(\mathbf{x}_1-\mu_1\mathbf{1},\mathbf{x}_2-\mu_2\mathbf{1},\ldots,\mathbf{x}_p-\mu_p\mathbf{1})$，从而有

$$\mathbf{S}=\frac{1}{n-1}\mathbf{X}_0^T\mathbf{X}_0$$

务必牢记 S 的矩阵形式。

---

1. 相关系数和相关矩阵

对于向量 $\mathbf{x}$ 和向量 $\mathbf{y}$

- 1) 向量 $\mathbf{x}$ 的标准化

$$\mathbf{x}'=\frac{\mathbf{x}-\bar{x}\mathbf{1}}{\langle\mathbf{x}-\bar{x}\mathbf{1},\mathbf{x}-\bar{x}\mathbf{1}\rangle^{1/2}}=\frac{\mathbf{x}-\bar{x}\mathbf{1}}{\|\mathbf{x}-\bar{x}\mathbf{1}\|}$$

- 2) 向量 $\mathbf{x}$ 和向量 $\mathbf{y}$ 的相关系数

$$r(\mathbf{x},\mathbf{y})=\langle\mathbf{x}',\mathbf{y}'\rangle$$

- 3) 两个向量 $\mathbf{x}$ 和 $\mathbf{y}$ 之间的夹角 θ

$$\cos\theta = \frac{\langle \mathbf{x}, \mathbf{y} \rangle}{\sqrt{\langle \mathbf{x}, \mathbf{x} \rangle \langle \mathbf{y}, \mathbf{y} \rangle}}$$

$$r(\mathbf{x}, \mathbf{y}) = \langle \mathbf{x}', \mathbf{y}' \rangle = \left\langle \frac{\mathbf{x} - \bar{x}\mathbf{1}}{\|\mathbf{x} - \bar{x}\mathbf{1}\|}, \frac{\mathbf{y} - \bar{y}\mathbf{1}}{\|\mathbf{y} - \bar{y}\mathbf{1}\|} \right\rangle$$
$$= \frac{\langle \mathbf{x} - \bar{x}\mathbf{1}, \mathbf{y} - \bar{y}\mathbf{1} \rangle}{\|\mathbf{x} - \bar{x}\mathbf{1}\| \|\mathbf{y} - \bar{y}\mathbf{1}\|} = \cos\gamma$$

γ 为向量 $\mathbf{x} - \bar{x}\mathbf{1}$ 与 $\mathbf{y} - \bar{y}\mathbf{1}$ 之间的夹角。

向量之间的相关性与加减 $\beta\mathbf{1}$ 无关，即均值的平移并不改变相关性。

- 4) 设有向量 $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$，若 $r(\mathbf{x}_i, \mathbf{x}_j) = r_{ij}$，则

$$\mathbf{R} = (r_{ij})_{n \times n} = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nn} \end{bmatrix}$$

称为向量 $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ 的相关矩阵。

> **辨析：**考试中，若问两向量的**余弦相似度**，那么自不必辨析，但是如果问**相关系数**，那么就需要理解，向量是同一个**标量**随机变量的 n 次采样，而非一个随机向量的单次采样。这一辨析同样适用于前文的方差与协方差部分

主成分分析：

主成分分析是一种数据降维的方法。

什么是数据降维呢？比如说对于 Person X，他有十个统计量，都是关于身体指标的，分别是 X_1（体重），X_2（身高），$X_3, X_4, ..., X_{10}$，但显然身高和体重或和其他指标显然是有一定相关性的。我们就可以考虑把他们通过组合来造出较少量的新统计量，那么就可以用更少的数据表示更多的数据。这就是数据降维。

因此需要找到一种合理的方法，在减少需要分析的变量同时，尽量减少原指标包含信息的损失，从而达到对所收集数据进行全面分析的目的。

* 主成分分析 * 就是把原有的多个指标转化成少数几个代表性较好的综合指标，这少数几个指标能够反应原来指标大部分的信息，并且各个指标之间保持独立，避免出现重叠信息。这些综合指标就称为主成分。

理论依据：* 最大方差理论 *，即将 p 维样本点转换为 k 维后 $(1 \leq k < p)$，每一维上的样本方差都应尽可能大。

形式化（formalization）：给定有 p 个统计相关的属性组合 $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \ldots, \mathbf{x}_p$，求得 k 个零均值的新特征集合 $(k < p)$，$\tilde{\mathbf{x}}_1, \tilde{\mathbf{x}}_2, \cdots, \tilde{\mathbf{x}}_k$ 使这些新特征相互正交。由于我们的目标函数是方差，所以平均值并不会影响方差的计算。为了简化计算，我们对 $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \ldots, \mathbf{x}_p$ 进行零均值化。记 $\mathbf{X}_0 = (\mathbf{x}_1 - \mu_1\mathbf{1}, \mathbf{x}_2 - \mu_2\mathbf{1}, \ldots, \mathbf{x}_p - \mu_p\mathbf{1})$。新特征记为 $\tilde{\mathbf{X}} = (\tilde{\mathbf{x}}_1, \tilde{\mathbf{x}}_2, \cdots, \tilde{\mathbf{x}}_k)$，即求矩阵 C。

由于主成分分析的每一个新特征，都是通过旧特征的线性组合构成的。那么 $\tilde{\mathbf{X}} = \mathbf{X}_0 C$，其中 C 为 $(c_1, c_2, \ldots, c_k)$. 那么 $\tilde{\mathbf{x}}_i = \mathbf{X}_0 c_i, (i = 1, 2, \ldots, k)$

老师讲的版本是按照单个维度进行推导的，但笔者认为或许用矩阵形式来推导会更易懂一些。矩阵形式可以直接得出 k 个新特征的情况。

目标函数：k 维的方差都最大化。即 k 维方差和最大。故最大化：

$$max \sum S^2(\tilde{\mathbf{x}}_i) = \frac{1}{n-1} \sum_{i=1}^{n} \tilde{\mathbf{x}}_i^T \tilde{\mathbf{x}}_i = \frac{1}{n-1} \sum_{i=1}^{n} c_i^T \mathbf{X}_0^T \mathbf{X}_0 c_i = \frac{1}{n-1} \mathbf{tr}(C^T \mathbf{X}_0^T \mathbf{X}_0 C)$$

记 $\mathbf{S} = \mathbf{X}_0^T \mathbf{X}_0$，$\mathbf{S}$ 为常量，为实对称矩阵.

故只需最大化：$\mathbf{tr}(C^T \mathbf{S} C)$

> 这里没那么严谨，需要更严谨一下。

我们如果对于 c_i 进行缩放，并不会影响 $\tilde{\mathbf{x}}_i$ 方差的最大性，故不妨令 $\|c_i\|$=1。又因为我们要求新特征互相正交，即 $c_j^T c_i = 0$. 那么这时，C 会获得一种很好的性质：$C^T C = I$。

这就是有约束条件的极大值求解。为了解决这类问题，我们引入一个对称的拉格朗日乘子矩阵 $\Lambda \in \mathbb{R}^{k \times k}$，（即 Λ 仅在主对角线上有非零元素）

令：

$$\mathcal{L}(C, \Lambda) = \mathbf{tr}(C^T \mathbf{S} C) - \mathbf{tr}\left(\Lambda (C^T C - I)\right)$$

利用矩阵微分公式 $\frac{\partial \mathbf{tr}(C^T \mathbf{A} C)}{\partial C} = (\mathbf{A} + \mathbf{A}^T) C$，以及 $\mathbf{S}$ 和 Λ 的对称性，我们对 C 求偏导：

$$\frac{\partial \mathcal{L}}{\partial C} = 2\mathbf{S}C - 2C\Lambda$$

令偏导数为 0：

$$2\mathbf{S}C - 2C\Lambda = 0 \implies \mathbf{S}C = C\Lambda$$

这正是标准的特征值问题的矩阵形式，且 Λ 中的每一个主对角元素都是 S 的特征值。

把上式两边同时左乘 C^T，利用 $C^T C = I$ 可得：

$$C^T \mathbf{S} C = \Lambda$$

代回我们的目标函数：

$$\mathbf{tr}(C^T \mathbf{S} C) = \mathbf{tr}(\Lambda) = \sum_{i=1}^{k} \lambda_i$$

要让总方差（迹）最大化，λ_i 必须是矩阵 $\mathbf{S}$（即协方差矩阵）的前 k 个最大的特征值。而矩阵 $C = (c_1, c_2, \ldots, c_k)$ 的每一列，就是这前 k 个最大特征值所对应的特征向量。

一个小 tip：S 的所有特征值一定是非负的。

> 这里其实需要解释一下为什么的，但是我忽然不想写了。懒（

上面说的都是 S 型分析，如果想要改成 R 型分析，只需要将一开始的零均值化过程改为标准化。这就意味着新的 Λ 中的元素均为标准化后的 $\mathbf{R} = \mathbf{X}_0'^T\mathbf{X}'_0$

呼，PCA 终于完结了！

PCA 计算例题：

下表为 10 位同学的身高 (x_1, cm)、胸围 (x_2, cm)、体重 (x_3, kg) 数据，使用 S 型分析求主成分。

表 9.1:

序号	身高 x_1	胸围 x_2	体重 x_3
1	149.5	69.5	38.5
2	162.5	77.0	55.5
3	162.7	78.5	50.8
4	162.2	87.5	65.5
5	156.5	74.5	49.0
6	156.1	74.5	45.5
7	172.0	76.5	51.0
8	173.2	81.5	59.5
9	159.5	74.5	43.5
10	157.7	79.0	53.5

解：

(1) 求样本均值：

$\bar{x}_1 = 161.19, \bar{x}_2 = 77.30, \bar{x}_3 = 51.23$

(2) 零均值化数据（每列减去对应均值），得 $\mathbf{X}_0$

(3) 求协方差矩阵（使用 $1/n$ 形式）：

$$\mathbf{S} = \frac{1}{10}\mathbf{X}_0^T\mathbf{X}_0 = \begin{bmatrix} 46.57 & 17.09 & 30.98 \\ 17.09 & 21.11 & 32.58 \\ 30.98 & 32.58 & 55.53 \end{bmatrix}$$

(4) 求 S 的特征值和特征向量：

解 $|\lambda\mathbf{I} - \mathbf{S}| = 0$，得：

- $\lambda_1 = 99.00$，对应单位特征向量 $\boldsymbol{\omega}_1$
- $\lambda_2 = 22.79$，对应单位特征向量 $\boldsymbol{\omega}_2$
- $\lambda_3 = 1.41$，对应单位特征向量 $\boldsymbol{\omega}_3$

(5) 计算贡献率：

总方差 = $\lambda_1 + \lambda_2 + \lambda_3 = 123.21$

- 第一主成分贡献率：$99.00/123.21 = 80.4\%$
- 第二主成分贡献率：$22.79/123.21 = 18.5\%$
- 第三主成分贡献率：$1.41/123.21 = 1.1\%$

- 前两个主成分**累计贡献率** = $80.4\% + 18.5\% = 98.9\%$

(6) 写出主成分表达式：

$$y_1 = \boldsymbol{\omega}_1^T \tilde{\mathbf{x}}, \quad y_2 = \boldsymbol{\omega}_2^T \tilde{\mathbf{x}}$$

其中 $\tilde{\mathbf{x}} = [x_1 - \bar{x}_1, x_2 - \bar{x}_2, x_3 - \bar{x}_3]^T$ 为零均值化后的数据。

> **解读：**前两个主成分已经能解释 98.9% 的总方差——这意味着原来 3 维的数据几乎可以用 2 维新特征无损表示。这就是 PCA 降维的威力。
>
> **考试 tip：**如果题目要求 R 型分析，只需在第 (3) 步之前先对原始数据做 Z-score 标准化（$(x - \bar{x})/s$），然后用相关系数矩阵 $\mathbf{R}$ 代替协方差矩阵 $\mathbf{S}$，其余步骤完全相同。另外注意考试中 $\mathbf{S}$ 的分母是 $1/n$ 还是 $1/(n-1)$ 不影响特征向量的方向，因此对主成分表达式无影响。

9.3 奇异值分解 (Singular Value Decomposition)

> 我暂时懒得写推导了。听说 SVD 就考个计算???

假设矩阵 A 是一个 $m \times n$ 的矩阵，那么定义矩阵 A 的 SVD 为：$A = U\Sigma V^T$

其中 U 是一个 $m \times m$ 的矩阵，Σ 是一个 $m \times n$ 的矩阵，并且除了

主对角线上的元素以外全为 0，主对角线上的每个元素都称为

奇异值，V 是一个 $n \times n$ 的矩阵。U 和 V 都是酉矩阵，即满足：

$U^T U = I, V^T V = I$

奇异值分解同样是一种数据降维的方式。它可以用于数据压缩等广泛领域。

这里我们直接以题带点：

计算下面矩阵的 SVD：

$$A = \begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

解：这道题的矩阵大小为 3×4，我们要对它进行奇异值分解（SVD），即求出 $A = U\Sigma V^T$。

第一步：计算 AA^T 并求其特征值与特征向量（构造 U 和 Σ）

因为 A 是 3×4 矩阵，AA^T 是 3×3 矩阵，计算量更小。

$$AA^T = \begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ -1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & -1 & 0 \\ -1 & 2 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

计算特征方程 $\det(\lambda I - AA^T) = 0$：

$$\det \begin{bmatrix} \lambda-2 & 1 & 0 \\ 1 & \lambda-2 & 0 \\ 0 & 0 & \lambda \end{bmatrix} = \lambda\left[(\lambda-2)^2 - 1\right] = \lambda(\lambda-3)(\lambda-1) = 0$$

解得特征值（按从大到小排序）：

$$\lambda_1 = 3, \quad \lambda_2 = 1, \quad \lambda_3 = 0$$

- **奇异值**（$\sigma = \sqrt{\lambda}$）：$\sigma_1 = \sqrt{3}$，$\sigma_2 = 1$。
- **构造 Σ 矩阵**（大小与 A 一致，即 3×4）：

$$\Sigma = \begin{bmatrix} \sqrt{3} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

接下来求 AA^T 的单位特征向量以构造 U：

- 对于 $\lambda_1 = 3$，解 $(3I - AA^T)u_1 = 0$，得单位特征向量：$u_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}$
- 对于 $\lambda_2 = 1$，解 $(1I - AA^T)u_2 = 0$，得单位特征向量：$u_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$
- 对于 $\lambda_3 = 0$，解 $(0I - AA^T)u_3 = 0$，得单位特征向量：$u_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$

由此得到左奇异矩阵 U：

$$U = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

第二步：计算右奇异矩阵 V

注意：为了保证 U 和 V 的符号匹配，非零奇异值对应的 v_i 必须通过 $v_i = \frac{1}{\sigma_i} A^T u_i$ 来计算。

- 计算 v_1：

$$v_1 = \frac{1}{\sqrt{3}} A^T u_1 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ -1 & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} = \frac{1}{\sqrt{6}} \begin{bmatrix} 1 \\ -1 \\ 0 \\ -2 \end{bmatrix}$$

- 计算 v_2：

$$v_2 = \frac{1}{1}A^T u_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ -1 & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

由于 V 需要是 4×4 的正交矩阵，我们还需要补齐对应 $\sigma=0$ 的空间（即 A 的零空间）。通过解 $Av=0$ 并正交归一化，或者直接观察法补齐：

- $v_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$ （显然与 v_1, v_2 正交且 $Av_3=0$）
- $v_4 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ -1 \\ 0 \\ 1 \end{bmatrix}$ （与 v_1, v_2, v_3 均正交且 $Av_4=0$）

由此得到右奇异矩阵 V：

$$V = \begin{bmatrix} \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{3}} \\ -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{3}} \\ 0 & 0 & 1 & 0 \\ -\frac{2}{\sqrt{6}} & 0 & 0 & \frac{1}{\sqrt{3}} \end{bmatrix}$$

最后，矩阵 A 的 SVD 分解结果 $A=U\Sigma V^T$ 为：

$$A = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \sqrt{3} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{6}} & 0 & -\frac{2}{\sqrt{6}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} & 0 & \frac{1}{\sqrt{3}} \end{bmatrix}$$

SVD 计算与书写的**核心注意事项**

手动推导 SVD 是考研和期末考试的传统手艺，极其容易在细节上翻车。请务必注意以下几点：

1. 符号对齐问题（最容易翻车的地方）

- 你**不能**独立去求 AA^T 的特征向量和 A^TA 的特征向量。因为特征向量的方向（正负号）是任意的，如果两边各自盲目决定正负号，最后乘起来 $U\Sigma V^T$ 就会差一个负号。
- **正确做法：**先求出 U（或 V），然后通过关系式 $v_i = \frac{1}{\sigma_i}A^T u_i$ 算出来另一方的非零部 * 分。这样能百分之百保证符号自适应对齐。

1. Σ 的尺寸和填充

- Σ 的维数必须与原矩阵 A **完全一致**。如果 A 是 3×4，Σ 必须写成 3×4。
- 很多人习惯只把非零奇异值写成对角矩阵，忘了在外围补零行或零列，这会导致矩阵乘法直接无法进行。

1. 奇异值的排序

- 奇异值必须按照**从大到小**的顺序在 Σ 的对角线上排列（$\sigma_1\geq\sigma_2\geq\cdots\geq0$）。
- 与之对应的 U 的列向量和 V 的列向量，也必须严格按照这个顺序排座位，绝对不能错位。

1. 补齐正交基（零空间的处理）

- 当 A 不是方阵时，非零奇异值算完后，U 或 V 往往还空着几列（对应 $\sigma=0$ 的部分）。
- 剩下的列必须通过解齐次线性方程组（或施密特正交化）补齐，确保 U 是 $m\times m$、V 是 $n\times n$ 的**标准正交矩阵**（每列模长为 1，且两两垂直）。

1. 别忘了转置

- 最后的答案公式是 $A=U\Sigma V^T$。在纸上写出最终结果时，第 3 个矩阵是 V **的转置矩阵**，写完后可以挑第一行第一列心算乘一下，看看能不能还原出 A_{11}，以此确保万无一失。

9.3.1 SVD 专项练习题

以下 10 道题覆盖了 SVD 计算中所有关键细节：特征值求法、Σ 的尺寸、U 和 V 的补齐、符号对齐、秩与四个基本子空间的关系。老师不会在数字上为难你——重点在于每一步的**操作逻辑**是否清晰。

第 1 题（热身）：$A=\begin{bmatrix}3&0\\0&1\end{bmatrix}$，直接写出 SVD。

解：A 已是对角阵且对角元为正，$U=V=I_2$，$\Sigma=A$。$\sigma_1=3,\sigma_2=1$。

第 2 题（矩形阵——选小的那边先算）：$A=\begin{bmatrix}1&0&1\\0&2&0\end{bmatrix}$，求奇异值和秩。

解：AA^T 是 2×2（比 3×3 的 A^TA 小），先算 $AA^T=\begin{bmatrix}2&0\\0&4\end{bmatrix}$。特征值 $4,2$，故 $\sigma_1=2,\sigma_2=\sqrt{2}$。非零奇异值个数 = 秩 = 2。

第 3 题（特征向量符号对齐——关键！）：$A=\begin{bmatrix}2&1\\1&2\\1&-1\end{bmatrix}$，完整 SVD。

解：$A^TA=\begin{bmatrix}6&3\\3&6\end{bmatrix}$，特征值 $\lambda_1=9,\lambda_2=3$，$\sigma_1=3,\sigma_2=\sqrt{3}$。

V：$v_1=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$，$v_2=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$。

U 的前两列通过 $u_i=\frac{1}{\sigma_i}Av_i$ 计算（**不是**独立解 AA^T 的特征向量！）：

$u_1 = \frac{1}{3\sqrt{2}} \begin{bmatrix} 3 \\ 3 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$，

$u_2 = \frac{1}{\sqrt{6}} \begin{bmatrix} 1 \\ -1 \\ 2 \end{bmatrix}$。

u_3 补齐：解 $u_3 \perp u_1, u_2$ 且 $\|u_3\| = 1$，得 $u_3 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ -1 \\ -1 \end{bmatrix}$。$\Sigma$ 为 3×2。

第 4 题（秩 1 矩阵——结构比计算更重要）： $A = \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}$，完整 SVD。

解： $A^TA = \begin{bmatrix} 0 & 0 \\ 0 & 4 \end{bmatrix}$，$\lambda_1 = 4, \lambda_2 = 0$，$\sigma_1 = 2$。$v_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, v_2 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$。$u_1 = \frac{1}{2}Av_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$，$u_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$。

$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^T$。

> **技巧：** 秩 1 矩阵的 SVD 只有一个非零奇异值，V 的补全就是 A^TA 的零特征向量（通常可以一眼看出）。

第 5 题（V 的补全——零空间）： $A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$，完整 SVD。

解： $AA^T = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$，$\sigma_1 = \sqrt{2}, \sigma_2 = 1$。$U = I_2$。$v_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$，$v_2 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$。$v_3$ 满足 $Av_3 = 0$ 且 $\|v_3\| = 1$：

解 $\begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} x = 0$ 得 $v_3 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}$。$V$ 是 3×3 正交阵。

第 6 题（四个基本子空间）： 给出 SVD 的对角元 $\sigma_1 = 5, \sigma_2 = 2, \sigma_3 = 0$（$4 \times 3$ 矩阵），写出各基本子空间的基。

解： 秩 $r = 2$。$\text{Col}(A) = \text{span}\{u_1, u_2\}$，$\text{Null}(A^T) = \text{span}\{u_3, u_4\}$，$\text{Row}(A) = \text{span}\{v_1, v_2\}$，$\text{Null}(A) = \text{span}\{v_3\}$。验证秩-零化度：$2 + 1 = 3$，$2 + 2 = 4$。

第 7 题（秩 1 矩阵——外积形式）： $A = \boldsymbol{a}\boldsymbol{b}^T$，$\boldsymbol{a} = \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}, \boldsymbol{b} = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$，求 SVD。

解： $\sigma_1 = \|\boldsymbol{a}\| \cdot \|\boldsymbol{b}\| = 3 \times 5 = 15$。$v_1 = \frac{\boldsymbol{b}}{\|\boldsymbol{b}\|} = \frac{1}{5} \begin{bmatrix} 3 \\ 4 \end{bmatrix}$，$u_1 = \frac{\boldsymbol{a}}{\|\boldsymbol{a}\|} = \frac{1}{3} \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}$。补全 $v_2 = \frac{1}{5} \begin{bmatrix} 4 \\ -3 \end{bmatrix}$，$u_2, u_3$ 为与 u_1 正交的任意标准正交基。

第 8 题（正交投影——SVD 的应用）： $A=\begin{bmatrix}1&0\\0&1\\1&1\end{bmatrix}$，求 $\mathrm{Col}(A)$ 上的正交投影矩阵。

解： $\sigma_1=\sqrt{3},\sigma_2=1$。$u_1=\frac{1}{\sqrt{6}}\begin{bmatrix}1\\1\\2\end{bmatrix}$，$u_2=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\\0\end{bmatrix}$。投影矩阵 $P=u_1u_1^T+u_2u_2^T$，满足 $P^2=P,P^T=P$。

第 9 题（最佳秩-k 近似）： $A=\begin{bmatrix}3&0\\0&2\end{bmatrix}$，求最佳秩 1 近似 A_1 及误差。

解： SVD 即 A 本身（已对角）。最大奇异值 $\sigma_1=3$，$A_1=3\begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1&0\end{bmatrix}=\begin{bmatrix}3&0\\0&0\end{bmatrix}$。误差 $\|A-A_1\|_F=\sigma_2=2$。

第 10 题（低秩近似——能量解释）： 已知 $\sigma_1=10,\sigma_2=6,\sigma_3=2,\sigma_4=1$。求：(1) $\|A\|_F^2$，(2) 秩 2 近似捕捉的能量百分比。

解： (1) $\|A\|_F^2=\sum\sigma_i^2=100+36+4+1=141$。(2) 前两个分量贡献 $100+36=136$，占比 $136/141\approx 96.5\%$。这意味着用秩 2 近似就几乎不失真地保留了原矩阵的信息——这正是 PCA 和图像压缩的数学基础。

9.4 【重点】函数矩阵的求导

> 注意：本节（9.4）与下面 9.5 节的" 矩阵求导" 是**两个完全不同的概念**。9.4 节讨论的是矩阵的元素是标量 x 的函数——即 $\boldsymbol{A}(x)=[a_{ij}(x)]$，求的是对 x 的导数 $\frac{d\boldsymbol{A}}{dx}$。而 9.5 节讨论的是标量/向量值函数对**矩阵变元**的导数 $\frac{\partial f}{\partial \boldsymbol{X}}$——求导方向和对象完全不同，不要混淆。

9.4.1 函数矩阵的定义

定义： 以变量 x 的函数 $a_{ij}(x)$ 为元素构成的矩阵称为**函数矩阵**：

$$\boldsymbol{A}(x)=\begin{bmatrix}a_{11}(x)&a_{12}(x)&\cdots&a_{1n}(x)\\a_{21}(x)&a_{22}(x)&\cdots&a_{2n}(x)\\\vdots&\vdots&\ddots&\vdots\\a_{m1}(x)&a_{m2}(x)&\cdots&\end{bmatrix}$$

函数矩阵的运算性质（加法、数乘、乘法、转置等）与常数矩阵**完全相同**。

定义： 设 $\boldsymbol{A}(x)$ 为 n 阶函数矩阵，如果存在 n 阶函数矩阵 $\boldsymbol{B}(x)$ 使得

$$\boldsymbol{A}(x)\boldsymbol{B}(x)=\boldsymbol{B}(x)\boldsymbol{A}(x)=\boldsymbol{I}$$

则称 $\boldsymbol{A}(x)$ 在该区间上**可逆**，$\boldsymbol{B}(x)$ 是 $\boldsymbol{A}(x)$ 的逆矩阵，记作 $\boldsymbol{A}^{-1}(x)$。

> 函数矩阵的求逆与常数矩阵完全类似——伴随矩阵法、初等变换法都适用，只是结果中每个元素都是 x 的函数。

例：求函数矩阵 $\boldsymbol{A}(x)=\begin{bmatrix}x & x^2\\ 2 & 4x\end{bmatrix}$ 的逆矩阵。

解：$\det(\boldsymbol{A}(x))=x\cdot 4x-x^2\cdot 2=4x^2-2x^2=2x^2$（当 $x\neq 0$ 时可逆）。

伴随矩阵：$\operatorname{adj}(\boldsymbol{A})=\begin{bmatrix}4x & -x^2\\ -2 & x\end{bmatrix}$

$$\boldsymbol{A}^{-1}(x)=\frac{1}{2x^2}\begin{bmatrix}4x & -x^2\\ -2 & x\end{bmatrix}=\begin{bmatrix}\frac{2}{x} & -\frac{1}{2}\\ -\frac{1}{x^2} & \frac{1}{2x}\end{bmatrix}$$

9.4.2 函数矩阵的导数

定义：若函数矩阵 $\boldsymbol{A}(x)$ 的所有元素 $a_{ij}(x)$ 在区间 $[a,b]$ 上对 x 处处可导，则称 $\boldsymbol{A}(x)$ 在该区间上对 x **可导**，其导数为逐元素求导：

$$\frac{d\boldsymbol{A}(x)}{dx}=\begin{bmatrix}\frac{da_{11}(x)}{dx} & \frac{da_{12}(x)}{dx} & \cdots & \frac{da_{1n}(x)}{dx}\\ \frac{da_{21}(x)}{dx} & \frac{da_{22}(x)}{dx} & \cdots & \frac{da_{2n}(x)}{dx}\\ \vdots & \vdots & \ddots & \vdots\\ \frac{da_{m1}(x)}{dx} & \frac{da_{m2}(x)}{dx} & \cdots & \end{bmatrix}$$

> 本质上就是把矩阵的每个元素分别求导，然后按原位置放回去。没有任何玄机。

例：求 $\boldsymbol{A}(x)=\begin{bmatrix}\sin x & x^2\\ e^x & \ln x\end{bmatrix}$ 对 x 的导数。

解：

$$\frac{d\boldsymbol{A}(x)}{dx}=\begin{bmatrix}\cos x & 2x\\ e^x & \frac{1}{x}\end{bmatrix}$$

9.4.3 函数矩阵导数的运算性质

函数矩阵导数运算与普通函数求导法则高度一致：

(1) 常数矩阵的导数为零矩阵：若 $\boldsymbol{A}$ 是常数矩阵，则 $\frac{d\boldsymbol{A}}{dx}=\boldsymbol{O}$。

(2) 线性性： $\frac{d}{dx}(\boldsymbol{A}+\boldsymbol{B})=\frac{d\boldsymbol{A}}{dx}+\frac{d\boldsymbol{B}}{dx}$

(3) 数乘： $\frac{d}{dx}(k\boldsymbol{A})=\frac{dk}{dx}\boldsymbol{A}+k\frac{d\boldsymbol{A}}{dx}$

(4) 乘法法则（重要！注意顺序不可交换）：

$$\frac{d}{dx}(\boldsymbol{A}(x)\boldsymbol{B}(x))=\frac{d\boldsymbol{A}(x)}{dx}\boldsymbol{B}(x)+\boldsymbol{A}(x)\frac{d\boldsymbol{B}(x)}{dx}$$

(5) 逆矩阵的导数（高频考点）：

$$\frac{d}{dx}(\boldsymbol{A}^{-1}(x))=-\boldsymbol{A}^{-1}(x)\frac{d\boldsymbol{A}(x)}{dx}\boldsymbol{A}^{-1}(x)$$

证明：由 $\boldsymbol{A}(x)\boldsymbol{A}^{-1}(x)=\boldsymbol{I}$，两边对 x 求导：

$$\frac{d\boldsymbol{A}}{dx}\boldsymbol{A}^{-1}+\boldsymbol{A}\frac{d\boldsymbol{A}^{-1}}{dx}=\boldsymbol{O}$$

移项得 $\boldsymbol{A}\frac{d\boldsymbol{A}^{-1}}{dx}=-\frac{d\boldsymbol{A}}{dx}\boldsymbol{A}^{-1}$，左乘 $\boldsymbol{A}^{-1}$ 即得证。

例（两种方法对比）：求 $\boldsymbol{A}(x)=\begin{bmatrix}x & 1\\ 1 & x+1\end{bmatrix}$ 的逆矩阵的导数。

法一（直接法）：先求逆再求导。$\det(\boldsymbol{A}(x))=x(x+1)-1=x^2+x-1$。

$$\boldsymbol{A}^{-1}(x)=\frac{1}{x^2+x-1}\begin{bmatrix}x+1 & -1\\ -1 & x\end{bmatrix}$$

再逐元素求导（过程略）。

法二（利用性质 (5)）：

$$\frac{d\boldsymbol{A}}{dx}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$

$$\frac{d\boldsymbol{A}^{-1}}{dx}=-\boldsymbol{A}^{-1}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\boldsymbol{A}^{-1}=-(\boldsymbol{A}^{-1})^2$$

法二简洁得多！这正是这些性质的威力——它们让你可以像处理标量函数一样处理矩阵函数的导数。

9.4.4 函数矩阵的高阶导数与积分

高阶导数就是逐元素反复求导：

$$\frac{d^k \boldsymbol{A}(x)}{dx^k} = \left[\frac{d^k a_{ij}(x)}{dx^k}\right]$$

函数矩阵的积分也是逐元素的：

$$\int_a^b \boldsymbol{A}(x)dx = \left[\int_a^b a_{ij}(x)dx\right]$$

9.5 【重点】矩阵求导（梯度与 Jacobian）

9.5.1 符号统一

- $\boldsymbol{x} = [x_1, \ldots, x_n]^T \in \mathbb{R}^n$ 为实向量变元;
- $\boldsymbol{X} = [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m] \in \mathbb{R}^{n\times m}$ 为实矩阵变元;
- $f(\boldsymbol{x}) \in \mathbb{R}$ 为实值标量函数，其变元为 $n \times 1$ 实值向量 $\boldsymbol{x}$，记作 $f : \mathbb{R}^n \to \mathbb{R}$;
- $f(\boldsymbol{X}) \in \mathbb{R}$ 为实值标量函数，其变元为 $n \times m$ 实值矩阵 $\boldsymbol{X}$，记作 $f : \mathbb{R}^{n\times m} \to \mathbb{R}$;
- $\boldsymbol{f}(\boldsymbol{x}) \in \mathbb{R}^p$ 为 p 维实列向量函数，其变元为 $n \times 1$ 实值向量 $\boldsymbol{x}$，记作 $\boldsymbol{f} : \mathbb{R}^n \to \mathbb{R}^p$;
- $\boldsymbol{f}(\boldsymbol{X}) \in \mathbb{R}^p$ 为 p 维实列向量函数，其变元为 $n \times m$ 实值矩阵 $\boldsymbol{X}$，记作 $\boldsymbol{f} : \mathbb{R}^{n\times m} \to \mathbb{R}^p$;
- $\boldsymbol{F}(\boldsymbol{x}) \in \mathbb{R}^{p\times q}$ 为 $p \times q$ 维实列向量函数，其变元为 $n \times 1$ 实值向量 $\boldsymbol{x}$，记作 $\boldsymbol{F} : \mathbb{R}^n \to \mathbb{R}^{p\times q}$;
- $\boldsymbol{F}(\boldsymbol{X}) \in \mathbb{R}^{p\times q}$ 为 $p\times q$ 维实列向量函数,其变元为 $n\times m$ 实值矩阵 $\boldsymbol{X}$,记作 $\boldsymbol{F} : \mathbb{R}^{n\times m} \to \mathbb{R}^{p\times q}$.

9.5.2 矩阵求导的本质

首先我们来谈谈矩阵求导的本质：实际上它是一个向量值函数对多个变元进行求导的过程。也就是你完全可以先将矩阵展平之后再按照你最熟悉的方式进行求导，然后再按照矩阵维度的“摆放”规则来重新排列它们的位置。这样就完成了矩阵的求导。

老师在课上能够以 $\sum$ 来推导确实很厉害。这种方法虽然根本，但是在考试过程中非常容易绕晕。因此这里我们介绍一种基于矩阵微分和矩阵的迹的求导方式，可以避免繁琐的 $\sum$ 符号。

由于我们是人工智能专业的学生，为了适配后续的机器学习，这里我们使用梯度算子进行求导，使用**分母布局**（即梯度 $\nabla_X f$ 的形状与矩阵 X 完全一致）。

若使用 **Jacobian** 矩阵：$\nabla_X f(X) = D_X^T f(X)$ 二者为转置关系。

1. 微分与梯度的映射：

只要你能把标量函数 f 的全微分 df 整理成以下标准形式，就能直接“读出”梯度：

> 这里的 $\mathbf{d}X$ 或许会稍显陌生，不过如果把它按照我们所说的“矩阵求导的本质”理解，就会很容易的知道它只是一种把 X 中的各个变元的微分按照 X 的排列方式排列的微分矩阵。

表 9.2:

求导类型	全微分标准形式 ($df = \dots$)	梯度结果 ($\nabla f = \dots$)
对向量求导 ($x \in \mathbb{R}^n$)	$df = g^T dx$	$\nabla_x f = g$
对矩阵求导 ($X \in \mathbb{R}^{m \times n}$)	$df = \text{tr}(G^T dX)$	$\nabla_X f = G$

什么是迹（Trace）？ > $\text{tr}(A)$ 是矩阵对角线元素之和。在微分中，$\text{tr}(G^T dX)$ 的本质就是把 G 和 dX 对应位置的元素相乘再相加，完美对应了多元全微分的定义。这个法则我们在 9.1 中迹那部分知识点里面讲解过，如果不理解大家可以

为什么这里只提到标量函数 f 的求导，因为在及其学习中，我们的目标函数通常都是一个标量，而中间变量通常都是矩阵。本着实用主义，我们只做这些介绍。

---

2. 四种微分法则

求微分 dX 的法则和高中的标量求导几乎一模一样，且完美保持线性：

1. **加减法**：$d(X \pm Y) = dX \pm dY$
2. **乘法**：$d(XY) = (dX)Y + X(dY)$ *(注意：矩阵顺序绝对不能颠倒)*
3. **转置**：$d(X^T) = (dX)^T$
4. **逆矩阵（高频）**：$d(X^{-1}) = -X^{-1}(dX)X^{-1}$

---

3. 迹性质的妙用（用于凑出标准形式）

由于我们必须把 df 凑成 $\text{tr}(G^T dX)$（即 dX 必须在最右边，且左边整体取转置），我们需要用“迹”的性质来任意揉捏矩阵：

- **标量强转**：如果 a 是标量，它自己就等于自己的迹：$a = \text{tr}(a)$。* 这一条非常重要，它是标量函数对矩阵进行求导的 * “唯一” * 途径。我们后面使用例题来阐明其重要性。*
- **循环移位（最常用）**：$\text{tr}(ABC) = \text{tr}(BCA) = \text{tr}(CAB)$ *(只要保持圆周相对顺序不变，谁挪到开头/结尾都行)*。
- **转置不变**：$\text{tr}(A) = \text{tr}(A^T)$。

使用矩阵求导来推导最小二乘法

我们来求一个深度学习中极常见的损失函数梯度：$f = \|AX - B\|_F^2$（**矩阵形式**的最小二乘误差。可以认为是在解“超定方程” $AX = B$。另外注意这里是 **Frobenius 范数**，前面讲过），求对矩阵 X 的梯度。

- **准备工作**：利用矩阵范数性质展开为迹的形式：$f = \text{tr}\left((AX - B)^T (AX - B)\right)$

  这里实际上就是“标量强转”的妙用了。

9.5.2.1 Step 1: 整体求微分

$$df = d\left(\text{tr}((AX-B)^T(AX-B))\right)$$

把迹的符号和微分符号互换，用乘法法则：

$$df = \text{tr}\left(d(AX-B)^T \cdot (AX-B) + (AX-B)^T \cdot d(AX-B)\right)$$

因为 $d(AX-B) = A \cdot dX$，带入得：

$$df = \text{tr}\left((dX)^T A^T (AX-B) + (AX-B)^T A \cdot dX\right)$$

9.5.2.2 Step 2: 利用迹的性质合并同类项

对第一项整体取转置（迹保持不变）：$\left((dX)^T A^T (AX-B)\right)^T = (AX-B)^T A \cdot dX$。

发现两项一模一样！合并为：

$$df = \text{tr}\left(2(AX-B)^T A \cdot dX\right)$$

9.5.2.3 Step 3: 对比标准公式，直接读出答案

对比标准形式 $df = \text{tr}(G^T dX)$，此时 $G^T = 2(AX-B)^T A$。

两边取转置拿到 G（即梯度）：

$$\nabla_X f = G = 2A^T(AX-B)$$

推导结束。没有求和号，也没有下标混乱。足见此方法还是很清晰简洁的。当然，这里推荐大家还是要会求和符号法，因为这是最本质的写法。考试中也推荐大家使用求和符号法进行书写，但是可以使用这里的这种方法进行验算。

9.5.3 反向传播梯度分析

以我们 PPT 上的这个例子为例：目标函数 **minimize** $f(x,W) = \|Wx\|^2$

$$\nabla_x \mathbf{tr}(x^T W^T W x) = 2W^T W x$$

$$\nabla_W \mathbf{tr}(x^T W^T W x) = 2Wxx^T$$

这样就求出了对于 W, x 的梯度。

9.5.4 补充例题

【例 1】 设 $f(\boldsymbol{x}) = \boldsymbol{x}^T A \boldsymbol{x}$，其中 $A \in \mathbb{R}^{n\times n}$ 为常数矩阵，$\boldsymbol{x} \in \mathbb{R}^n$，求 $\nabla_{\boldsymbol{x}} f$。

解（迹方法）：

求全微分：$df = d(\boldsymbol{x}^T A \boldsymbol{x}) = d\boldsymbol{x}^T \cdot A\boldsymbol{x} + \boldsymbol{x}^T A \cdot d\boldsymbol{x}$

两项都是标量，转置第二项：$\boldsymbol{x}^T A d\boldsymbol{x} = (A^T \boldsymbol{x})^T d\boldsymbol{x}$

第一项也是标量，转置：$(d\boldsymbol{x}^T)(A\boldsymbol{x}) = (A\boldsymbol{x})^T d\boldsymbol{x}$（标量的转置等于自身）

故 $df = (A\boldsymbol{x})^T d\boldsymbol{x} + (A^T \boldsymbol{x})^T d\boldsymbol{x} = \boldsymbol{x}^T (A + A^T)^T d\boldsymbol{x}$

对比标准形式 $df = g^T d\boldsymbol{x}$，得：

$$\boxed{\nabla_{\boldsymbol{x}} f = (A + A^T)\boldsymbol{x}}$$

> 特别地，若 A 为对称矩阵（$A = A^T$），则 $\nabla_{\boldsymbol{x}}(\boldsymbol{x}^T A \boldsymbol{x}) = 2A\boldsymbol{x}$。这一结果在优化和机器学习中极其常见。

【例 2】 设 $f(X) = \text{tr}(X^T A X B)$，其中 $X \in \mathbb{R}^{m\times n}$，$A \in \mathbb{R}^{m\times m}$ 为对称矩阵，$B \in \mathbb{R}^{n\times n}$ 为常数矩阵，求 $\nabla_X f$。

解（迹方法）：

求全微分：$df = d\,\text{tr}(X^T A X B) = \text{tr}(d(X^T A X B))$

$$= \text{tr}(dX^T \cdot AXB + X^T A \cdot dX \cdot B)$$

处理第一项：利用 $\text{tr}(M^T) = \text{tr}(M)$，

$$\text{tr}(dX^T AXB) = \text{tr}((dX^T AXB)^T) = \text{tr}(B^T X^T A^T dX) = \text{tr}(B^T X^T A dX) \quad (\text{因} A^T = A)$$

处理第二项（用迹的循环移位把 dX 换到最右边）：

$$\text{tr}(X^T A \cdot dX \cdot B) = \text{tr}(BX^T A \cdot dX)$$

合并：

$$df = \text{tr}\left((B^T X^T A + B X^T A)\, dX\right) = \text{tr}\left((AX(B + B^T))^T dX\right)$$

对比标准形式 $df = \text{tr}(G^T dX)$，得：

$$\boxed{\nabla_X f = AX(B + B^T)}$$

若 $B = I$，则 $\nabla_X \text{tr}(X^T AX) = 2AX$，与例 1 的对称结果一致。

9.6 广义逆矩阵与最小二乘法

首先对于**广义逆矩阵**，顾名思义，它并非逆矩阵，但是具有某些性质，让我们能够把它叫做一个“逆矩阵”。PPT 上的分类没有那么清晰，我们这里给出一个笔者认为更合适的梳理顺序。

> 核心思想：按照方阵与非方阵来做同概念梳理，按照传统逆的不断被打破的性质来递进。

定义：满足 $LA = I$，但不满足 $AL = I$ 的矩阵 L 称为矩阵 A 的**左逆矩阵**。类似地，满足 AR=I，但不满足 RA=I 的矩阵 R 称为矩阵 A 的右逆矩阵。

> 由于我们 PPT 上给出的定义都是只满足单侧逆，所以可逆方阵的逆既非左逆，也非右逆。所以，只有这是最贴近“狭义逆矩阵”，即可逆方阵的逆矩阵，的“广义逆矩阵”。他们的共同要求是满秩。只不过对于方阵而言，其行秩 = 列秩 = 矩阵阶数。对于“胖矩阵”，它只有列满秩，所以只有右逆，无左逆；对于“高矩阵”，它只有左逆，无右逆。这里的“逆”，还尚且没有脱离相乘为单位矩阵 I 的桎梏。

左逆和**右逆**都不是唯一的（这里是）。但是，聪明的人类分别想到了一个看起来非常不错的，很直接的，又有着良好的性质和形式美感的左逆和右逆，取名叫做**左伪逆矩阵**和**右伪逆矩阵**。

它们两个具有良好的性质，不仅形式极其对称，更是各自优化问题中的“天选之子”。

1. **左伪逆矩阵（Left Pseudo-inverse）**

对于“高矩阵”（行数 $m >$ 列数 n 且列满秩），由于方程个数多于未知数，线性方程组 $Ax = b$ 通常无解（超定方程）。此时，我们定义左伪逆矩阵（通常记作 L）：

$$L = (A^T A)^{-1} A^T$$

显然，它满足 $LA = (A^T A)^{-1}(A^T A) = I_n$。核心性质：最小二乘最优解既然方程组无解，我们的目标是让预测残差的平方和最小，即 $\min \|Ax - b\|_2^2$。在几何上，这相当于把向量 b 正交投影到 A 的列空间中。而利用左伪逆得到的解 $\hat{x} = Lb$，恰恰就是这个唯一的最小二乘最优解。

这就是它为什么被放在“最小二乘法”这一节的核心原因。

1. **右伪逆矩阵（Right Pseudo-inverse）**

对于“胖矩阵”（行数 $m <$ 列数 n 且行满秩），由于未知数多于方程个数，线性方程组 $Ax = b$ 通常有无数个解（欠定方程）。此时，我们定义右伪逆矩阵（记作 R）：

$$R = A^T(AA^T)^{-1}$$

显然，它满足 $AR = (AA^T)(AA^T)^{-1} = I_m$。核心性质：最小范数（能量最低）解在无数个可行解中，我们往往希望找到一个最“干净”、冗余最少、消耗控制能量最低的解。右伪逆给出的解 $\hat{x} = Rb$，在所有能让方程成立的解中，其欧几里得范数 $\|x\|_2$ 是绝对最小的（即最省力、无冗余）。

> 从这里能看出左和右在解方程的时候它们的处理是不一样的，结果也是不一样的。**左伪逆矩阵**是通过左乘提供了一个“最好的近似解”，而右伪逆矩阵是通过对 x 进行代入，提供了庞大解空间中的一个“可行解”，且其 L2 范数最小。

1. **Moore-Penrose 广义逆（MP 逆）**

> 看到这里，细心的读者可能会问：如果矩阵既不方、也不满秩（比如一个不可逆的方阵，或者行列都不满秩的长方形矩阵），那该怎么办？这时候，“相乘等于单位阵 I”的桎梏就被彻底打破了。

数学家 Moore 和 Penrose 提出了更普遍的定义。对于任意一个矩阵 A，只要有一个矩阵 A^+ 能够同时满足以下四个代数条件（称为彭罗斯条件），它就被称为 Moore-Penrose 伪逆：

- $AA^+A = A$
- $A^+AA^+ = A^+$
- $(AA^+)^T = AA^+$ （对称性）
- $(A^+A)^T = A^+A$ （对称性）

事实上，这四个条件的约束是非常强的。它们强到可以证明，任何矩阵的 MP 逆都是唯一存在的。

> 这里我们会发现到了 MP 这个层次，“左”和“右” （梦回史纲） 的概念就已经被消解了。因为通过前两个条件，你很难说这个逆究竟是在左还是在右。所以 MP 没有左右之分，它就是唯一的。MP 还有一个强大的特点。无论方阵与否，无论奇异与否，MP 照单全收！（总有一款适合你）

MP 逆的性质：

- 唯一性前文已有叙述。
- A 的 MP 逆的 MP 逆是 A，即 $(A^+)^+ = A$. 这一点是由唯一性保证的。
- 若 $D = \mathrm{diag}(d_{11}, \ldots, d_{nn})$ 为 $n \times n$ 对角矩阵，则 $D^+ = \mathrm{diag}(d_{11}^+, \ldots, d_{nn}^+)$，其中 $d_{ii}^+ = d_{ii}^{-1}$（若 $d_{ii} \neq 0$）或者 $d_{ii}^+ = 0$（若 $d_{ii} = 0$）。

1. **统一性**

当 A 是可逆方阵时，$A^+ = A^{-1}$（进化为传统逆）；

当 A 是列满秩高矩阵时，A^+ 退化为上述的左伪逆；

当 A 是行满秩胖矩阵时，A^+ 退化为上述的右伪逆。

1. **最广义的逆矩阵**

当一个矩阵，它对于 MP 的四个条件只能满足第一条，$AA^+A = A$ 时，我们称之为 A 的广义逆，并用 A^- 来表示。即 $AA^-A = A$。

由此，广义逆矩阵完成了它的闭环：无论原矩阵退化、残缺到什么地步，MP 逆永远在最后兜底，为数据科学和工程计算提供最稳定的数学基石。

下面给出 MP 逆如何**计算**：

若 $n \times m$ 矩阵 A 的奇异值分解为 $A = U\Sigma V^T$，其中 U 是 $n \times n$ 的正交阵，

V 是 $m \times m$ 的正交阵，Σ 是 $n \times m$ 的对角阵，则 $A^+ = V\Sigma^+U^T$。

验证 $A^+ = V\Sigma^+U^T$ 满足 Moore-Penrose 条件

(1) $AA^+A = A$

$U\Sigma V^T V\Sigma^+U^T U\Sigma V^T = U\Sigma\Sigma^+\Sigma V^T = U\Sigma V^T$

(2) $A^+AA^+ = A^+$

$V\Sigma^+U^T U\Sigma V^T V\Sigma^+U^T = V\Sigma^+\Sigma\Sigma^+U^T = V\Sigma^+U^T$

(3) $AA^+ = (AA^+)^T$

即证：$\Sigma\Sigma^+ = (\Sigma\Sigma^+)^T$

(4) $A^+A = (A^+A)^T$

即证：$\Sigma^+\Sigma = (\Sigma^+\Sigma)^T$

9.6.1 MP 逆矩阵专项练习题

以下 10 道题覆盖了 MP 逆的三种退化形态（左伪逆、右伪逆、SVD 构造法）以及实际应用。重点是理解” 什么情况下用哪个公式” 和”MP 逆在解方程中的作用”。

第 1 题（对角阵 MP 逆——最简单的情况）：$D = \begin{bmatrix} 4 & 0 \\ 0 & 0 \end{bmatrix}$，求 D^+。

解：非零奇异值 $\sigma_1 = 4$，$\Sigma^+ = \begin{bmatrix} 1/4 & 0 \\ 0 & 0 \end{bmatrix}$。由于 D 已对角且 $U = V = I_2$，$D^+ = \begin{bmatrix} 1/4 & 0 \\ 0 & 0 \end{bmatrix}$。规则：对角元非零则取倒数，为零则保持零。

第 2 题（列满秩 → 左伪逆）：$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}$（$3 \times 2$，高矩阵），求 A^+。

解：列满秩，用左伪逆公式 $A^+ = (A^TA)^{-1}A^T$。$A^TA = \begin{bmatrix}2&0\\0&1\end{bmatrix}$，$(A^TA)^{-1} = \begin{bmatrix}1/2&0\\0&1\end{bmatrix}$。$A^+ = \begin{bmatrix}1/2&0&1/2\\0&1&0\end{bmatrix}$。验证 $A^+A = I_2$。

第 3 题（行满秩 → 右伪逆）：$A = \begin{bmatrix}1&0&1\\0&1&0\end{bmatrix}$（$2\times 3$，胖矩阵），求 A^+。

解：行满秩，用右伪逆公式 $A^+ = A^T(AA^T)^{-1}$。$AA^T = \begin{bmatrix}2&0\\0&1\end{bmatrix}$，$(AA^T)^{-1} = \begin{bmatrix}1/2&0\\0&1\end{bmatrix}$。$A^+ = \begin{bmatrix}1/2&0\\0&1\\1/2&0\end{bmatrix}$。验证 $AA^+ = I_2$。

第 4 题（秩亏缺 → 用 SVD 构造 MP 逆）：$A = \begin{bmatrix}1&2\\2&4\end{bmatrix}$，求 A^+。

解：$\mathrm{rank}(A) = 1$（两行成比例）。A^TA 特征值 25 和 0，$\sigma_1 = 5$。$v_1 = \frac{1}{\sqrt{5}}\begin{bmatrix}1\\2\end{bmatrix}$，$u_1 = \frac{1}{\sqrt{5}}\begin{bmatrix}1\\2\end{bmatrix}$。$A^+ = v_1\cdot\frac{1}{\sigma_1}\cdot u_1^T = \frac{1}{25}\begin{bmatrix}1&2\\2&4\end{bmatrix}$。

第 5 题（用 MP 逆解超定方程——最小二乘）：用 $A = \begin{bmatrix}1&0\\0&1\\1&1\end{bmatrix}$ 的 MP 逆解 $Ax = \begin{bmatrix}2\\3\\5\end{bmatrix}$。

解：先求 A^+。列满秩，$A^TA = \begin{bmatrix}2&1\\1&2\end{bmatrix}$，$(A^TA)^{-1} = \frac{1}{3}\begin{bmatrix}2&-1\\-1&2\end{bmatrix}$。$A^+ = \frac{1}{3}\begin{bmatrix}2&-1&1\\-1&2&1\end{bmatrix}$。$\hat{x} = A^+b = \frac{1}{3}\begin{bmatrix}2&-1&1\\-1&2&1\end{bmatrix}\begin{bmatrix}2\\3\\5\end{bmatrix} = \begin{bmatrix}2\\3\end{bmatrix}$。此时 $A\hat{x} = \begin{bmatrix}2\\3\\5\end{bmatrix} = b$，残差为零——$b$ 恰好在 $\mathrm{Col}(A)$ 中。

注意：如果 b 不在 $\mathrm{Col}(A)$ 中，$\hat{x} = A^+b$ 给出的就是**最小二乘解**（使 $\|Ax-b\|_2$ 最小）。

第 6 题（用 MP 逆解欠定方程——最小范数解）：用 $A = \begin{bmatrix}1&0&1\\0&1&0\end{bmatrix}$ 的 MP 逆解 $Ax = \begin{bmatrix}2\\3\end{bmatrix}$。

解：行满秩 2×3，有无穷多解。A^+ 见第 3 题 = $\begin{bmatrix}1/2&0\\0&1\\1/2&0\end{bmatrix}$。$\hat{x} = A^+b = \begin{bmatrix}1\\3\\1\end{bmatrix}$。在所有满足 $Ax = \begin{bmatrix}2\\3\end{bmatrix}$ 的解中，$\hat{x}$ 的 ℓ_2 范数最小。

第 7 题（验证 MP 四条件）：验证第 4 题求得的 $A^+ = \frac{1}{25}\begin{bmatrix}1&2\\2&4\end{bmatrix}$ 满足 $AA^+A = A$ 和 $A^+AA^+ = A^+$。

解：(1) $AA^+ = \frac{1}{25}\begin{bmatrix}1&2\\2&4\end{bmatrix}\begin{bmatrix}1&2\\2&4\end{bmatrix} = \frac{1}{25}\begin{bmatrix}5&10\\10&20\end{bmatrix} = \frac{1}{5}\begin{bmatrix}1&2\\2&4\end{bmatrix}$。$AA^+A = \frac{1}{5}\begin{bmatrix}1&2\\2&4\end{bmatrix}\begin{bmatrix}1&2\\2&4\end{bmatrix} = \frac{1}{5}\begin{bmatrix}5&10\\10&20\end{bmatrix} = A$。

(2) $A^+AA^+ = \cdots = A^+$。

第 8 题（已给 SVD，直接写 MP 逆）：已知 $A = U\Sigma V^T$，$\Sigma = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}_{3\times 3}$，求 A^+。

解：$\Sigma^+ = \begin{bmatrix} 1/3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$。$A^+ = V\Sigma^+U^T$。若 U, V 为单位阵，则 $A^+ = \Sigma^+$。

第 9 题（左伪逆 vs MP 逆——什么时候等价?）：$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 2 & 0 \end{bmatrix}$，用两种方法求 A^+，验证结果一致。

解：列满秩，左伪逆 $A^+ = (A^TA)^{-1}A^T$。$A^TA = \begin{bmatrix} 5 & 0 \\ 0 & 1 \end{bmatrix}$，$A^+ = \begin{bmatrix} 1/5 & 0 & 2/5 \\ 0 & 1 & 0 \end{bmatrix}$。由于 A 列满秩，MP 逆就是左伪逆，结果相同。

第 10 题（综合——SVD + MP 逆一题到底）：$A = \begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$（前面 SVD 例题的矩阵），已有 $\sigma_1 = \sqrt{3}, \sigma_2 = 1$，求 A^+。

解：Σ 为 3×4，Σ^+ 为 4×3：$\Sigma^+ = \begin{bmatrix} 1/\sqrt{3} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$。$A^+ = V\Sigma^+U^T$，代入前面求得的 U, V 计算即可。

矩阵方程

在众多科学与工程学科，许多问题都可用数学建模成矩阵方程 $A\boldsymbol{x} = \boldsymbol{b}$。根据数据向量 $\boldsymbol{b} \in \mathbb{R}^n$ 和数据矩阵 $A \in \mathbb{R}^{n\times m}$ 的不同，矩阵方程有以下三种主要类型：

1. **超定矩阵方程** $n > m$，并且数据矩阵 A 和数据向量 $\boldsymbol{b}$ 均已知，其中之一或者二者可能存在误差或干扰。
1. **盲矩阵方程**仅数据向量 $\boldsymbol{b}$ 已知，数据矩阵 A 未知。
1. **欠定系数矩阵方程** $n < m$，数据矩阵 A 和数据向量 $\boldsymbol{b}$ 均已知，但未知向量 $\boldsymbol{x}$ 为稀疏向量。

考虑超定矩阵方程 $A\boldsymbol{x} = \boldsymbol{b}$，其中 $\boldsymbol{b}$ 为 $n\times 1$ 数据向量，A 为 $n\times m$ 数据矩阵，并且 $n > m$。

加性观测误差或噪声：$\boldsymbol{b} = \boldsymbol{b}_0 + \boldsymbol{e}$

校正向量 $\Delta\boldsymbol{b}$，使 $A\boldsymbol{x} = \boldsymbol{b} + \Delta\boldsymbol{b}$

$$\boldsymbol{b} + \Delta\boldsymbol{b} = \boldsymbol{b}_0 + \boldsymbol{e} + \Delta\boldsymbol{b} \to \boldsymbol{b}_0$$

目标：$\Delta\boldsymbol{b} \to 0$

$$\min_{\boldsymbol{x}} \|\boldsymbol{b}\|^2 = \|A\boldsymbol{x} - \boldsymbol{b}\|_2^2 = (A\boldsymbol{x} - \boldsymbol{b})^T (A\boldsymbol{x} - \boldsymbol{b})$$

$$\phi = \boldsymbol{x}^T A^T A\boldsymbol{x} - \boldsymbol{x}^T A^T \boldsymbol{b} - \boldsymbol{b}^T A\boldsymbol{x} + \boldsymbol{b}^T \boldsymbol{b}$$

$$\frac{d\phi}{d\boldsymbol{x}} = 0 = 2A^T A\boldsymbol{x} - 2A^T \boldsymbol{b}$$

$$A^T A\boldsymbol{x} = A^T \boldsymbol{b}$$

情形一：超定方程 $(n > m)$ 满列秩，即 $\text{rank}(A) = m$

由于 $A^T A$ 非奇异，所以方程有唯一解

$$\boldsymbol{x}_{\text{LS}} = (A^T A)^{-1} A^T \boldsymbol{b}$$

情形二：超定方程 $(n > m)$ 秩亏缺，即 $\text{rank}(A) < m$

$$\boldsymbol{x}_{\text{LS}} = (A^T A)^{\dagger} A^T \boldsymbol{b}$$

其中 $B^{\dagger}$ 代表 B 的广义逆矩阵。

9.7 【不考】稀疏矩阵与稀疏编码

9.7.1 什么是稀疏表示

一个含有大多数零元素的向量/矩阵称为**稀疏向量/稀疏矩阵**。

在信号处理中，一个信号向量 $\boldsymbol{y} \in \mathbb{R}^n$ 可以分解为一组基向量的线性组合。如果使用**完备正交基**（如傅里叶基、小波基），恰好需要 n 个基向量 $\boldsymbol{g}_k \in \mathbb{R}^n (k = 1, \cdots, n)$：

$$\boldsymbol{y} = \boldsymbol{G}\boldsymbol{c} = \sum_{i=1}^{n} c_i \boldsymbol{g}_i$$

此时系数向量 $\boldsymbol{c}$ **通常是非稀疏的**——几乎所有系数都非零。这是因为正交基追求的是”完备性”（刚好 n 个基撑起 n 维空间），而不是”经济性”（用最少的基表达信号）。

> 一个典型的例子：一张自然图像在傅里叶基下的表示几乎”占满”所有频率——图像中的边缘、纹理等结构需要大量余弦波叠加才能刻画。但在另一种基（比如小波基或学习到的字典）下，同样的图像可能只需要很少的几个原子的组合。

过完备字典的思路是：用 $m > n$ 个向量 $\boldsymbol{d}_i \in \mathbb{R}^n$（称为**原子**或码字）作为基的候选池，从中选出**尽可能少的几个**来线性组合表示信号 $\boldsymbol{y}$：

$$\boldsymbol{y} = \boldsymbol{D}\boldsymbol{x} = \sum_{i=1}^{m} x_i \boldsymbol{d}_i \quad (m > n)$$

其中 $\boldsymbol{D} = [\boldsymbol{d}_1, \cdots, \boldsymbol{d}_m] \in \mathbb{R}^{n \times m}$ 称为**字典**或**码本**。因为 $m > n$，字典是**过完备**（overcomplete）的。

> **为什么过完备？**如果只有 n 个正交基，你就像只有 n 把固定的”尺子”去度量世界——所有信号都被强制用同样的语言描述。但有了 $m > n$ 个冗余的原子，你可以从不同的角度选择最匹配的几个来描述信号——不同信号用不同的原子组合，每个信号只用很少几个。这就是稀疏编码的核心哲学：**用冗余换取稀疏性**。

字典的典型假设：

1. $\boldsymbol{D}$ 的行数 n 小于列数 m（过完备）
2. $\boldsymbol{D}$ 满行秩，即 $\text{rank}(\boldsymbol{D}) = n$（能覆盖整个 $\mathbb{R}^n$）
3. $\boldsymbol{D}$ 的每列具有单位 ℓ_2 范数：$\|\boldsymbol{d}_j\|_2 = 1$

9.7.2 稀疏表示的数学形式

对于过完备字典，$\boldsymbol{y} = \boldsymbol{D}\boldsymbol{x}$ 有无穷多组解。我们希望找到**最稀疏**的那组解。

(1) 理想形式（ℓ_0 范数最小化）

$$\min_{\boldsymbol{x}} \|\boldsymbol{x}\|_0 \quad \text{subject to} \quad \boldsymbol{D}\boldsymbol{x} = \boldsymbol{y}$$

其中 $\|\boldsymbol{x}\|_0$ 表示 $\boldsymbol{x}$ 中非零元素的个数。

(2) 有噪声情况（稀疏逼近）

实际数据总含噪声。引入容差 ε：

$$\min_{\boldsymbol{x}} \|\boldsymbol{x}\|_0 \quad \text{subject to} \quad \|\boldsymbol{D}\boldsymbol{x} - \boldsymbol{y}\|_2 \leq \varepsilon$$

称为目标信号 $\boldsymbol{y}$ 相对于字典 $\boldsymbol{D}$ 的**稀疏逼近**。

> **ℓ_0 vs ℓ_2 的深刻区别：**
>
> 经典方法用 $\min \|\boldsymbol{x}\|_2$（最小能量解）——它会产生一个所有分量都非零但都很小的稠密解。稀疏编码用 $\min \|\boldsymbol{x}\|_0$ ——它强制大部分系数精确为零。两者的哲学完全不同：- ℓ_2：”把能量平均分配给所有基” - ℓ_0：”只用最关键的几个基，其他基的系数设为零”
>
> 这也是为什么在压缩感知（Compressed Sensing）中，ℓ_1 范数常被用作 ℓ_0 的凸松弛——但它能保留稀疏性，而 ℓ_2 不能。

重要困难：直接求解 ℓ_0 最小化是 **NP-hard** 的——因为你需要枚举所有可能的非零元素组合（搜索空间是组合爆炸的）。因此实际中采用两类策略：

- **贪婪算法**：每次选一个" 最好" 的原子加入（MP、OMP）
- **凸松弛**：用 ℓ_1 范数代替 ℓ_0 范数（LASSO、基追踪）

9.7.3 稀疏编码问题

稀疏编码的形式化描述：给定一组 n 维输入向量 $\{\boldsymbol{y}_1, \boldsymbol{y}_2, \cdots, \boldsymbol{y}_N\}$，确定基矩阵 $\boldsymbol{D} \in \mathbb{R}^{n\times m}$ 和稀疏系数矩阵 $\boldsymbol{S} \in \mathbb{R}^{m\times N}$，使得

$$\boldsymbol{Y} \approx \boldsymbol{D}\boldsymbol{S}$$

其中 $\boldsymbol{S}$ 的每一列都是稀疏向量。

稀疏编码有两个核心子问题：

1. **稀疏表示（给定字典 $\boldsymbol{D}$ 求系数 $\boldsymbol{S}$）**：这就是上面讲的 ℓ_0 最小化
2. **字典训练（给定数据 $\boldsymbol{Y}$ 求字典 $\boldsymbol{D}$）**：如何从数据中学习一个好的字典

9.7.4 贪婪求解算法

9.7.4.1 (1) 匹配追踪（Matching Pursuit, MP）

基本思想：迭代地从字典中选择与当前残差" 最匹配" 的原子。

算法步骤：

1. 初始化残差 $\boldsymbol{r}_0 = \boldsymbol{y}$
2. 在第 k 步，选择与残差内积绝对值最大的原子：

$$\boldsymbol{d}_{i_k} = \arg\max_{\boldsymbol{d}_j} |\langle \boldsymbol{r}_{k-1}, \boldsymbol{d}_j \rangle|$$

1. 更新系数：$x_{i_k} \leftarrow x_{i_k} + \langle \boldsymbol{r}_{k-1}, \boldsymbol{d}_{i_k} \rangle$
2. 更新残差：$\boldsymbol{r}_k = \boldsymbol{r}_{k-1} - \langle \boldsymbol{r}_{k-1}, \boldsymbol{d}_{i_k} \rangle \boldsymbol{d}_{i_k}$
3. 重复直到残差足够小或达到预设的稀疏度

> **注意**：在 MP 中，每次更新只涉及最新选中的那个原子。之前选中的原子的系数**不会被重新优化**。这意味着残差只与最新加入的原子正交，而不一定与之前选中的所有原子正交。这导致 MP 的收敛速度可能较慢——同一个原子可能在后续迭代中被再次选中。

实际预处理：通常将信号 $\boldsymbol{y}$ 零均值化，字典原子也零均值化并归一化（$\|\boldsymbol{d}_j\| = 1$）。此时" 最匹配" 等价于内积绝对值最大（因为归一化后内积就是相关系数）。

MP 的特点：计算速度快，但收敛性较差（可能需很多步）。

9.7.4.2 (2) 正交匹配追踪（Orthogonal Matching Pursuit, OMP）

关键改进：在每一步，对**已选中的所有原子**重新做最小二乘拟合，保证残差与所有已选原子正交。

算法步骤：

1. 初始化残差 $\boldsymbol{r}_0 = \boldsymbol{y}$，已选原子索引集 $\Lambda_0 = \emptyset$
2. 在第 k 步，选出最匹配的原子索引：

$$i_k = \arg\max_j |\langle \boldsymbol{r}_{k-1}, \boldsymbol{d}_j \rangle|$$

1. 更新索引集：$\Lambda_k = \Lambda_{k-1} \cup \{i_k\}$
2. 对 Λ_k 中原子构成的子字典 $\boldsymbol{D}_{\Lambda_k}$，用最小二乘求解系数：

$$\boldsymbol{x}_{\Lambda_k} = \arg\min_{\boldsymbol{x}} \|\boldsymbol{D}_{\Lambda_k}\boldsymbol{x} - \boldsymbol{y}\|_2^2 = (\boldsymbol{D}_{\Lambda_k}^T \boldsymbol{D}_{\Lambda_k})^{-1} \boldsymbol{D}_{\Lambda_k}^T \boldsymbol{y}$$

1. 更新残差：$\boldsymbol{r}_k = \boldsymbol{y} - \boldsymbol{D}_{\Lambda_k}\boldsymbol{x}_{\Lambda_k}$
2. 重复直到收敛

OMP 的核心优势：因为每个原子不会被选中两次（一旦选中，残差就与它正交了），OMP 在最多 m 步内必然收敛。而且由于每一步都对所有已选原子重新优化，收敛速度远快于 MP。

在实际应用中，OMP 是更常用的选择——特别是在信号处理、图像去噪和压缩感知中。

MP vs OMP 对比：

表 9.3:

	MP	OMP
残差正交性	仅与最新原子正交	与所有已选原子正交
系数更新	仅更新最新原子系数	所有已选原子重新拟合
收敛速度	较慢	较快（有限步内收敛）
计算复杂度	低（每步）	较高（每步需最小二乘）

9.7.5 字典训练：K-SVD 算法

既然稀疏表示的效果高度依赖字典的质量，那么**如何从数据中学习一个好的字典**？

K-SVD 算法（Aharon, Elad et al., 2006）是最经典的字典训练算法。

优化目标：

$$\min_{\boldsymbol{D},\boldsymbol{X}} \|\boldsymbol{Y}-\boldsymbol{D}\boldsymbol{X}\|_F^2 \quad \text{subject to} \quad \forall i, \|\boldsymbol{x}_i\|_0 \le T_0$$

其中 $\boldsymbol{Y}\in\mathbb{R}^{n\times N}$ 是 N 个训练样本，$\boldsymbol{D}\in\mathbb{R}^{n\times m}$ 是字典，$\boldsymbol{X}\in\mathbb{R}^{m\times N}$ 是系数矩阵（每列稀疏，非零元不超过 T_0 个）。

K-SVD 的两步交替优化：

(1) 稀疏编码阶段（固定 $\boldsymbol{D}$，求 $\boldsymbol{X}$）：

使用 OMP 等算法对每个样本 $\boldsymbol{y}_i$ 求其稀疏系数 $\boldsymbol{x}_i$。

(2) 字典更新阶段（固定 $\boldsymbol{X}$，逐列更新 $\boldsymbol{D}$）：

这是 K-SVD 的精髓。当更新字典的第 k 列 $\boldsymbol{d}_k$ 时，保持其他列不变。总误差：

$$\|\boldsymbol{Y}-\boldsymbol{D}\boldsymbol{X}\|_F^2 = \left\|\left(\boldsymbol{Y}-\sum_{j\neq k}\boldsymbol{d}_j\boldsymbol{X}_j^T\right)-\boldsymbol{d}_k\boldsymbol{X}_k^T\right\|_F^2 = \|\boldsymbol{E}_k-\boldsymbol{d}_k\boldsymbol{X}_k^T\|_F^2$$

其中 $\boldsymbol{E}_k$ 是去掉第 k 个原子贡献后的残差矩阵，$\boldsymbol{X}_k^T$ 是系数矩阵的第 k 行。

> 直接对 $\boldsymbol{E}_k$ 做 SVD（$\boldsymbol{E}_k=\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^T$），取 $\boldsymbol{d}_k=\boldsymbol{u}_1$（$\boldsymbol{U}$ 的第一列），$\boldsymbol{X}_k^T=\sigma_1\boldsymbol{v}_1^T$（乘上最大奇异值）——这就是 K-SVD 名字的由来（K-means + SVD）。但注意：这样得到的 $\boldsymbol{X}_k^T$ 可能不再稀疏！所以实际实现中只对 $\boldsymbol{E}_k$ 中用到第 k 个原子的那些样本（即 $\boldsymbol{X}_k^T$ 中非零元素对应的列）做 SVD，以保持系数向量的稀疏性。

K-SVD 流程总结：

1. 初始化字典 $\boldsymbol{D}$（可随机选取样本，或用已有正交基）
2. 重复直到收敛：

- **稀疏编码**：用 OMP 求每个样本的稀疏系数
- **字典更新**：逐列更新 $\boldsymbol{d}_k$——对用到了 $\boldsymbol{d}_k$ 的样本的残差做 SVD，用第一主成分更新 $\boldsymbol{d}_k$ 和相应系数

1. 返回训练好的字典 $\boldsymbol{D}$

> K-SVD 是字典学习领域的里程碑算法。它的思想简洁而强大：先用当前字典做稀疏编码，再根据稀疏编码的结果反向优化字典——典型的 EM（期望最大化）类算法结构。在图像去噪、超分辨率、压缩感知等应用中，K-SVD 训练的字典显著优于固定字典（如 DCT、小波）。

9.7.6 稀疏编码的影响因素

影响稀疏编码精度的关键因素：

1. **字典质量**：字典原子是否” 贴合” 信号的本质结构
2. **稀疏度约束**：T_0 的选择——太大会引入噪声，太小则欠拟合
3. **求解算法**：MP/OMP 的逼近质量、ℓ_1 松弛与 ℓ_0 真解之间的差距
4. **数据噪声**：噪声水平 ε 的设定直接影响稀疏解的稳定性

第 10 章 拟合与回归

10.1 拟合回归简介

如果向量 $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_p$ 与向量 $\boldsymbol{y}$ 之间存在相关关系，能找到一个关于 $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_p$ 的函数 f 和一个满足要求的范数较小的 $\boldsymbol{\varepsilon}$，使得

$$\boldsymbol{y} = f(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_p) + \boldsymbol{\varepsilon}$$

则称 $f(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_p)$ 是 $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_p$ 对 $\boldsymbol{y}$ 的**拟合**。

$\boldsymbol{y}$ 称为**响应变量（因变量）**，$\boldsymbol{x}_i$ 称为**解释变量（自变量）**。

因为满足要求的函数 f 有无数种可能，从而有各种拟合方法：

如果 f 是线性的，就叫**线性拟合**或者**线性回归**（主要在统计中），否则叫作**非线性拟合**或者**非线性回归**。

当拟合的结果是一条曲线时，称为**曲线拟合**，曲线拟合中 f 的表达式也可以是分段函数，这种情况下叫作**样条拟合**。

> 事实上，如果我们不限制拟合方法，同时又追求 ε 的最小值，那么就会构成一个问题：过拟合（Overfit）。实际数据中的 $\boldsymbol{\varepsilon}$ 通常包含随机测量误差或无法解释的噪音。如果强求 $\boldsymbol{\varepsilon}$ 的范数极小，函数 f 就会把这些随机噪声误当成“确定性规律”去强行契合。因此，在实际应用中（如岭回归、LASSO 等），通常会引入正则化惩罚项，主动放弃一部分对训练误差的极致追求，以此换取模型更强的泛化能力和更清爽的真实规律。所以在量化金融等领域 •，线性回归实际上依然是最常用的统计分析模型之一。

10.2 简单回归

10.2.1 简单回归

一元线性回归，又称为简单回归，是两个变量之间最简单的回归模型。如果向量 $\boldsymbol{x} = [x_1, x_2, \ldots, x_n]^T$ 与 $\boldsymbol{y} = [y_1, y_2, \ldots, y_n]^T$ 之间存在线性关系，简单回归寻找两个回归系数 β_0 与 β_1，使得

$$y_i = \beta_0 + \beta_1 x_i, \quad i = 1, 2, \ldots, n$$

或者

$$\boldsymbol{y} \approx \beta_0 \mathbf{1} + \beta_1 \boldsymbol{x}$$

此时，称 $\hat{\boldsymbol{y}} = \beta_0 \mathbf{1} + \beta_1 \boldsymbol{x}$ 为 $\boldsymbol{y}$ 的估计量。

10.2.2 简单回归方程的一般解法

一般地，将 β_0 与 β_1 的求解问题转换为最小化二范数问题，即

$$\min \|\boldsymbol{\varepsilon}\|_2^2,\ \text{s.t. } \boldsymbol{y} = \beta_0 \mathbf{1} + \beta_1 \boldsymbol{x} + \boldsymbol{\varepsilon}$$

$$\|\boldsymbol{\varepsilon}\|^2 = \sum_{i=1}^{n} [y_i - (\beta_0 + \beta_1 x_i)]^2$$

利用最小二乘法，有：

$$\frac{\partial \|\boldsymbol{\varepsilon}\|^2}{\partial \beta_0} = 0 \iff \sum_{i=1}^{n} \frac{\partial [y_i - (\beta_0 + \beta_1 x_i)]^2}{\partial \beta_0} = 0$$

$$\iff 0 = \sum_{i=1}^{n} y_i - n\beta_0 - \beta_1 \sum_{i=1}^{n} x_i$$

$$\frac{\partial \|\boldsymbol{\varepsilon}\|^2}{\partial \beta_1} = 0 \iff \sum_{i=1}^{n} \frac{\partial [y_i - (\beta_0 + \beta_1 x_i)]^2}{\partial \beta_1} = 0$$

$$\iff 0 = \sum_{i=1}^{n} x_i y_i - \beta_0 \sum_{i=1}^{n} x_i - \beta_1 \sum_{i=1}^{n} x_i^2$$

令 $\bar{x} = \frac{\sum_{i=1}^{n} x_i}{n}$，$\bar{y} = \frac{\sum_{i=1}^{n} y_i}{n}$ 分别为 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的元素均值，则

$$\hat{\beta}_0 = \bar{y} - \hat{\beta}_1 \bar{x}$$

$$\hat{\beta}_1 = \frac{\sum_{i=1}^{n} x_i y_i - n\bar{x}\bar{y}}{\sum_{i=1}^{n} x_i^2 - n(\bar{x})^2}$$

其中 $\hat{\beta}_0, \hat{\beta}_1$ 分别是参数 β_0 与 β_1 的最小二乘估计。

在实际中对向量 $\boldsymbol{x}$ 与向量 $\boldsymbol{y}$，只需先分别求出它们的样本均值 $\bar{x}$ 和 $\bar{y}$ 以及 $\sum_{i=1}^{n} x_i^2$ 和 $\sum_{i=1}^{n} x_i y_i$，就可以根据上式求出参数 β_0 与 β_1 的估计值。

10.3 【重点】多元回归方程的一般解法与稀疏回归问题

10.3.1 多元回归问题

多元回归是使用多个变量的线性组合来对响应变量进行逼近的回归模型。即对向量 $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m$ 与响应向量 $\boldsymbol{y}$，寻找回归系数 $\beta_0, \beta_1, \beta_2, \ldots, \beta_m$ 使得

$$\boldsymbol{y} \approx \beta_0 \mathbf{1} + \beta_1 \boldsymbol{x}_1 + \beta_2 \boldsymbol{x}_2 + \cdots + \beta_m \boldsymbol{x}_m$$

此时，称 $\hat{\boldsymbol{y}} = \beta_0 \mathbf{1} + \beta_1 \boldsymbol{x}_1 + \beta_2 \boldsymbol{x}_2 + \cdots + \beta_m \boldsymbol{x}_m$ 为 $\boldsymbol{y}$ 的估计量。

10.3.2 多元回归方程的一般解法（帽子矩阵法）

类似地，将拟合系数 $\beta_0, \beta_1, \beta_2, \ldots, \beta_m$ 的求解问题转换为最小化二范数问题，即

$$\min \|\boldsymbol{\varepsilon}\|_2^2, \text{ s.t. } \boldsymbol{y} = \beta_0 \mathbf{1} + \beta_1 \boldsymbol{x}_1 + \beta_2 \boldsymbol{x}_2 + \cdots + \beta_m \boldsymbol{x}_m + \boldsymbol{\varepsilon}$$

这里做两个小思考：对给定的 X 和 y，它们的行维度和列维度分别表示的是什么？为什么我们回归出来的是一串常数呢？

令 $X = \begin{bmatrix} \mathbf{1} & \boldsymbol{x}_1 & \boldsymbol{x}_2 & \cdots & \boldsymbol{x}_m \end{bmatrix}$，$\boldsymbol{\beta} = \begin{bmatrix} \beta_0 & \beta_1 & \cdots & \beta_m \end{bmatrix}^T$，则有

$$\boldsymbol{y} = X\boldsymbol{\beta} + \boldsymbol{\varepsilon}$$

这里 $\boldsymbol{\beta}$ 要写在 X 右边，大家需要习惯这一点。

从而有

$$\|\boldsymbol{\varepsilon}\|_2^2 = \langle \boldsymbol{y} - X\boldsymbol{\beta}, \boldsymbol{y} - X\boldsymbol{\beta} \rangle = \boldsymbol{y}^T\boldsymbol{y} - 2\boldsymbol{y}^T X\boldsymbol{\beta} + \boldsymbol{\beta}^T X^T X\boldsymbol{\beta}$$

利用最小二乘法，有

$$\frac{\partial \|\boldsymbol{\varepsilon}\|_2^2}{\partial \boldsymbol{\beta}} = -2X^T\boldsymbol{y} + 2X^T X\hat{\boldsymbol{\beta}} = 0$$

因此，

$$X^T X\hat{\boldsymbol{\beta}} = X^T\boldsymbol{y}$$

当 $(X^T X)^{-1}$ 存在时，即得拟合参数的最小二乘估计为

$$\hat{\boldsymbol{\beta}} = (X^T X)^{-1} X^T\boldsymbol{y}$$

这里还有 callback，这里的 $(X^T X)^{-1} X^T$ 实际上就是 X 的左逆。

最后有

$$\hat{\boldsymbol{\beta}} = (X^T X)^{-1} X^T \boldsymbol{y}$$

$$\hat{\boldsymbol{y}} = X(X^T X)^{-1} X^T \boldsymbol{y}$$

其中称 $H = X(X^T X)^{-1} X^T$ 称为**帽子矩阵**，它是对称幂等阵，即

$$H^T = H, \quad H^n = H, \quad (I - H)^n = I - H$$

$(I - H)^n = I - H$ 这一条由数学归纳法易得。

10.3.3 补充例题

【例 1：二元线性回归计算】已知数据集：

表 10.1:

x_1	x_2	y
1	2	5
2	1	6
3	3	11
4	2	12

试用最小二乘法求 $\hat{\boldsymbol{\beta}} = [\beta_0, \beta_1, \beta_2]^T$，并写出帽子矩阵 H。

解：

(1) 构造设计矩阵 X（第一列为全 1）：

$$X = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 2 & 1 \\ 1 & 3 & 3 \\ 1 & 4 & 2 \end{bmatrix}, \quad \boldsymbol{y} = \begin{bmatrix} 5 \\ 6 \\ 11 \\ 12 \end{bmatrix}$$

(2) 计算 $X^T X$：

$$X^T X = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 & 2 \\ 1 & 2 & 1 \\ 1 & 3 & 3 \\ 1 & 4 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 10 & 8 \\ 10 & 30 & 23 \\ 8 & 23 & 18 \end{bmatrix}$$

(3) 计算 $X^T\boldsymbol{y}$：

$$X^T\boldsymbol{y}=\begin{bmatrix}1&1&1&1\\1&2&3&4\\2&1&3&2\end{bmatrix}\begin{bmatrix}5\\6\\11\\12\end{bmatrix}=\begin{bmatrix}34\\98\\75\end{bmatrix}$$

(4) 求 $(X^TX)^{-1}$：

$$\det(X^TX)=4(540-529)-10(180-184)+8(230-240)=44+40-80=4$$

$$(X^TX)^{-1}=\frac{1}{4}\begin{bmatrix}30\cdot18-23\cdot23&-(10\cdot18-8\cdot23)&10\cdot23-8\cdot30\\-(10\cdot18-23\cdot8)&4\cdot18-8\cdot8&-(4\cdot23-8\cdot10)\\10\cdot23-30\cdot8&-(4\cdot23-10\cdot8)&4\cdot30-10\cdot10\end{bmatrix}^T$$

计算得（过程从略）：

$$(X^TX)^{-1}=\frac{1}{4}\begin{bmatrix}11&4&-10\\4&8&-12\\-10&-12&20\end{bmatrix}$$

(5) 求回归系数：

$$\hat{\boldsymbol{\beta}}=(X^TX)^{-1}X^T\boldsymbol{y}=\frac{1}{4}\begin{bmatrix}11&4&-10\\4&8&-12\\-10&-12&20\end{bmatrix}\begin{bmatrix}34\\98\\75\end{bmatrix}=\frac{1}{4}\begin{bmatrix}374+392-750\\136+784-900\\-340-1176+1500\end{bmatrix}=\frac{1}{4}\begin{bmatrix}16\\20\\-16\end{bmatrix}=\begin{bmatrix}4\\5\\-4\end{bmatrix}$$

故回归方程为：$\boxed{\hat{y}=4+5x_1-4x_2}$

(6) 帽子矩阵：

$$H=X(X^TX)^{-1}X^T$$

（可代入数值验证 $H^2=H$ 的幂等性质。）

【例 2：验证帽子矩阵的对称幂等性】

设 X 为 $n\times(m+1)$ 设计矩阵（列满秩），帽子矩阵 $H=X(X^TX)^{-1}X^T$。证明 $H^T=H$ 且 $H^2=H$。

证：

(1) 对称性：

$$H^T = [X(X^TX)^{-1}X^T]^T = X[(X^TX)^{-1}]^TX^T = X[(X^TX)^T]^{-1}X^T = X(X^TX)^{-1}X^T = H$$

其中用到 $(X^TX)^T = X^TX$（X^TX 是对称矩阵）。

(2) 幂等性：

$$H^2 = X(X^TX)^{-1}X^T \cdot X(X^TX)^{-1}X^T = X(X^TX)^{-1}(X^TX)(X^TX)^{-1}X^T = X(X^TX)^{-1}IX^T = X(X^TX)^{-1}X^T =$$

证毕。

> **推论：** $(I-H)^2 = I - 2H + H^2 = I - 2H + H = I - H$，故 $I - H$ 也是幂等矩阵。$(I-H)^n = I - H$ 对任意正整数 n 成立（归纳法易证）。
>
> **几何意义：** $H\boldsymbol{y} = \hat{\boldsymbol{y}}$ 将响应向量投影到 X 的列空间上；$(I-H)\boldsymbol{y} = \boldsymbol{y} - \hat{\boldsymbol{y}} = \hat{\boldsymbol{\varepsilon}}$（残差），将 $\boldsymbol{y}$ 投影到列空间的正交补上。

【例 3：用帽子矩阵做预测】

沿用例 1 的数据和回归方程 $\hat{y} = 4 + 5x_1 - 4x_2$：

表 10.2:

x_1	x_2	y（实际）	$\hat{y}$（预测）	残差 ε
1	2	5	$4+5-8=1$	4
2	1	6	$4+10-4=10$	-4
3	3	11	$4+15-12=7$	4
4	2	12	$4+20-8=16$	-4

残差平方和 $SSE = 4^2 + (-4)^2 + 4^2 + (-4)^2 = 64$。

> **考试提示：** 考试中如要求计算帽子矩阵，可按 $H = X(X^TX)^{-1}X^T$ 直接代公式，重点是理解其对称幂等性质以及 $\hat{\boldsymbol{y}} = H\boldsymbol{y}$ 的投影含义。计算 $(X^TX)^{-1}$ 时务必仔细，二阶矩阵手动求逆即可（$A^{-1} = \frac{1}{\det A}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$），三阶及以上建议用伴随矩阵法验算。

10.4 基于条件不相关性的稀疏回归方法

第 10.3 节介绍了用帽子矩阵做多元回归——但当我们有 m 个候选自变量时，选择哪些变量进入模型？（选多了过拟合，选少了欠拟合）。10.4 节的核心问题是：**如何衡量一组自变量与因变量之间的整体相关性**，从而指导变量选择。这需要从两两相关系数推广到多元相关系数。

10.4.0.1 多元相关系数与多元不相关系数

回顾两变量：$\boldsymbol{a}$ 和 $\boldsymbol{b}$ 的（Pearson）相关系数 $\rho_{\boldsymbol{ab}}$ 衡量线性关联强度。当变量超过两个时，需要新的工具。

定义：设 $\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_m$ 是非零方差的向量，其相关矩阵为 $\boldsymbol{R}$。

- **无符号多元相关系数（UCC）**：

$$r^2 = 1 - \det(\boldsymbol{R})$$

- **无符号多元不相关系数（UIC）**：

$$\omega^2 = \det(\boldsymbol{R})$$

显然 $r^2 + \omega^2 = 1$ ——相关与不相关互补。

> **直观理解**：$\det(\boldsymbol{R})$ 衡量的是相关矩阵的” 体积”。如果所有变量两两不相关，$\boldsymbol{R} = \boldsymbol{I}$，则 $\det(\boldsymbol{R}) = 1$，$r^2 = 0$；如果变量之间存在强线性关系，$\boldsymbol{R}$ 接近奇异，$\det(\boldsymbol{R}) \approx 0$，$r^2 \approx 1$。

10.4.0.2 三元相关系数

对于三个向量 $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$，三元相关系数的平方为：

$$\boxed{r^2_{\boldsymbol{abc}} = \rho^2_{\boldsymbol{ab}} + \rho^2_{\boldsymbol{bc}} + \rho^2_{\boldsymbol{ca}} - 2\rho_{\boldsymbol{ab}}\rho_{\boldsymbol{bc}}\rho_{\boldsymbol{ca}}}$$

性质（常考）：

性质 1：$r^2_{\boldsymbol{abc}}$ 是 $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ 的对称函数——变量顺序不影响结果。

性质 2：$0 \le r^2_{\boldsymbol{abc}} \le 1$。

> 证明左不等式（≥ 0）：
>
> $$\begin{aligned} r^2_{\boldsymbol{abc}} &= \rho^2_{\boldsymbol{ab}} + \rho^2_{\boldsymbol{bc}} + \rho^2_{\boldsymbol{ca}} - 2\rho_{\boldsymbol{ab}}\rho_{\boldsymbol{bc}}\rho_{\boldsymbol{ca}} \\ &= (|\rho_{\boldsymbol{ab}}| - |\rho_{\boldsymbol{bc}}|)^2 + \rho^2_{\boldsymbol{ca}} + 2|\rho_{\boldsymbol{ab}}\rho_{\boldsymbol{bc}}| - 2\rho_{\boldsymbol{ab}}\rho_{\boldsymbol{bc}}\rho_{\boldsymbol{ca}} \ge 0 \end{aligned}$$
>
> 证明右不等式（≤ 1）：令 $\boldsymbol{a}', \boldsymbol{b}', \boldsymbol{c}'$ 分别为标准化向量。考虑
>
> $$\langle \boldsymbol{a}' - \langle \boldsymbol{a}', \boldsymbol{c}' \rangle \boldsymbol{c}',\ \boldsymbol{b}' - \langle \boldsymbol{b}', \boldsymbol{c}' \rangle \boldsymbol{c}' \rangle^2$$
>
> 利用柯西-施瓦茨不等式可证 $r^2_{\boldsymbol{abc}} \le 1$。

性质 3：$r^2_{\boldsymbol{abc}} = 1$ 当且仅当 $\boldsymbol{a}', \boldsymbol{b}', \boldsymbol{c}'$ 在同一个平面上（即存在线性关系 $\lambda_1 \boldsymbol{a}' + \lambda_2 \boldsymbol{b}' + \lambda_3 \boldsymbol{c}' = 0$）。

当三个标准化向量共面时，任意一个都可以被另外两个线性表示——这意味着一组变量之间存在严格的线性依赖。

性质 4：$r^2_{abc}=0$ 当且仅当 $\rho_{ab}=\rho_{bc}=\rho_{ca}=0$（三变量两两不相关）。

10.4.0.3 条件不相关性

条件不相关性的思想：在给定一组预测变量 $\boldsymbol{x}_1,\cdots,\boldsymbol{x}_k$ 后，衡量响应变量 $\boldsymbol{y}$ 中还剩下多少" 未被解释" 的变异。

定义：给定 $\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_k$ 条件下，$\boldsymbol{y}$ 的**条件不相关系数**为：

$$\omega(\boldsymbol{y}\mid\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_k)=\frac{\omega(\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_k,\boldsymbol{y})}{\omega(\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_k)}$$

其中分子是包含 $\boldsymbol{y}$ 在内的 $(k+1)$ 元 UIC，分母是仅含预测变量的 k 元 UIC。

类比：这很像条件概率公式 $P(B|A)=P(A\cap B)/P(A)$ ——把" 不相关系数" 当作" 不确定性" 的度量。条件不相关越小，说明 $\boldsymbol{x}_1,\cdots,\boldsymbol{x}_k$ 已经解释了 $\boldsymbol{y}$ 的大部分信息。

等价形式（用 MSE 表示）：

$$\omega^2(\boldsymbol{y}\mid\boldsymbol{x}_1,\cdots,\boldsymbol{x}_k)=\frac{\min_{\beta_0,\cdots,\beta_k}\mathrm{MSE}(\beta_0+\beta_1\boldsymbol{x}_1+\cdots+\beta_k\boldsymbol{x}_k,\boldsymbol{y})}{s^2_{\boldsymbol{y}}}$$

其中 $s^2_{\boldsymbol{y}}$ 是 $\boldsymbol{y}$ 的方差，分子是**最优**（最小二乘意义下）线性拟合的均方误差。

解读：条件不相关系数 = 最优线性拟合的残差方差 / 响应变量总方差。如果预测变量完全解释了 $\boldsymbol{y}$，则 MSE=0，条件不相关系数 =0；如果预测变量完全没用，最优拟合就是瞎猜（残差 = 总方差），系数 =1。

10.4.0.4 条件不相关系数的计算

设 $\boldsymbol{S}$ 为预测变量 $\boldsymbol{x}_1,\cdots,\boldsymbol{x}_k$ 的协方差矩阵，$\boldsymbol{S}_{\bullet\boldsymbol{y}}$ 为各 $\boldsymbol{x}_i$ 与 $\boldsymbol{y}$ 的协方差列向量，$s^2_{\boldsymbol{y}}$ 为 $\boldsymbol{y}$ 的方差。则：

$$\omega^2(\boldsymbol{y}\mid\boldsymbol{x}_1,\cdots,\boldsymbol{x}_k)=1-\frac{\boldsymbol{S}^T_{\bullet\boldsymbol{y}}\boldsymbol{S}^{-1}\boldsymbol{S}_{\bullet\boldsymbol{y}}}{s^2_{\boldsymbol{y}}}$$

用相关系数表示（记 $\rho_{i\boldsymbol{y}}$ 为 $\boldsymbol{x}_i$ 与 $\boldsymbol{y}$ 的相关系数，$\boldsymbol{R}_{\boldsymbol{x}}$ 为 $\boldsymbol{x}_i$ 之间的相关矩阵）：

$$\begin{bmatrix} \hat{\beta}_1 s_1/s_{\boldsymbol{y}} \\ \hat{\beta}_2 s_2/s_{\boldsymbol{y}} \\ \vdots \\ \hat{\beta}_k s_k/s_{\boldsymbol{y}} \end{bmatrix} = \boldsymbol{R}_{\boldsymbol{x}}^{-1} \begin{bmatrix} \rho_{1\boldsymbol{y}} \\ \rho_{2\boldsymbol{y}} \\ \vdots \\ \rho_{k\boldsymbol{y}} \end{bmatrix}$$

其中 s_i 是 $\boldsymbol{x}_i$ 的标准差，$\hat{\beta}_i$ 是最小二乘回归系数。

> **稀疏回归中的应用：**有了条件不相关性这个度量，就可以用它来**筛选变量**——逐步添加那些" 最能降低条件不相关系数" 的变量（即最能解释 $\boldsymbol{y}$ 剩余变异的变量），当条件不相关系数低于某个阈值时停止。这比盲目用全部变量做回归更稳健——特别是 m 很大而 n 较小时（高维回归问题）。

10.4.0.5 方法总结

基于条件不相关性的稀疏回归方法的核心步骤：

1. **计算所有候选变量与 $\boldsymbol{y}$ 的相关系数**
2. **逐步选择：**每次加入使条件不相关系数下降最多的变量
3. **停止准则：**当条件不相关系数低于阈值（已经解释得足够好）或达到预设的变量个数 k
4. **在选出的 k 个变量上做最小二乘回归**

> 这个方法本质上是一种包装式的特征选择（wrapper method），与 LASSO 等嵌入式方法不同——它显式地用条件不相关性作为选择准则。在自变量之间相关性复杂时（多重共线性），条件不相关性比简单的两两相关系数更能反映变量的实际贡献。

第 11 章 代数系统

代数系统是一个相当广的概念。我们所学的群，环，域，其实都是代数系统的具体实例。让我们先来看一些例子：

- 整数全体 $\mathbb{Z}$，定义了加法运算和乘法运算并满足一定的性质。
- 有理数全体、实数全体以及复数全体分别构成有理数域、实数域及复数域均是代数系统。
- 数域 $\mathbb{F}$ 上的一元多项式的全体 $\mathbb{F}[x]$，定义了多项式的加法运算、乘法运算并满足一定性质，构成代数系统。
- 数域 $\mathbb{F}$ 上的 $m \times n$ 阶矩阵的全体 $\mathbb{F}^{m\times n}$，定义了矩阵的加法运算并满足一定性质，构成代数系统。
- 数域 $\mathbb{F}$ 上的 n 阶方阵的全体 $\mathbb{F}^{n\times n}$，不仅对于矩阵加法运算构成代数系统，而且还定义了矩阵乘法运算，也构成代数系统。

下面给出代数系统的定义。

如果一个非空集合 S 上定义了一个（或几个）运算，它（或它们）满足一定的基本性质，则称这种具有一定运算的集合为**代数系统**

二元运算的定义：非空集合 S 上的一个运算，是指 S×S 到 S 的一个映射，它使 S 中任意两个元都有 S 中的一个唯一确定的元与他们对应。

非空集合上的运算具有三个特性：

1）运算的**封闭性**；

2）运算的**顺序性**；

3）运算结果的**唯一性**。

接下来，我们深入地介绍一下群，环，域这三种代数系统。

11.0.1 代数结构速查总表

> 群、环、域之间的递进关系可以概括为：**群只有一种运算，环有两种运算（加法 + 乘法），域是”能做除法的环”。**

判断流程图：

1. 有几个运算？

1 个运算 → 检查：结合律？有单位元？有逆元？

全满足 → 群 → 再加：交换律？→ Abel 群

满足前 2 → 幺半群

只满足第 1 → 半群

表 11.1:

结构	运算	核心要求	最简单例子	不构成的例子
半群	1 个	结合律	$(\mathbb{N},+)$	—
幺半群	1 个	结合律 + 单位元	$(\mathbb{N},+)$ 有单位元 0	—
群	1 个	结合律 + 单位元 + 逆元	$(\mathbb{Z},+)$	$(\mathbb{Z}^+,\times)$ 无逆元
Abel 群	1 个	群的 3 条 + 交换律	$(\mathbb{Z},+)$	$(GL_n(\mathbb{R}),\times)$ 矩阵乘法不交换
环	2 个 (+ 和 ×)	加法 Abel 群 + 乘法半群 + 分配律	$(\mathbb{Z},+,\times)$	$\mathbb{R}[x]_n$ 乘法不封闭
交换环	2 个	环 + 乘法交换律	$(\mathbb{Z},+,\times)$	$(M_n(\mathbb{R}),+,\times)$
域	2 个	环 + 乘法单位元 + 乘法逆元 + 乘法交换律	$(\mathbb{Q},+,\times)$	$(\mathbb{Z},+,\times)$ 2 没有逆元

2 个运算 → 先看加法是否构成 Abel 群？

是 → 再看乘法：结合律？分配律？ → 环

乘法有交换律？ → 交换环

乘法有单位元？非零元有逆元？交换？ → 域

否则 → 环

否 → 连环都不是

快速判断技巧：

- $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ 对 $+$ 都是 Abel 群
- $\mathbb{Z}$ 对 $+,\times$ 是整环（交换环 + 无零因子），但不是域
- $\mathbb{Q},\mathbb{R},\mathbb{C}$ 对 $+,\times$ 是域
- 矩阵集 $\mathbb{F}^{n\times n}$ 对 $+$ 是 Abel 群，对 $+,\times$ 是环（$n>1$ 时非交换）
- $GL_n(\mathbb{R})$（可逆矩阵）对 $\times$ 是群，非 Abel
- $SO(n), SE(3)$ 对矩阵乘法是群（几何意义：旋转/刚体运动）

11.1 【重点】群

群：若在一个非空集合 G 上定义了一个运算，记为”$\cdot$”，称为乘法，并满足下列条件：

1. **结合律**成立，对任意 $a,b,c\in G$，有

$$a\cdot(b\cdot c)=(a\cdot b)\cdot c$$

1. 有**单位元素**（**幺元**）$e\in G$，满足：对任意 $a\in G$，有

$$a\cdot e=e\cdot a=a$$

1. G 中任意元素 a 均有**逆元素** $a^{-1}\in G$，满足

$$a\cdot a^{-1}=a^{-1}\cdot a=e$$

则称 G 对于运算“$\cdot$”构成一个**群**，或简称 G 为一个群。

只满足 1) 为**半群**，只满足 1) 和 2) 为**带幺半群**。

> 这里，群只是要求有一种符合上述要求的运算即可。这里称为“乘法”，但并不一定是我们熟悉的“标量乘法”、“矩阵乘法”。这里的“乘法”甚至可以是“加法”。比如说在一个 Abel 群中，“加法”亦是乘法。而在集合 $\mathbb{R}\setminus\{0\}$ 中，我们平时所熟知的“乘法”，反而成了此时这个 Abel 群中的“加法”。“乘即是加，加即是乘。”如果一个运算被命名为“加法”，就要求它具有交换律；而如果一个运算被命名为“乘法”，便不预先承认它有交换律。

若上述定义的运算为加法，则将运算符号“$\cdot$”改为“$+$”，幺元改为**零元**，逆元改为**负元**。

若群 G 对于上述运算还有交换律成立，即对于任意 $a,b\in G$，有 $a\cdot b=b\cdot a$，则称 G 为**交换群**（或称 Abel 群）。

群是一种代数系统，它是由一个非空集合与一个运算构成的。若集合不同，构成的群当然不同。对同一个集合，运算不同则构成的群也不同。

群的**实例**：

- 单位元群，即只有一个元素的群。如数集 $\{1\}$ 对于数的乘法，构成一个单位元群。
- 加法群：$\mathbb{Z}$、$\mathbb{C}$、$\mathbb{R}$、$\mathbb{Q}$、$\mathbb{R}^n$、$\mathbb{R}[x]_n$（这是指所有 n 次 1 元多项式）、$\mathbb{R}^{m\times n}$
- 乘法群：$GL_n(\mathbb{R})$（General Linear，是所有 n 阶实数可逆矩阵构成的集合，并且在这个集合上定义了矩阵乘法）
- 不构成群：$\mathbb{Z}^+$ 关于数的加法或乘法均不构成群，因为没有逆元。

按群 G 具有元素的个数（元数）多少分为**无限群**与**有限群**。

【不考】有限群实例：含有 n 个元素的有限集上的所有可逆映射（称为 n 元置换），对于映射的乘法构成一个群，称为 n **元置换群**，或称为 n **次对称群**，记为 S_n。S_n 的每一个元素可以表示成一个 n 元置换：

$$\sigma=\begin{bmatrix}1 & 2 & 3 & \dots & n\\ j_1 & j_2 & j_3 & \dots & j_n\end{bmatrix}$$

其中，$j_1,j_2,j_3,\dots,j_n$ 为 $1,2,3,\dots,n$ 的某个排列。

讨论： n 次对称群是否为 Abel 群？其元数为多少？

无限群实例：非空集合 U 到其自身的所有可逆映射（或称为变换），对于映射的乘法构成群，称为**集合 U 的全变换群**，记为 S_U。当 U 为无限集时，S_U 为无限群。S_U 的非空子集，若对于映射的乘法也构成群，则称为**变换群**。

群有以下简单性质：

(1) 任意一个群的单位元是唯一的。群的任意元的逆元也是唯一的。

> **【重点证明】单位元的唯一性**（考试高频简单证明题）：
>
> **证：**设 e 和 e' 都是群 G 的单位元。- 因为 e 是单位元，所以对任意 $g\in G$，有 $e\cdot g=g\cdot e=g$。取 $g=e'$，得 $e\cdot e'=e'\cdot e=e'$。- 因为 e' 也是单位元，所以对任意 $g\in G$，有 $e'\cdot g=g\cdot e'=g$。取 $g=e$，得 $e'\cdot e=e\cdot e'=e$。- 比较两式：$e=e\cdot e'=e'$。

故 $e = e'$，单位元唯一。□

【重点证明】逆元的唯一性：

证：设 $a \in G$，b 和 c 都是 a 的逆元，即 $a \cdot b = b \cdot a = e$，$a \cdot c = c \cdot a = e$。

则 $b = b \cdot e = b \cdot (a \cdot c) = (b \cdot a) \cdot c = e \cdot c = c$。

故 $b = c$，逆元唯一。□

(2) 若 $(G, \cdot)$ 是一个群，则对任意 $a, b \in G$，方程

$$a \cdot x = b \quad 与 \quad y \cdot a = b$$

均有唯一解。

这里就可以联想到 $GL_n(\mathbb{R})$

(3) **消去律**成立，即

$$a \cdot x = a \cdot y \Rightarrow x = y$$

$$x \cdot a = y \cdot a \Rightarrow x = y$$

群中可以定义幂：

$$a^1 = a,\ a^{n+1} = a^n \cdot a,$$

$$a^0 = e,\ a^{-n} = (a^{-1})^n,\ n > 0$$

如果群 G 的非空子集 H 对于 G 上定义的运算也构成一个群，则称 H 为 G 的**子群**。

非常重要！

判断子群的几个条件

1. 对**一种**运算的**封闭性**
2. 有**单位元/零元**
3. 有**逆元/负元**

定理 2 群 G 的非空子集 H 是 G 的子群的充要条件是：

(1) 对任意 $a,b\in H$，有 $a\cdot b\in H$；

(2) 对任意 $a\in H$，有 $a^{-1}\in H$.

定理 3 群 G 的非空子集 H 是 G 的子群的充要条件是：对任意 $a,b\in H$，有 $a\cdot b^{-1}\in H$.

证充分性：由于 H 非空，所以至少应含有一个元素 a，于是

$$e=a\cdot a^{-1}\in H$$

又由 $a,e\in H$，可得

$$a^{-1}=e\cdot a^{-1}\in H$$

对任意 $a,b\in H$，由上知 $b^{-1}\in H$，于是

$$a\cdot b=a\cdot(b^{-1})^{-1}\in H$$

由定理 2 可知，H 是 G 的子群。

例：验证 $H=\{a+bi\mid a,b\in\mathbb{R},a^2+b^2=1\}$（单位圆上的复数）在复数乘法下构成群 $(\mathbb{C}\setminus\{0\},\times)$ 的子群。

证（使用子群判定定理：$\forall x,y\in H,xy^{-1}\in H$）：

任取 $z_1=a_1+b_1i\in H$，$z_2=a_2+b_2i\in H$，则 $a_1^2+b_1^2=1,a_2^2+b_2^2=1$。

$z_2^{-1}=\frac{a_2-b_2i}{a_2^2+b_2^2}=a_2-b_2i$（因为 $a_2^2+b_2^2=1$）

$z_1z_2^{-1}=(a_1+b_1i)(a_2-b_2i)=(a_1a_2+b_1b_2)+(b_1a_2-a_1b_2)i$

验证模长：$(a_1a_2+b_1b_2)^2+(b_1a_2-a_1b_2)^2=(a_1^2+b_1^2)(a_2^2+b_2^2)=1\times1=1$

故 $z_1z_2^{-1}\in H$，由子群判定定理，H 是子群。

> 这个子群在几何上就是复平面上的**单位圆群** $U(1)$。后面在三维刚体运动中，单位四元数也构成一个类似的” 单位球面群” S^3，它是 $SU(2)$，且是 $SO(3)$ 的二重覆盖。

例在群 $\mathbb{Z}$ 中，非空子集

$$n\mathbb{Z}=\{na\mid a\in\mathbb{Z},\ n\text{ 为一个整数}\}$$

对于 $\mathbb{Z}$ 上定义的数的加法，显然构成 $\mathbb{Z}$ 的子群。

这里其实是左陪集，后面将会介绍左陪集的概念。

例 $\mathbb{R}[x]_n$ 是 $\mathbb{R}[x]$ 的一个子群。

理由：

封闭性：任意两个次数不超过 n 的多项式相加，其结果的次数显然仍不超过 n；

零元存在性：父群的零元（零多项式 0）属于该子集；

逆元封闭性：任一该子集中的多项式 $f(x)$，其负元 $-f(x)$ 的次数保持不变，依然属于该子集。

综上，$\mathbb{R}[x]_n$ 构成 $\mathbb{R}[x]$ 的子群。

设 G 是任意一个群，e 是 G 的单位元，则单位元群 $\{e\}$ 是 G 的子群，且 G 本身也构成 G 的子群。这两个特殊的子群，称为 G 的**平凡子群**。除此之外，G 的其他子群 H 可称为**非平凡子群**。

特殊的反倒平凡了

【不考】定义设 H 是群 G 的子群，对任意给定的 $a \in G$，记

$$aH = \{a \cdot h \mid \text{任意} h \in H\}$$

与

$$Ha = \{h \cdot a \mid \text{任意} h \in H\}$$

分别称为 H 的**左陪集**与**右陪集**（不考）。

这里的 $\cdot$，是 H 群中定义的乘法

定义若群 G 中子群 H 的任意左陪集同时又是 H 的右陪集，也就是说，H 能够与 G 的任意元素 a 交换，即对任意 $a \in G$ 有

$$aH = Ha$$

则称 H 为 G 的**正规子群**。

交换群的任意子群均是正规子群。

正规子群 H 可以定义左陪集的乘法运算：

$$aH \cdot bH = aHb \cdot H = abH \cdot H = abH \quad \text{对任意} a, b \in G$$

G 中所有 H 的左陪集构成的集合对于上述乘法运算构成群。

【不考】定义设 G 与 G' 是两个群，如果有一个 G 到 G' 上的一一对应 σ，对于 G 与 G' 的运算，有

$$\sigma(x \cdot y) = \sigma(x) \circ \sigma(y)$$

对任意 $x, y \in G$ 均成立，则称 G **同构**于 G'（不考），记为 $G \cong G'$，称满足上述条件的映射为**同构映射**（简称同构）。

同构把 G 的单位元变为 G' 的单位元，把 G 的逆元变为 G' 的逆元。

> **直观理解**：同构的本质是" 换了个名字，但结构完全一样"。就像你把一本书从中文翻译成英文——每个字都换了，但故事的结构、情节的逻辑完全保留。两个同构的群，从抽象代数的角度看是**同一个东西**，只是里面的元素叫法不同。

例试证明群 $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$。

证：任取实数 x，令 $\sigma(x) = e^x$。显然 σ 是一个 $(\mathbb{R}, +)$ 到 $(\mathbb{R}^+, \cdot)$ 的一一对应，且

$$\sigma(x + y) = e^{x+y} = e^x e^y = \sigma(x)\sigma(y)$$

对任意实数 x, y 均成立。□

> 这个例子非常漂亮——它告诉我们加法和乘法在某种意义下是" 同一个结构"。你平时觉得加法和乘法很不一样对吧？但在同构的映射下，实数加法本质上和正实数乘法是一回事。这也就是为什么对数尺可以把乘法变成加法。
>
> 特别提醒：同构的概念在后面的**三维刚体运动**中还会出现——$\mathfrak{so}(3)$（李代数）和 $\mathbb{R}^3$ 的叉积空间、$SO(3)$（李群）之间的关系，本质上也是同构在起作用。

11.2 【重点】环

群只有**一种**运算。但很多我们熟悉的数学对象（如整数、多项式）同时有加法和乘法两种运算。**环**就是在这个需求下诞生的代数结构。

定义设非空集合 R 上定义了两个运算，一个称为加法（用 $+$ 表示），一个称为乘法（用 $\cdot$ 表示），它们满足以下条件：

1. 对于加法运算，R 构成**加法群**（即加法满足结合律、有零元、有负元、有交换律）；

2. 对于乘法运算有**结合律**（构成半群），即对任意 $a,b,c\in R$，有

$$a\cdot(b\cdot c)=(a\cdot b)\cdot c$$

1. 对于加法与乘法运算有**分配律**，即对于任意 $a,b,c\in R$，有

$$a\cdot(b+c)=a\cdot b+a\cdot c$$

$$(b+c)\cdot a=b\cdot a+c\cdot a$$

则称 R 为**环**。

> **记忆技巧**：环 = 加法 Abel 群 + 乘法半群 + 分配律。你可以这样记：环就是” 可以加加减减，也可以乘，而且乘法和加法之间还能分配” 的集合。

若环 R 又满足**乘法交换律**，即对任意 $a,b\in R$，有 $a\cdot b=b\cdot a$，则称 R 为**交换环**。

环的实例：

- 全体整数集 $\mathbb{Z}$ 对于数的加法与乘法——**整数环**（这是交换环）
- 一元实系数多项式 $\mathbb{R}[x]$ 的全体对于多项式的加法与乘法——**多项式环**（交换环）
- $\mathbb{R}[x]_n$（次数不超过 n 的多项式）对于多项式的加法与乘法——**不构成环！**因为乘法不封闭（两个 n 次多项式相乘得到 $2n$ 次多项式，跑出集合了）
- $M_n(\mathbb{Z})$（元素为整数的 n 阶方阵全体）对于矩阵加法和乘法——**全矩阵环**（注意：$n>1$ 时非交换！因为矩阵乘法不交换）

> 这里有一个很微妙的地方：为什么多项式环是交换环，但矩阵环不是？因为多项式的乘法本质上就是系数的卷积，自然是交换的；而矩阵乘法对应的是线性变换的复合，复合的顺序当然不能随便交换。这说明**环的结构反映了运算本身的性质**。

零环：设 G 为一个加法群，在 G 上定义乘法为：对任意 $a,b\in G$，$a\cdot b=o$（o 是 G 的零元）。这满足结合律与分配律，所以 G 构成一个环。如集合 $\{0\}$ 对于数的加法与乘法构成零环。

> 零环是最” 无聊” 的环——所有乘法结果都是零。但它作为一个极端例子，可以帮助我们检验很多定理的边界条件。

环的乘法性质（重要！与群不同）：

因环 R 是一个加法群，所以有零元 o 与负元 $-a$ 和加法群的一切性质。但与乘法有关的性质需要特别注意：

1. $o\cdot a=a\cdot o=o$ 对任意 $a\in R$ 均成立（零元乘以任何东西都是零——这和普通数的乘法一样）；

2. $(-a)\cdot b = a\cdot(-b) = -(a\cdot b)$，且 $(-a)\cdot(-b) = a\cdot b$（负负得正）；
3. **乘法交换律一般不成立**（这与群不同，群要求 Abel 才有交换律，环也不默认交换）；
4. **乘法消去律一般不成立**——即当 $a \neq o$ 时，由 $a\cdot x = a\cdot y$ **不一定**能推出 $x = y$；
5. 由 $a\cdot b = o$ **不一定**能推出 $a = o$ 或 $b = o$。

> 第 4、5 条是环和”我们熟悉的数”之间最大的区别！在整数中，如果 $2x = 2y$，消去 2 一定得到 $x = y$。但在一般的环中这不一定成立。比如在矩阵环中，即使 $A \neq O$，$AX = AY$ 也不意味着 $X = Y$（除非 A 可逆）。
>
> 第 5 条也很反直觉：在模 12 的整数环 $\mathbb{Z}_{12}$ 中，$3\times 4 = 12 \equiv 0 \pmod{12}$，但 $3 \neq 0$ 且 $4 \neq 0$。这种非零元乘起来等于零元的现象，引出了**零因子**的概念——这是环论中的一个核心议题。

子环：若环 R 的子集 S 对于定义在环 R 上的两个运算也构成环，则称 S 为 R 的**子环**。

定理环 R 的非空子集 S 是 R 的子环的充要条件是：

1. S 对加法运算构成群；
2. S 对乘法运算具有封闭性。

全体偶数集 $2\mathbb{Z}$ 构成整数环 $\mathbb{Z}$ 的子环。

11.3 【重点】域

现在我们已经有了环——它能做加减法和乘法。但我们还缺什么？**除法**。在整数环 $\mathbb{Z}$ 中，$3\div 2$ 就不再是整数了。这促使我们迈向更强的结构：**域**。

定义设 F 是一个至少含有两个元素的环，如果 F 对于乘法还满足以下条件：

1. 有**单位元** e，即对任意 $a \in F$，有 $a\cdot e = e\cdot a = a$；
2. 除零元外其余元素均有**逆元**，即对任意 $a(\neq o) \in F$，均有 $a^{-1} \in F$ 存在，使 $a\cdot a^{-1} = a^{-1}\cdot a = e$；
3. **交换律**成立，即对于任意 $a, b \in F$，有 $a\cdot b = b\cdot a$。

则称 F 为**域**。

> **一句话总结**：域 = 加法 Abel 群 + 非零元乘法 Abel 群 + 分配律。也就是说，在域里面，你可以自由地做加减乘除（除以零除外），就像你在 $\mathbb{Q}$、$\mathbb{R}$、$\mathbb{C}$ 中习惯的那样。域是我们在初等代数中最熟悉的代数结构。

域与环的关系——递进式理解：

我们不妨用一张”进化图”来理解代数结构的递进关系：

$$\text{半群} \xrightarrow{+\text{幺元}} \text{带幺半群} \xrightarrow{+\text{逆元}} \text{群} \xrightarrow{+\text{交换律}} \text{Abel 群}$$

$$\text{Abel 加法群} + \text{乘法半群} + \text{分配律} = \text{环}$$

$$\text{环} + \text{乘法幺元} + \text{乘法逆元} + \text{乘法交换律} = \text{域}$$

从这条链可以看出：域是最高级、条件最苛刻的代数结构。整数集 $\mathbb{Z}$ 只是环而不是域（因为 2 没有乘法逆元）。有理数集 $\mathbb{Q}$ 才是域。

域的实例：

- $\mathbb{Q}$、$\mathbb{R}$、$\mathbb{C}$ 都是域
- 由两个元素组成的域 $F = \{\text{单}, \text{双}\}$，定义加法：单 + 单 = 双 + 双 = 双，单 + 双 = 双 + 单 = 单；定义乘法：单 • 单 = 单，单 • 双 = 双 • 双 = 双 • 单 = 双。这是最小的域（二元域，记作 $\mathbb{F}_2$ 或 $GF(2)$）
- 全体数量阵构成 $M_n(F)$ 的一个子域
- 在 $M_n(F)$ $(n > 1)$ 中，全体对角阵虽然有单位元 I_n 且构成交换子环，但**不构成子域**（因为对角线上有零的对角阵不可逆）

11.3.1 数域——域的”数”的侧面

PPT 在讲群环域之前先介绍了**数域**。从代数结构的角度看，数域就是”由数构成的域”。但 PPT 给出了一个更具体的定义。

定义 1：设 $\mathbb{F}$ 是复数域 $\mathbb{C}$ 的一个子集，如果：

1. $\mathbb{F}$ 中至少含有一个非零数；
2. 对 $\mathbb{F}$ 中任意两个数 a, b，$a+b, a-b, a\cdot b$ 都在 $\mathbb{F}$ 中；当 $b \neq 0$ 时 $\frac{a}{b}$ 也在 $\mathbb{F}$ 中。

则称 $\mathbb{F}$ 是一个**数域**。

换句话说，数域就是对加减乘除（除数非零）**封闭**的复数子集。

例：令 $\mathbb{H} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$，则 $\mathbb{H}$ 是一个数域。

验证：任取 $a_1 + b_1\sqrt{2}, a_2 + b_2\sqrt{2} \in \mathbb{H}$，加减乘的结果显然仍是 $a + b\sqrt{2}$ 的形式。除法的封闭性：

$$\frac{a_1 + b_1\sqrt{2}}{a_2 + b_2\sqrt{2}} = \frac{(a_1 + b_1\sqrt{2})(a_2 - b_2\sqrt{2})}{a_2^2 - 2b_2^2} = \frac{a_1a_2 - 2b_1b_2}{a_2^2 - 2b_2^2} + \frac{b_1a_2 - a_1b_2}{a_2^2 - 2b_2^2}\sqrt{2} \in \mathbb{H}$$

（当 $a_2 + b_2\sqrt{2} \neq 0$ 时，分母 $a_2^2 - 2b_2^2 \neq 0$——因为 $\sqrt{2}$ 是无理数。）

定理 1（常考！）：任何数域都包含有理数域 $\mathbb{Q}$。即 $\mathbb{Q}$ 是**最小的数域**。

证明思路：设 $\mathbb{F}$ 为任意数域。由定义，$\mathbb{F}$ 中至少有一个非零数 a。由除法的封闭性，$a/a = 1 \in \mathbb{F}$。由加法的封闭性，$1+1=2 \in \mathbb{F}$，$1+2=3 \in \mathbb{F}$……由此所有正整数 $\in \mathbb{F}$。再由减法的封闭性，$0 \in \mathbb{F}$ 且负整数 $\in \mathbb{F}$，故 $\mathbb{Z} \subseteq \mathbb{F}$。再由除法的封闭性，任意两个整数（除数非零）之商 $\in \mathbb{F}$，即 $\mathbb{Q} \subseteq \mathbb{F}$。□

推论：不存在比 $\mathbb{Q}$ 更小的数域。任何数域都" 至少" 包含有理数。这也是为什么 $\mathbb{Q}$ 被称为**最小数域**。

常见的数域：$\mathbb{Q}$、$\mathbb{R}$、$\mathbb{C}$ 等都是数域。但 $\mathbb{Z}$ 不是数域（2 没有倒数在 $\mathbb{Z}$ 中——这个例子再一次说明了域和环的区别：$\mathbb{Z}$ 是环不是域）。

最后一条很有意思：对角阵在矩阵环里已经" 足够好" 了（有单位元、交换），但依然不是域——因为有些对角阵没有逆。这说明逆元的存在性是一个很高的门槛。

定义如果环 R 的子环 R_1 构成域，则称 R_1 为 R 的**子域**。若 R 也为域，也称 R 为其子域 R_1 的**扩域**。

实数域 $\mathbb{R}$ 是复数域 $\mathbb{C}$ 的子域；有理数域 $\mathbb{Q}$ 是实数域 $\mathbb{R}$ 的子域，当然也是复数域 $\mathbb{C}$ 的子域。

域的同构：域也是环，所谓域之间的同构就是它们作为环的同构。同构的域具有相同的代数性质，从抽象观点来看可以不加区别。

有意思的是，全体二阶数量阵构成的域和原来的数域 F 是同构的（映射 $\sigma(\alpha I_2) = \alpha$）。这意味着从代数结构的角度看，一个数 α 和一个 αI_2 的数量阵是" 同一个东西的两种写法"。

第 12 章 三维空间刚体运动

这是笔者认为本课程最精彩的部分之一。它把前面学的群论、矩阵分解、矩阵指数等知识全部串了起来，实实在在地应用到了机器人学和计算机视觉中。你会发现，抽象的数学在这里变得无比具体——旋转就是矩阵，平移就是加法，而" 群" 这个概念自然地出现在了 $SO(3)$ 和 $SE(3)$ 的定义中。

12.1 预备知识：向量的内积与外积

在三维空间中，两个向量 $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{R}^3$ 之间有两种基本的乘积运算：

内积：$\boldsymbol{a} \cdot \boldsymbol{b} = \boldsymbol{a}^T \boldsymbol{b} = \|\boldsymbol{a}\| \|\boldsymbol{b}\| \cos \theta_{\boldsymbol{ab}}$——得到一个**标量**，反映了两向量方向的一致性。

外积（叉积）：$\boldsymbol{a} \times \boldsymbol{b}$——得到一个**向量**，垂直于 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 构成的平面，方向由右手定则确定，模长为 $\|\boldsymbol{a}\| \|\boldsymbol{b}\| \sin \theta_{\boldsymbol{ab}}$。

这里引入一个非常重要的工具：**反对称矩阵**。对于向量 $\boldsymbol{a} = [a_1, a_2, a_3]^T$，定义其反对称矩阵为：

$$\boldsymbol{a}^\wedge = \begin{bmatrix} 0 & -a_3 & a_2 \\ a_3 & 0 & -a_1 \\ -a_2 & a_1 & \end{bmatrix}$$

符号 $\wedge$（wedge）把向量映射为一个反对称矩阵。这个映射是一一对应的：给定任意一个 3×3 反对称矩阵，你可以唯一地还原出原来的向量。

反对称矩阵的一个关键性质是：**叉积可以写成矩阵乘法**，即

$$\boldsymbol{a} \times \boldsymbol{b} = \boldsymbol{a}^\wedge \boldsymbol{b}$$

这看起来只是换了个写法，但实际上非常重要——它把非线性的叉积运算变成了线性的矩阵乘法！在后面的旋转求导中，这会大大简化计算。

12.2 旋转矩阵与 $SO(3)$

12.2.1 从基变换到旋转矩阵

考虑 $\mathbb{R}^3$ 中两组不同的单位正交基 $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3\}$ 和 $\{\boldsymbol{e}'_1, \boldsymbol{e}'_2, \boldsymbol{e}'_3\}$。同一个向量 $\boldsymbol{a}$，在两组基下的坐标分别为 $[a_1, a_2, a_3]^T$ 和 $[a'_1, a'_2, a'_3]^T$：

$$\boldsymbol{a} = [\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3] \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} = [\boldsymbol{e}'_1, \boldsymbol{e}'_2, \boldsymbol{e}'_3] \begin{bmatrix} a'_1 \\ a'_2 \\ a'_3 \end{bmatrix}$$

通过左边同时左乘 $[\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3]^T$，可以导出：

$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} = \underbrace{\begin{bmatrix} \boldsymbol{e}_1^T \boldsymbol{e}'_1 & \boldsymbol{e}_1^T \boldsymbol{e}'_2 & \boldsymbol{e}_1^T \boldsymbol{e}'_3 \\ \boldsymbol{e}_2^T \boldsymbol{e}'_1 & \boldsymbol{e}_2^T \boldsymbol{e}'_2 & \boldsymbol{e}_2^T \boldsymbol{e}'_3 \\ \boldsymbol{e}_3^T \boldsymbol{e}'_1 & \boldsymbol{e}_3^T \boldsymbol{e}'_2 & \boldsymbol{e}_3^T \boldsymbol{e}'_3 \end{bmatrix}}_{\boldsymbol{R}} \begin{bmatrix} a'_1 \\ a'_2 \\ a'_3 \end{bmatrix}$$

这个矩阵 $\boldsymbol{R}$ 就是**旋转矩阵**。它的每个元素都是两组基向量的内积，因而也是两个基向量夹角的余弦值，所以 $\boldsymbol{R}$ 也称为**方向余弦矩阵**。

> 这个推导非常自然：旋转矩阵本质上就是在描述" 新坐标系的基向量在旧坐标系里分别指向什么方向"。$\boldsymbol{R}$ 的第 i 列就是 $\boldsymbol{e}'_i$ 在旧基下的坐标。想通这一点，你对旋转矩阵的理解就上了一个层次。

12.2.2 $SO(n)$ 的定义

旋转矩阵具有两个关键性质：

1. **正交性**：$\boldsymbol{R}\boldsymbol{R}^T = \boldsymbol{I}$（因为两组标准正交基的乘积还是标准正交基）
2. **行列式为 1**：$\det(\boldsymbol{R}) = 1$（保证旋转变换保持手性，不产生镜像反射）

反之，任何满足这两个条件的矩阵也是一个旋转矩阵。因此，n 维旋转矩阵的集合定义为：

$$SO(n) = \{\boldsymbol{R} \in \mathbb{R}^{n \times n} \mid \boldsymbol{R}\boldsymbol{R}^T = \boldsymbol{I}, \det(\boldsymbol{R}) = 1\}$$

$SO(n)$ 表示**特殊正交群**（Special Orthogonal Group）。其中 $SO(3)$ 就是三维空间的旋转。

> **callback 到群论**：$SO(n)$ 关于矩阵乘法是否构成群？我们来验证：- 封闭性：两个正交且行列式为 1 的矩阵相乘，结果仍是正交且行列式为 1 - 结合律：矩阵乘法天然满足 - 幺元：单位矩阵 $\boldsymbol{I}$ 满足条件 - 逆元：$\boldsymbol{R}^{-1} = \boldsymbol{R}^T$，而行列式 $\det(\boldsymbol{R}^T) = \det(\boldsymbol{R}) = 1$
>
> 所以 $SO(n)$ 确实是一个群！而且注意，它不是 Abel 群——三维旋转的先后顺序不同，结果通常不同（你可以拿手边的手机转一转试试：先绕 x 轴转 90° 再绕 y 轴转 90°，和先绕 y 轴再绕 x 轴，手机最终的姿态是不同的）。

$\boldsymbol{a} = \boldsymbol{R}\boldsymbol{a}'$ 表示坐标 $\boldsymbol{a}'$ 通过 $\boldsymbol{R}$ 变换为坐标 $\boldsymbol{a}$，其逆变换 $\boldsymbol{R}^T$ 描述了一个相反的旋转：$\boldsymbol{a}' = \boldsymbol{R}^{-1}\boldsymbol{a} = \boldsymbol{R}^T\boldsymbol{a}$。

> 小 tip：实际应用中，$\boldsymbol{a}$ 和 $\boldsymbol{a}'$ 可能是同一个向量在不同坐标系下的坐标，也可能是同一个坐标系中的向量经过了旋转。前者叫" 坐标变换"（被动旋转），后者叫" 点变换"（主动旋转）。在学习中注意区分这两种视角，虽然在矩阵形式上是一致的。

12.3 欧式变换与 $SE(3)$

仅有旋转还不够——真实的刚体运动还包括**平移**。

一个完整的欧式变换（旋转 + 平移）可以表示为：

$$\boldsymbol{a}' = \boldsymbol{R}\boldsymbol{a} + \boldsymbol{t}$$

其中 $\boldsymbol{t} \in \mathbb{R}^3$ 为平移向量。

但这里有个麻烦：如果连续做两次变换，

$$\boldsymbol{b} = \boldsymbol{R}_1\boldsymbol{a} + \boldsymbol{t}_1, \quad \boldsymbol{c} = \boldsymbol{R}_2\boldsymbol{b} + \boldsymbol{t}_2$$

那么从 $\boldsymbol{a}$ 到 $\boldsymbol{c}$ 的变换为：

$$\boldsymbol{c} = \boldsymbol{R}_2\boldsymbol{R}_1\boldsymbol{a} + \boldsymbol{R}_2\boldsymbol{t}_1 + \boldsymbol{t}_2$$

> 注意：两次旋转加平移的复合，**不是简单的线性关系！**如果你只用一个 3×3 矩阵，只能表示旋转；加上平移向量后，复合起来非常不便。这就是引入**齐次坐标**的动机。

齐次坐标的妙处：在三维向量的末尾加 1，将其变为四维向量：

$$\begin{bmatrix} \boldsymbol{a}' \\ 1 \end{bmatrix} = \begin{bmatrix} \boldsymbol{R} & \boldsymbol{t} \\ \boldsymbol{0}^T & 1 \end{bmatrix} \begin{bmatrix} \boldsymbol{a} \\ 1 \end{bmatrix} = \boldsymbol{T} \begin{bmatrix} \boldsymbol{a} \\ 1 \end{bmatrix}$$

矩阵 $\boldsymbol{T}$ 称为**变换矩阵**。现在整个关系变成了**线性关系！**两次变换的复合变得极其简洁：

$$\boldsymbol{T} = \boldsymbol{T}_2\boldsymbol{T}_1$$

> 这个技巧太漂亮了——把仿射变换（线性 + 平移）用高一维的线性变换表示出来。这是计算机图形学和机器人学中最常用的技术之一。代价仅仅是在每个向量的末尾多写一个 1。

变换矩阵 $\boldsymbol{T}$ 的逆为：

$$\boldsymbol{T}^{-1} = \begin{bmatrix} \boldsymbol{R}^T & -\boldsymbol{R}^T\boldsymbol{t} \\ \boldsymbol{0}^T & 1 \end{bmatrix}$$

特殊欧式群 $SE(3)$：

$$SE(3) = \left\{ \boldsymbol{T} = \begin{bmatrix} \boldsymbol{R} & \boldsymbol{t} \\ \boldsymbol{0}^T & 1 \end{bmatrix} \in \mathbb{R}^{4\times 4} \mid \boldsymbol{R} \in SO(3), \boldsymbol{t} \in \mathbb{R}^3 \right\}$$

$SE(3)$ 表示**特殊欧式群**（Special Euclidean Group）。同样地，$SE(3)$ 关于矩阵乘法构成群。

> 自由度数：三维旋转有 3 个自由度（但旋转矩阵有 9 个元素，冗余了 6 个）；欧式变换有 6 个自由度（3 旋转 +3 平移，但变换矩阵有 16 个元素，冗余了 10 个）。这就是为什么我们需要更紧凑的旋转表示——接下来要讲的旋转向量、欧拉角和四元数。

12.4 【重点】罗德里格斯公式（Rodrigues' Formula）

既然旋转只有 3 个自由度，有没有办法只用 3 个数来表示旋转？有——**旋转向量**（或称轴角，Angle-Axis）。

基本思想：任何三维旋转都可以描述为绕某个单位向量 $\boldsymbol{n}$（旋转轴）旋转某个角度 θ。因此，可以用一个向量 $\boldsymbol{\phi} = \theta \boldsymbol{n}$ 来紧凑地表示旋转——方向是旋转轴，长度是旋转角。恰好 3 维。

12.4.1 从旋转向量到旋转矩阵：罗德里格斯公式

$$\boxed{\boldsymbol{R} = \cos\theta \cdot \boldsymbol{I} + (1 - \cos\theta)\boldsymbol{n}\boldsymbol{n}^T + \sin\theta \cdot \boldsymbol{n}^\wedge}$$

> 这个公式是本课程最重要的公式之一！它建立了旋转向量和旋转矩阵之间的桥梁。让我们仔细品味每一项的含义：- $\cos\theta \cdot \boldsymbol{I}$：单位矩阵的缩放，这是旋转的" 保底" 成分——即使不转（$\theta = 0$），$\boldsymbol{R} = \boldsymbol{I}$ - $(1 - \cos\theta)\boldsymbol{n}\boldsymbol{n}^T$：沿旋转轴方向的投影矩阵，代表旋转轴方向不受旋转影响 - $\sin\theta \cdot \boldsymbol{n}^\wedge$：反对称矩阵部分，是旋转的" 动力" 来源，当 θ 很小时，$\sin\theta \approx \theta$，这一项主导了旋转

12.4.2 从旋转矩阵到旋转向量

对罗德里格斯公式两边求迹：

$$\mathrm{tr}(\boldsymbol{R}) = 3\cos\theta + (1 - \cos\theta)\mathrm{tr}(\boldsymbol{n}\boldsymbol{n}^T) = 3\cos\theta + (1 - \cos\theta)\|\boldsymbol{n}\|^2 = 1 + 2\cos\theta$$

因此：

$$\theta = \arccos \frac{\mathrm{tr}(\boldsymbol{R}) - 1}{2}$$

旋转轴 $\boldsymbol{n}$ 则是 $\boldsymbol{R}$ 的特征值 1 对应的特征向量（因为 $\boldsymbol{R}\boldsymbol{n} = \boldsymbol{n}$，旋转轴上的向量在旋转中不动）：

$$(\boldsymbol{R}-\boldsymbol{I})\boldsymbol{n}=\boldsymbol{0},\quad \|\boldsymbol{n}\|=1$$

> 轴角的表示也有奇异性：转 30° 和转 390°（30° + 360°）的轴角表示是一样的。但实际上这是同一个旋转，所以不算大问题。真正的问题是：当 $\theta=0$ 时，旋转轴 $\boldsymbol{n}$ 是不确定的（任意方向都可以），这会导致数值不稳定。

例：已知旋转向量 $\boldsymbol{\phi}=\theta\boldsymbol{n}$，其中 $\theta=60°$，$\boldsymbol{n}=[0,0,1]^T$（绕 z 轴旋转 60°），求对应的旋转矩阵 $\boldsymbol{R}$。

解：由罗德里格斯公式 $\boldsymbol{R}=\cos\theta\boldsymbol{I}+(1-\cos\theta)\boldsymbol{n}\boldsymbol{n}^T+\sin\theta\cdot\boldsymbol{n}^\wedge$：

- $\cos 60°=0.5,\sin 60°=\frac{\sqrt{3}}{2}$
- $\boldsymbol{n}\boldsymbol{n}^T=\begin{bmatrix}0&0&0\\0&0&0\\0&0&1\end{bmatrix}$
- $\boldsymbol{n}^\wedge=\begin{bmatrix}0&-1&0\\1&0&0\\0&0&0\end{bmatrix}$

$$\boldsymbol{R}=0.5\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}+0.5\begin{bmatrix}0&0&0\\0&0&0\\0&0&1\end{bmatrix}+\frac{\sqrt{3}}{2}\begin{bmatrix}0&-1&0\\1&0&0\\0&0&0\end{bmatrix}$$

$$=\begin{bmatrix}0.5&-\frac{\sqrt{3}}{2}&0\\\frac{\sqrt{3}}{2}&0.5&0\\0&0&1\end{bmatrix}$$

这正是我们熟知的绕 z 轴旋转 60° 的矩阵！

【例 2：旋转矩阵 → 轴角】已知旋转矩阵

$$\boldsymbol{R}=\begin{bmatrix}0&0&1\\0&1&0\\-1&0&0\end{bmatrix}$$

求对应的旋转轴 $\boldsymbol{n}$ 和旋转角 θ。

解：

(1) 求旋转角 θ：

$$\mathrm{tr}(\boldsymbol{R})=0+1+0=1$$

$$\theta = \arccos\frac{\mathrm{tr}(\boldsymbol{R})-1}{2} = \arccos\frac{1-1}{2} = \arccos(0) = \frac{\pi}{2} = 90^\circ$$

(2) 求旋转轴 $\boldsymbol{n}$：解 $(\boldsymbol{R}-\boldsymbol{I})\boldsymbol{n}=\boldsymbol{0}$。

$$\boldsymbol{R}-\boldsymbol{I} = \begin{bmatrix} -1 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & -1 \end{bmatrix}$$

由第一行：$-n_1+n_3=0 \Rightarrow n_1=n_3$；

由第三行：$-n_1-n_3=0 \Rightarrow n_1=-n_3$；

二者同时成立 $\Rightarrow n_1=n_3=0$。

第二行无约束，故 n_2 任意。归一化得 $\boldsymbol{n}=[0,1,0]^T$。

(3) 验证：$\boldsymbol{R}$ 表示绕 y 轴旋转 90°。代入罗德里格斯公式：

$$\boldsymbol{R} = 0\cdot\boldsymbol{I} + (1-0)\boldsymbol{n}\boldsymbol{n}^T + 1\cdot\boldsymbol{n}^\wedge = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{bmatrix}$$

与原矩阵一致，答案正确。□

【例 3：绕任意轴旋转】已知旋转轴 $\boldsymbol{n}=\frac{1}{\sqrt{3}}[1,1,1]^T$，旋转角 $\theta=120^\circ$，求旋转矩阵 $\boldsymbol{R}$。

解：$\cos 120^\circ = -\frac{1}{2}$，$\sin 120^\circ = \frac{\sqrt{3}}{2}$。

$$\boldsymbol{n}\boldsymbol{n}^T = \frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \quad \boldsymbol{n}^\wedge = \frac{1}{\sqrt{3}}\begin{bmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 0 \end{bmatrix}$$

代入罗德里格斯公式 $\boldsymbol{R}=\cos\theta\boldsymbol{I}+(1-\cos\theta)\boldsymbol{n}\boldsymbol{n}^T+\sin\theta\cdot\boldsymbol{n}^\wedge$：

$$\boldsymbol{R} = -\frac{1}{2}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + \frac{3}{2}\cdot\frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} + \frac{\sqrt{3}}{2}\cdot\frac{1}{\sqrt{3}}\begin{bmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} -\frac{1}{2} & 0 & 0 \\ 0 & -\frac{1}{2} & 0 \\ 0 & 0 & -\frac{1}{2} \end{bmatrix} + \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{bmatrix} + \begin{bmatrix} 0 & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

验证：该矩阵将 x 轴转到 y 轴、y 轴转到 z 轴、z 轴转到 x 轴——这正是绕 $[1,1,1]^T$ 方向旋转 120° 的效果（循环置换坐标轴）。$\det(\boldsymbol{R}) = 1$，$\boldsymbol{R}\boldsymbol{R}^T = \boldsymbol{I}$，确认是合法旋转矩阵。

考试提示：罗德里格斯公式及其逆运算（迹公式求 θ + 特征向量求 $\boldsymbol{n}$）是必考内容。旋转角 θ 通常用 $\theta = \arccos\frac{\mathrm{tr}(\boldsymbol{R})-1}{2}$ 求（注意 $\theta \in [0,\pi]$），旋转轴 $\boldsymbol{n}$ 通过解 $(\boldsymbol{R}-\boldsymbol{I})\boldsymbol{n} = \boldsymbol{0}$ 并归一化得到。

12.5 欧拉角与万向锁

旋转矩阵和轴角表示虽然精确，但都有一个共同的缺点：**不够直观**。你能一眼看出一个 3×3 旋转矩阵对应的是什么旋转吗？很难。欧拉角就是为了解决直观性问题而诞生的。

欧拉角的基本思想极其朴素：把一个复杂的三维旋转分解为三次绕坐标轴的简单旋转。例如：

$$\boldsymbol{R} = \boldsymbol{R}_z(\theta_z)\boldsymbol{R}_y(\theta_y)\boldsymbol{R}_x(\theta_x)$$

其中绕 z 轴旋转 α 角度的矩阵为：

$$\boldsymbol{R}_z(\alpha) = \begin{bmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

绕 x 轴、y 轴的旋转矩阵类似。在无人机系统中，常用的欧拉角是 **yaw-pitch-roll**（偏航-俯仰-滚转）：先绕 z 轴转（yaw），再绕旋转后的 y 轴转（pitch），最后绕旋转后的 x 轴转（roll）。

欧拉角极其直观——飞行员、无人机操作员、3D 建模师每天都在用。一个角度对应一个旋转自由度，人类可以直观理解。

但是，欧拉角有一个著名的问题：**万向锁**（Gimbal Lock）。

当俯仰角（pitch）为 ±90° 时，第一次旋转（绕 z 轴）和第三次旋转（绕 x 轴）将使用**同一个轴**，导致丢失一个自由度。这意味着：在这种姿态下，无论你怎么调整 yaw 和 roll，飞机只能绕两个独立的方向旋转，而不是三个。

万向锁不是数学上的”不可能”，而是欧拉角这种**参数化方式**在某些姿态下的退化。旋转本身没有问题——你仍然可以绕任意方向旋转——只是欧拉角的三个参数不再能唯一地表示所有旋转了。这就是为什么在需要全姿态覆盖的场合（如航天器姿态控制），欧拉角不够用。

总结各种旋转表示的问题：

表 12.1:

表示方式	参数个数	问题
旋转矩阵	9	冗余（3 自由度用 9 个数），有正交约束，优化困难
轴角/旋转向量	3	有奇异性（$\theta = 0$ 时轴不确定，周期性问题）
欧拉角	3	万向锁奇异性

有没有一种表示，既**紧凑**（4 个参数，只比最小多 1 个），又**没有奇异性**？答案就是——**四元数**。

12.6 【重点】四元数（Quaternion）

12.6.1 动机：从复数到四元数

在二维平面上，旋转可以用**单位复数**优雅地表示：乘上 $e^{i\theta} = \cos\theta + i\sin\theta$ 就是将向量逆时针旋转 θ 角。四元数是复数的推广——如果把复数理解为”二维旋转的代数”，那么四元数就是”三维旋转的代数”。

四元数的定义：

$$\boldsymbol{q} = s + xi + yj + zk = [s, \boldsymbol{v}]^T$$

其中 $s \in \mathbb{R}$ 是**实部**（标量部分），$\boldsymbol{v} = [x, y, z]^T \in \mathbb{R}^3$ 是**虚部**（向量部分）。三个虚单位满足：

$$i^2 = j^2 = k^2 = ijk = -1$$

注意这里虚单位的乘法**不交换**！$ij = k$ 但 $ji = -k$。这种非交换性恰好对应了三维旋转的非交换性——这不是巧合，而是四元数天然适合描述三维旋转的深层原因。

虚四元数：$s = 0$，即 $\boldsymbol{q} = [0, x, y, z]^T$——只有虚部，用于表示三维空间中的点。

四元数的基本运算：

- **加减法**：逐元素加减
- **数乘**：$k[s, \boldsymbol{v}]^T = [ks, k\boldsymbol{v}]^T$
- **乘法**（核心运算）：

$$\boldsymbol{q}_a\boldsymbol{q}_b = \begin{bmatrix} s_a s_b - \boldsymbol{v}_a^T\boldsymbol{v}_b \\ s_a\boldsymbol{v}_b + s_b\boldsymbol{v}_a + \boldsymbol{v}_a \times \boldsymbol{v}_b \end{bmatrix}$$

注意到叉积 $\boldsymbol{v}_a \times \boldsymbol{v}_b$ 的出现——这解释了为什么四元数乘法不交换。

- **共轭**：$\boldsymbol{q}^* = [s, -\boldsymbol{v}]^T$
- **模长**：$\|\boldsymbol{q}\| = \sqrt{s^2 + x^2 + y^2 + z^2}$
- **逆**：$\boldsymbol{q}^{-1} = \boldsymbol{q}^*/\|\boldsymbol{q}\|^2$（当模长为 1 时，逆就是共轭）

例：已知四元数 $\boldsymbol{q}_1 = [1, 2, 0, 3]^T$（实部为 1，虚部为 $[2, 0, 3]^T$），$\boldsymbol{q}_2 = [0, -1, 0, 2]^T$，求 $\boldsymbol{q}_1\boldsymbol{q}_2$。

解：使用四元数乘法公式 $\boldsymbol{q}_a\boldsymbol{q}_b = \begin{bmatrix} s_a s_b - \boldsymbol{v}_a^T\boldsymbol{v}_b \\ s_a\boldsymbol{v}_b + s_b\boldsymbol{v}_a + \boldsymbol{v}_a \times \boldsymbol{v}_b \end{bmatrix}$：

- $s_a = 1, \boldsymbol{v}_a = [2, 0, 3]^T$
- $s_b = 0, \boldsymbol{v}_b = [-1, 0, 2]^T$
- 实部：$1 \cdot 0 - [2, 0, 3] \cdot [-1, 0, 2] = 0 - (-2 + 0 + 6) = -4$
- 虚部：$1 \cdot [-1, 0, 2]^T + 0 \cdot [2, 0, 3]^T + [2, 0, 3]^T \times [-1, 0, 2]^T$
- 叉积：$\boldsymbol{v}_a \times \boldsymbol{v}_b = \begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ 2 & 0 & 3 \\ -1 & 0 & 2 \end{vmatrix} = [0, -7, 0]^T$
- 虚部 = $[-1, 0, 2]^T + [0, 0, 0]^T + [0, -7, 0]^T = [-1, -7, 2]^T$

故 $\boxed{\boldsymbol{q}_1\boldsymbol{q}_2 = [-4, -1, -7, 2]^T}$。

12.6.2 单位四元数与旋转

核心操作：将一个三维点 $\boldsymbol{p}$ 用虚四元数 $\mathbf{p} = [0, x, y, z]^T$ 表示，用一个单位四元数 $\boldsymbol{q}$（$\|\boldsymbol{q}\| = 1$）表示旋转。则旋转后的点 $\mathbf{p}'$ 为：

$$\mathbf{p}' = \boldsymbol{q}\mathbf{p}\boldsymbol{q}^{-1} = \boldsymbol{q}\mathbf{p}\boldsymbol{q}^*$$

结果的虚部就是旋转后的坐标。这个操作有一个漂亮的性质：结果 $\mathbf{p}'$ 的实部恰好为 0（即仍是虚四元数）。

> 这里可能会觉得奇怪：为什么要左乘 $\boldsymbol{q}$ 又右乘 $\boldsymbol{q}^{-1}$？只乘一次不行吗？
>
> 答案是：不行。如果只做 $\boldsymbol{q}\mathbf{p}$，结果会有一个非零的实部，不再是三维空间中的点。只有 $\boldsymbol{q}\mathbf{p}\boldsymbol{q}^{-1}$ 这种”夹心”结构才能保证旋转后的点仍然在三维子空间中。这个操作在数学上称为**共轭作用**，是群论中的一个基本操作。

四元数到旋转矩阵的变换（定理 6）：

$$\boldsymbol{R} = s^2\boldsymbol{I} + 2s\boldsymbol{v}^\wedge + \boldsymbol{v}\boldsymbol{v}^T + \boldsymbol{v}^\wedge\boldsymbol{v}^\wedge$$

展开写为：

$$\boldsymbol{R} = \begin{bmatrix} 1-2(y^2+z^2) & 2(xy-sz) & 2(xz+sy) \\ 2(xy+sz) & 1-2(x^2+z^2) & 2(yz-sx) \\ 2(xz-sy) & 2(yz+sx) & \end{bmatrix}$$

旋转向量到四元数的转换（定理 7）：

绕单位向量 $\boldsymbol{n}$ 逆时针旋转 θ，对应的单位四元数为：

$$\boldsymbol{q} = \begin{bmatrix} \cos\frac{\theta}{2} \\ \boldsymbol{n}\sin\frac{\theta}{2} \end{bmatrix}$$

> 注意这里的 $\frac{\theta}{2}$！旋转角度在四元数中减半了。从某种意义上说，四元数描述的是”旋转的一半”，而 $\boldsymbol{q}\mathbf{p}\boldsymbol{q}^{-1}$ 这种两次乘法恰好完成了完整的旋转。单位四元数群 S^3 是 $SO(3)$ 的**二重覆盖**——每个旋转对应两个四元数（$\boldsymbol{q}$ 和 $-\boldsymbol{q}$ 表示同一个旋转）。

12.6.3 补充例题

【例 2：用四元数旋转三维点】已知旋转轴 $\boldsymbol{n} = [0,0,1]^T$（绕 z 轴），旋转角 $\theta = 90°$。求对应单位四元数 $\boldsymbol{q}$，并用它旋转点 $\boldsymbol{p} = [1,0,0]^T$。

解：

(1) 旋转向量 → 四元数：

$$\boldsymbol{q} = \begin{bmatrix} \cos\frac{\theta}{2} \\ \boldsymbol{n}\sin\frac{\theta}{2} \end{bmatrix} = \begin{bmatrix} \cos 45° \\ 0 \\ 0 \\ \sin 45° \end{bmatrix} = \begin{bmatrix} \frac{\sqrt{2}}{2} \\ 0 \\ 0 \\ \frac{\sqrt{2}}{2} \end{bmatrix}$$

即 $s = \frac{\sqrt{2}}{2}$，$\boldsymbol{v} = [0, 0, \frac{\sqrt{2}}{2}]^T$。

(2) 将点表示为虚四元数：

$$\mathbf{p} = [0,1,0,0]^T$$

(3) 计算 $\mathbf{p}' = \boldsymbol{q}\mathbf{p}\boldsymbol{q}^*$：先算 $\boldsymbol{q}\mathbf{p}$：

实部：$s \cdot 0 - \boldsymbol{v} \cdot [1,0,0]^T = 0 - 0 = 0$

虚部：$s[1,0,0]^T + 0 \cdot \boldsymbol{v} + \boldsymbol{v} \times [1,0,0]^T$

叉积：$[0, 0, \frac{\sqrt{2}}{2}]^T \times [1,0,0]^T = \begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ 0 & 0 & \frac{\sqrt{2}}{2} \\ 1 & 0 & 0 \end{vmatrix} = [0, \frac{\sqrt{2}}{2}, 0]^T$

虚部 $= [\frac{\sqrt{2}}{2}, 0, 0]^T + [0, 0, 0]^T + [0, \frac{\sqrt{2}}{2}, 0]^T = [\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}, 0]^T$

故 $\boldsymbol{q}\mathbf{p} = [0, \frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}, 0]^T$。

再右乘 $\boldsymbol{q}^* = [\frac{\sqrt{2}}{2}, 0, 0, -\frac{\sqrt{2}}{2}]^T$：

$\mathbf{p}' = (\boldsymbol{q}\mathbf{p})\boldsymbol{q}^*$

实部：$0 \cdot \frac{\sqrt{2}}{2} - [\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}, 0]^T \cdot [0, 0, -\frac{\sqrt{2}}{2}]^T = 0 - 0 = 0$

虚部：$0 \cdot [0, 0, -\frac{\sqrt{2}}{2}]^T + \frac{\sqrt{2}}{2}[\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}, 0]^T + [\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}, 0]^T \times [0, 0, -\frac{\sqrt{2}}{2}]^T$

第一项 = $[0, 0, 0]^T$

第二项 = $[\frac{1}{2}, \frac{1}{2}, 0]^T$

第三项（叉积）：$\begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 \\ 0 & 0 & -\frac{\sqrt{2}}{2} \end{vmatrix} = [-\frac{1}{2}, \frac{1}{2}, 0]^T$

虚部 $= [0, 0, 0]^T + [\frac{1}{2}, \frac{1}{2}, 0]^T + [-\frac{1}{2}, \frac{1}{2}, 0]^T = [0, 1, 0]^T$

故旋转后 $\mathbf{p}' = [0, 0, 1, 0]^T$，即 $\boxed{\boldsymbol{p}' = [0, 1, 0]^T}$。

> **验证**：原点是 $[1, 0, 0]^T$（x 轴正方向），绕 z 轴旋转 $90°$ 应该到达 $[0, 1, 0]^T$（y 轴正方向），结果正确！

【例 3：四元数 → 旋转矩阵】已知单位四元数 $\boldsymbol{q} = [\frac{\sqrt{2}}{2}, 0, 0, \frac{\sqrt{2}}{2}]^T$（即例 2 中的 $\boldsymbol{q}$），求对应的旋转矩阵 $\boldsymbol{R}$。

解：$s = \frac{\sqrt{2}}{2}$，$x = 0$，$y = 0$，$z = \frac{\sqrt{2}}{2}$。

代入四元数 → 旋转矩阵公式：

$$\boldsymbol{R} = \begin{bmatrix} 1 - 2(y^2 + z^2) & 2(xy - sz) & 2(xz + sy) \\ 2(xy + sz) & 1 - 2(x^2 + z^2) & 2(yz - sx) \\ 2(xz - sy) & 2(yz + sx) & \end{bmatrix}$$

计算各元素：

- $R_{11} = 1 - 2(0 + \frac{1}{2}) = 0$
- $R_{12} = 2(0 - \frac{\sqrt{2}}{2} \cdot \frac{\sqrt{2}}{2}) = 2(-\frac{1}{2}) = -1$
- $R_{13} = 2(0 + 0) = 0$
- $R_{21} = 2(0 + \frac{\sqrt{2}}{2} \cdot \frac{\sqrt{2}}{2}) = 2(\frac{1}{2}) = 1$
- $R_{22} = 1 - 2(0 + \frac{1}{2}) = 0$
- $R_{23} = 2(0 - 0) = 0$
- $R_{31} = 2(0 - 0) = 0$
- $R_{32} = 2(0 + 0) = 0$

- $R_{33} = 1 - 2(0 + 0) = 1$

$$\boxed{\boldsymbol{R} = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}}$$

这正是绕 z 轴旋转 90° 的旋转矩阵。□

考试提示：四元数计算题通常考查以下三种转换之一：1. 四元数乘法（直接套公式，注意叉积）2. 旋转向量 → 四元数（$\boldsymbol{q} = [\cos\frac{\theta}{2}, \boldsymbol{n}\sin\frac{\theta}{2}]^T$）3. 四元数 → 旋转矩阵（代入 3×3 展开式）

用四元数旋转一个点（$\mathbf{p}' = \boldsymbol{q}\mathbf{p}\boldsymbol{q}^*$）也是常考操作，核心是两次四元数乘法。

12.6.4 四元数的优势总结

1. **紧凑**：只需 4 个数（旋转矩阵要 9 个）
2. **无奇异性**：不像欧拉角有万向锁，不像轴角在 $\theta = 0$ 处退化
3. **计算高效**：旋转的复合就是四元数乘法，比矩阵乘法快得多
4. **插值方便**：可以在两个四元数之间做球面线性插值（Slerp），生成平滑的旋转动画——这在游戏和动画中至关重要

四元数是由爱尔兰数学家哈密顿（Hamilton）在 1843 年散步时突然想到的，激动得在布鲁厄姆桥上刻下了 $i^2 = j^2 = k^2 = ijk = -1$。但在那个时代，四元数因为过于抽象而被冷落。直到 20 世纪末，计算机图形学和机器人学才发现：四元数几乎是描述三维旋转的最佳工具。一个被遗忘了 150 年的数学发明，最终在计算机时代找到了它的归宿——这是数学史上最美的故事之一。

12.7 旋转表示的总结与比较

表 12.2:

表示方式	维度	约束	奇异性	直观性	旋转复合
旋转矩阵	3×3=9	$\boldsymbol{R}^T\boldsymbol{R} = \boldsymbol{I}, \det = 1$	无		矩阵乘法
轴角	3	无	$\theta = 0$ 时轴不确定		罗德里格斯公式
欧拉角	3	无	万向锁		三次旋转复合

选择建议：- 需要做优化/求解问题时 → 用**四元数**或**轴角**（参数少，约束简单）- 需要和人类交互/显示时 → 用**欧拉角**（最直观）- 需要做大量旋转复合时 → 用**旋转矩阵**或**四元数** - 在机器人/无人机/自动驾驶领域 → 实际系统中通常内部用四元数计算，显示给用户时转为欧拉角

笔者写到这里，深感线性代数、群论、微积分在三维空间中完美交汇。$SO(3)$ 是群，旋转矩阵是它的矩阵表示，四元数是它的覆盖群，轴角 $\theta\boldsymbol{n}$ 对应李代数 $\mathfrak{so}(3)$ 中的元素，而罗德里格斯公式本质上就是李代数到李群的**指数映射**——$\boldsymbol{R} = \exp(\theta\boldsymbol{n}^\wedge)$。这正是前面 9.1 节中矩阵指数 $e^{\boldsymbol{A}}$ 的深刻应用。数学的美，在于它总是在你最意想不到的地方自我呼应。