离散数学与结构 (图灵班)

作者：李新年, 严绍恒 (PhotonYan), 蒋承佑，汪煦康，陈易涵，刘鹏飞，牛煦，刘小康，韩若水，朱汶宣，李思成
组织：北京大学信息科学与技术学院
时间：2025-2026 秋季学期

目录

第一章 朴素集合论 (Naive Set Theory)

内容提要

- ❑ 相信大家早就知道
- ❑ 不会有人不知道吧
- ❑ 这是我们已经熟知的
- ❑ 这是小学生的做法
- ❑ 我们有更简单的办法

1.1 基本概念

相信大家早已熟知:

$$\exists \text{injection} f: S \rightarrowtail T \quad \Rightarrow \quad S \preccurlyeq T \tag{1.1}$$

$$\exists \text{bijection} f: S \to T \quad \Rightarrow \quad S \sim T \tag{1.2}$$

$$2^S \succ S \tag{1.3}$$

(1.3)可由罗素悖论证明:

证明 定义单射 $i: S \to 2^S$ 为 $i(x) = \{x\}$，故 $|2^S| \geq |S|$。设反证存在满射 $f: S \to 2^S$。定义

$$R = \{ x \in S \mid x \notin f(x) \} \in 2^S. \tag{1.4}$$

由满射性，存在 $a \in S$ 使得 $f(a) = R$。于是

$$a \in R \iff a \notin f(a) = R, \tag{1.5}$$

矛盾。故不存在满射 $S \to 2^S$，即 $|2^S| \not\leq |S|$。

综上，$|2^S| > |S|$。

在实分析与测度论里有类似的证明:

证明 显然存在单射 $i: S \to 2^S$，定义为 $i(s) = \{s\}$，所以 $|2^S| \geq |S|$。接下来证明不存在满射 $f: S \to 2^S$。将 2^S 与 $\{0,1\}^S$ 对应，每个子集 $A \subseteq S$ 对应其特征函数 $\chi_A: S \to \{0,1\}$。假设 $f: S \to \{0,1\}^S$ 为任意函数，定义新函数

$$g: S \to \{0,1\}, \qquad g(s) = 1 - f(s). \tag{1.6}$$

则 $g \in \{0,1\}^S$。若存在 $a \in S$ 使得 $f(a) = g$，则

$$g(a) = f(a), \tag{1.7}$$

但由构造 $g(a) = 1 - f(a)$，矛盾。因此 $g \notin f(S)$，说明 f 不是满射。综上，不存在 $S \to 2^S$ 的满射，而存在单射 $S \hookrightarrow 2^S$，故

$$|2^S| > |S|. \tag{1.8}$$

本质上即集合范畴上否定函数没有不动点:

证明 取 $X = \{0,1\}$，定义自映射

$$F: \{0,1\} \longrightarrow \{0,1\}, \qquad F(0) = 1,\ F(1) = 0, \tag{1.9}$$

即前面两种方法内取反的操作。该映射显然没有不动点。根据 Lawvere 不动点原理，若存在满射 $e: S \to X^S$，则 F 应该有不动点，矛盾。因此，不存在满射 $S \to X^S$。再结合显然的单射 $S \hookrightarrow X^S$，可得

$$|X^S| > |S|. \tag{1.10}$$

取 $X = \{0,1\}$ 即得

$$|2^S| > |S|. \tag{1.11}$$

命题 1.1 (Schröder–Bernstein Theorem)

$$\forall S,T,\quad S\succcurlyeq T\wedge T\succcurlyeq S\quad\Rightarrow\quad S\sim T \tag{1.12}$$

♠

证明 这里给出简要思路。设 $f:S\to T$ 与 $g:T\to S$ 均为单射。下证 f 的陪集为 T 的全集。定义双射 Π:

1. $\Pi(g(y))=y$ 当 $y\in T-f(S)$;
2. $\Pi(x)=f(x)$ 当 $x\in S-g(T)$.

接着便可通过归纳递归证明。

证明 考虑两可数集。对于可数集，均可被离散点列表示。在两组离散点列的单射下，存在四种结构:

1. 有起点:
   (a). 左起点——选择左集合到右集合的边;
   (b). 右起点——选择右集合到左集合的边;
2. 无起点: 环路或无穷延伸. 任意选择一组边。

形式化语言。存在双射 Π:

$$\Pi=\begin{cases}g^{-1}(x) & \text{if } (g^{-1}\circ f)^n(x)\notin f(S)\\ f(x) & \text{if } (f^{-1}\circ g)^n(x)\notin g(T)\\ f(x) & \text{o.w.}\end{cases} \tag{1.13}$$

满足要求。

注 事实上，虽然上述过程（包括课堂板书）中我们是针对可数集进行的分析，但最终得到的双射函数 Π 对连续统一样有效，从而可以推广至任意无穷集上。

相信大家早已熟知:

$$\mathbb{R}^{\mathbb{N}}\sim\mathbb{R}\sim 2^{\mathbb{N}},\quad \mathbb{N}\sim\mathbb{Q}. \tag{1.14}$$

引理 1.1

等势具有传递性，只需引入向共同等价的中间集的映射 τ^{-1} 和 π，然后构造 $\pi\circ f\circ\tau^{-1}$ 即可。

♡

引理 1.2

$$(S^T)^W\quad\sim\quad S^{T\times W} \tag{1.15}$$

♡

证明 可以通过以下伪代码理解。

Algorithm 1 上述引理的直觉化解释

```
function f'(w)
    return lambda t. f(t, w)
end function
```

下面简要说明等势的证明思路:

证明 证明是简单的，这里给出一个比较明智的思路:

$$\mathbb{R}^{\mathbb{N}}\sim(2^{\mathbb{N}})^{\mathbb{N}}\sim 2^{\mathbb{N}\times\mathbb{N}} \tag{1.16}$$

笔记 为避免无穷小数的表示不完备，在此规定 n 进制下循环节不为 $n-1$. 即我们尽量取闭式。(这与老师的选择是不一样的，但我认为这更有道理)

自然数的定义可见《代数学方法》。其中后继运算可写作:

$$n+1:=n\cup\{n\} \tag{1.17}$$

其中，递归出口为自然数 $0:=\varnothing$.

命题 1.2

$$\bigcup_{i=0}^{\infty} S_i \sim \mathbb{R} \quad \Rightarrow \exists i, \quad S_i \sim \mathbb{R} \tag{1.18}$$

♠

定义 1.1 (Dedekind 有限集)

称一个集合 S 是 Dedekind 有限的，如果 S 不与它的任何真子集存在双射。等价地，S 是 Dedekind 有限的，当且仅当对于任意单射 $f : S \to S$，它必然是满射。或 S 是 Dedekind 有限集，当且仅当：

$$\forall T \subsetneqq S, \quad T \prec S \tag{1.19}$$

♣

定义 1.2 (序关系)

设 P 是一个集合，$\preccurlyeq$ 是 P 上的一个二元关系。

1. 如果 $\preccurlyeq$ 满足以下条件：
   - (自反性) $\forall x \in P,\ x \preccurlyeq x$；
   - (反对称性) $\forall x, y \in P,\ (x \preccurlyeq y \wedge y \preccurlyeq x) \Rightarrow x = y$；
   - (传递性) $\forall x, y, z \in P,\ (x \preccurlyeq y \wedge y \preccurlyeq z) \Rightarrow x \preccurlyeq z$；

   则称 $(P, \preccurlyeq)$ 为一个偏序 (partial-ordered) 集。
2. 如果偏序关系 $\preccurlyeq$ 还满足

   $$\forall x, y \in P, \quad x \preccurlyeq y \ \text{ or } \ y \preccurlyeq x, \tag{1.20}$$

   则称 $(P, \preccurlyeq)$ 为一个全序 (total-ordered) 集。

♣

定义 1.3 (良序)

设 P 是一个集合，$\preccurlyeq$ 是 P 上的一个二元关系。若满足：

1. $(P, \preccurlyeq)$ 是一个全序集；
2. 对任意非空子集 $A \subseteq P$，都存在最小元，即存在 $a \in A$ 使得

   $$\forall x \in A, \quad a \preccurlyeq x, \tag{1.21}$$

则称 $(P, \preccurlyeq)$ 是一个良序 (well-ordered) 集。

♣

定义 1.4 (选择函数)

设 $\mathcal{F}$ 是一族非空集合。若存在函数

$$f : \mathcal{F} \longrightarrow \bigcup \mathcal{F} \tag{1.22}$$

使得对每个 $A \in \mathcal{F}$ 都有 $f(A) \in A$，则称 f 为一个选择函数。

♣

公理 1.1 (选择公理 (Axiom of Choise))

对任意非空集合族 $\mathcal{F}$，必存在选择函数。

♡

选择公理和良序公理等价：

公理 1.2 (良序公理)

每一个集合都可以配备某种良序关系（即，每个非空子集都有最小元）。

♡

当我们承认选择公理：

1. S 是 Dedekind 有限的 $\Leftrightarrow S$ 是有限的；
2. $S \succcurlyeq T \vee T \succcurlyeq S$；

3. 对于无限集，$S \sim S \times S$;

定义 1.5 (连续统假设, Continuum Hypothesis)

设 $\aleph_0$ 为可数基数 $\|\mathbb{N}\|$，$2^{\aleph_0}$ 表示实数集 $\mathbb{R}$ 的基数（即连续统）。连续统假设即：

$$\nexists \kappa \quad \text{s.t.} \quad \aleph_0 < \kappa < 2^{\aleph_0}. \tag{1.23}$$

即：

$$2^{\aleph_0} = \aleph_1. \tag{1.24}$$

在 ZFC+CH 下，有命题成立：

命题 1.3

$$S \succ T \Rightarrow 2^S \succ 2^T \tag{1.25}$$

$$2^S \succcurlyeq 2^T \Rightarrow S \succcurlyeq T \tag{1.26}$$

反之，可构造反例使得上述命题不成立。

第二章 命题逻辑 (Proposition Logic)

内容提要

- ❑ 我们看起来讲了很多，但其实什么都没讲
- ❑ 这个事情很是不容易
- ❑ 这也是小学时大家就会的
- ❑ 你需要干的只是一些很繁琐琐碎的事情

定义 2.1 (谓词)

在逻辑学中，谓词（Predicate）是一个函数或关系符号，用来表示对象之间的某种性质或关系。形式上，它是一个从对象域（domain of discourse）到布尔值 {True, False} 的映射。

$$P : D^n \to \{\text{True}, \text{False}\}, \quad (x_1, x_2, \ldots, x_n) \mapsto P(x_1, x_2, \ldots, x_n) \tag{2.1}$$

例如：

- 一元谓词：$P(x)$ 表示 “x 是素数”。
- 二元谓词：$R(x, y)$ 表示 “$x < y$”。

♣

定义 2.2 (字母表-Alphabet)

- 谓词（Predicate）：$P, Q, P_1, P_2, P_3 \cdots$
- 连接词（Connectiuities）：Implies $\to$, or $\vee$, and $\wedge$, iff $\leftrightarrow$, not $\neg$, fobs $\bot$.
- 辅助词（Auxiliary）：(,).

♣

定义所有字符串组成的集合为 Σ^*。而合法句子构成的集合 PROP 包括以下几类命题：

1. 任意原子命题（Atomic proposition）:$P_i, \bot$
2. PROP 对二元连接运算封闭；
3. PROP 对否定封闭.

我们取最小的满足上述条件的集合为 PROP，就像我们在研究 σ-代数的时候一样。

笔记 事实上，我们会发现这与代数（Algebra）的定义是相当吻合的。或许这就是为什么命题逻辑也被称作布尔代数。

定义 2.3 (代数)

设 W 是一个集合，$\mathcal{A}$ 是 W 的子集的集合。若满足以下条件，则称 $\mathcal{A}$ 是 W 上的一个代数 **(algebra)**：

1. $\varnothing \in \mathcal{A}$；
2. 若 $E \in \mathcal{A}$，则 $W \setminus E \in \mathcal{A}$；
3. 若 $E, F \in \mathcal{A}$，则 $E \cup F \in \mathcal{A}$。

♣

由于合法集合 PROP 是**最小的**，因此对于任意满足以下条件的命题 $A \in \Sigma^*$，$\forall \varphi \in \text{PROP}$，$A(\varphi)$ 均成立：

1. 任意原子命题（Atomic proposition）为真:$A(P_i)$, $A(\bot)$
2. 对二元连接运算封闭：$A(\varphi) \wedge A(\psi) \to A(\varphi \square \psi)$，其中 $\square$ 是任意二元连接符；
3. 对否定封闭：$A(\varphi) \to A(\neg\varphi)$.

如何形式化定义命题的函数 F：PROP $\to \Omega$ 呢？我们只需要给定：

1. $H_{\text{atomic}} : \{P_1, P_2, \cdots, \bot\} \to \Omega$;
2. $H_{\square} : \Omega \times \Omega \to \Omega$;
3. $H_{\neg} : \Omega \to \Omega$.

而：

1. $F(P_i) = H_{\text{atomic}}(P_i)$;
2. $F((\varphi \square \psi)) = H_{\square}(F(\varphi), F(\psi))$;
3. $F(\neg\varphi) = H_{\neg}(F(\varphi))$.

例题 2.1Valuation 定义赋值 Valuation v : PROP $\to \{0,1\}$.

$$\begin{aligned} v(\neg\bot) &= 0, \\ v(\neg\varphi) &= 1 - v(\varphi), \\ v(\varphi \wedge \psi) &= \min\{\, v(\varphi),\, v(\psi)\,\}, \\ v(\varphi \vee \psi) &= \max\{\, v(\varphi),\, v(\psi)\,\}, \\ v(\varphi \to \psi) &= 1 - v(\varphi)\cdot(1 - v(\psi)). \end{aligned}$$

φ 在 v 下的赋值被记作 $[\![\varphi]\!]_v$.

定义 2.4 (生成序列-Generation Sequence)

从原子命题出发，通过不断作用谓词生成的，后续项可由前项与谓词耦合而成的序列。 ♣

生成序列并不唯一，甚至并不最小。

定义 2.5 (重言式 (恒真式、套套逻辑)-Tautology)

φ 是恒真式，记作 $\models \varphi$，当且仅当 $[\![\varphi]\!]_v\ \forall v$. ♣

设 Γ 是命题集合，若对于任意给定赋值，$\forall\varphi \in \Gamma$ 都有 $[\![\varphi]\!]_v \to [\![\psi]\!]_v$，则记作 $\Gamma \models \psi$.

定理 2.1

$$\models \varphi \quad \Rightarrow \quad \models \varphi[\Psi/P] \tag{2.2}$$

即，将恒真式中的某原子命题 P 换作任意 PROP 中元素，恒真性不变。 ♡

定义 2.6

$$\varphi \approx \psi \quad \Leftrightarrow \quad \varphi \models \psi \wedge \psi \models \varphi \tag{2.3}$$

♣

命题逻辑有的时候具有规律:

1. 交换律: $(P \wedge Q) \approx (Q \wedge P)$;
2. 结合律: $((P \wedge Q) \wedge R) \approx (P \wedge (Q \wedge R))$
3. 分配律: $((\varphi \wedge \psi) \vee \delta) \approx ((\varphi \vee \delta) \wedge (\psi \vee \delta))$
4. $\neg\neg\varphi \approx \varphi$.

2.1 自然归纳法

以上为模型论，下面开始讨论语法。

定义 2.7 (自然归纳法-Natural Deduction)

Inply 的引入规则:

$$\frac{\begin{array}{c}[\![\varphi]\!]^1 \\ \vdots \\ \psi\end{array}}{\varphi \to \psi} \to I,\ 1$$

Inply 的消去规则：

$$\varphi \quad \varphi \to \psi \vdash \psi \tag{2.4}$$

And 的引入规则：

$$\varphi \quad \psi \vdash \varphi \wedge \psi \tag{2.5}$$

And 的消去规则：

$$\varphi \wedge \psi \vdash \varphi \quad \psi \tag{2.6}$$

RAA：

$$\begin{array}{c} [\neg\varphi]^1 \\ \vdots \\ \dfrac{\bot}{\varphi}\ \text{RAA, 1} \end{array}$$

爆炸规则：

$$\bot \vdash \varphi \tag{2.7}$$

$\varphi \leftrightarrow \psi$ 即 $(\varphi \to \psi) \wedge (\psi \to \varphi)$；
$\varphi \vee \psi$ 即 $\neg((\neg\varphi) \wedge (\neg\psi))$；
$\neg\varphi$ 即 $\varphi \to \bot$.

♣

例题 2.2 证明 $(\neg Q \to \neg P) \leftrightarrow (P \to Q)$.

证明 正向：

$$\dfrac{\dfrac{\dfrac{[\neg Q \to \neg P]^1 \qquad [\neg Q]^3}{\neg P} \to E \qquad [\![P]\!]^2}{\dfrac{\bot}{Q}\ \text{RAA, 3}} \to E}{\dfrac{\dfrac{Q}{P \to Q} \to I, 2}{(\neg Q \to \neg P) \to (P \to Q)} \to I, 1}$$

反向：

$$\dfrac{\dfrac{\dfrac{[P \to Q]^1 \qquad [\![P]\!]^3}{Q} \to E \qquad [\neg Q]^2}{\dfrac{\bot}{\neg P}\ \neg I, 3} \to E}{\dfrac{\dfrac{\neg P}{\neg Q \to \neg P} \to I, 2}{(P \to Q) \to (\neg Q \to \neg P)} \to I, 1}$$

关于列表式的自然证明。

1. $\neg\neg P \vdash P$
2. $\vdots$ $\neg P$
3. $\vdots$ $\bot$ $\to E(2)(1)$
4. P $\to RAA(2)$

其中，缩进的部分被称作「幻想」的。我们再给出另一个例子：

1. $\vdash p \to \neg\neg P$
2. $[\![P]\!]$
3. $\vdots$ $[\neg P]$
4. $\vdots$ $\bot$ $\to E(1)(2)$

5. ⋮ $\neg\neg P$ $I(2)(3)$
6. $P \to \neg\neg P$ $\to I(1)(4)$

在这个过程中，我们可以利用列表法记录下每一步推理所用到的假设和规则：

Ass. Set	No.	Prop.	Rule
①	①	$[\neg p]$	
②	②	$[\![P]\!]$	
②	③	$\bot$	$\to E$
②	④	$\neg\neg p$	$\to I_{31}$
	⑤	$p \to \neg\neg p$	$\to I_{42}$

注 $\Vdash$ 是语义蕴含（Semantic entailment），$\vdash$ 是语法推导（Syntactic entailment）。

我们希望蕴含与推导之间有以下几条性质：

1. Soundness 一致性：if $\Gamma \vdash \varphi$, then $\Gamma \Vdash \varphi$.
2. Completeness 完备性：if $\Gamma \Vdash \varphi$, then $\Gamma \vdash \varphi$.

定义 2.8 (满足关系与语义蕴涵)

设命题语言的模型为布尔赋值 $v : \mathrm{Prop} \to \{0,1\}$。对于公式 θ，记

$$v \models \theta \quad \overset{\text{def}}{\Longleftrightarrow} \quad [\![\theta]\!]_v = 1 \tag{2.8}$$

这里 $[\![\theta]\!]_v$ 表示公式 θ 在赋值 v 下的真值。

对于公式集合 Γ 与公式 φ，我们定义语义蕴涵为

$$\Gamma \Vdash \varphi \quad \overset{\text{def}}{\Longleftrightarrow} \quad \forall v \, (v \models \Gamma \;\Rightarrow\; v \models \varphi) \tag{2.9}$$

其中

$$v \models \Gamma \quad \overset{\text{def}}{\Longleftrightarrow} \quad \forall \theta \in \Gamma,\ v \models \theta \tag{2.10}$$

换言之，$\Gamma \Vdash \varphi$ 表示：对任意赋值 v，如果 v 使得 Γ 中的所有公式都为真，那么 φ 也为真。

笔记 排中律可用于分解命题为多个子命题。

$$\frac{\vdash \psi \vee \neg\psi \qquad \Gamma, \psi \vdash \varphi \qquad \Gamma, \neg\psi \vdash \varphi}{\Gamma \vdash \varphi} \vee E$$

注 老师在课上用的更基本的规则，在此处我们暂时简省。

接下来我们来证明二者之间的完备性。我们的证明目标是：取任意赋值 v，若 $\Gamma \vDash \varphi$，则 $\Gamma \vdash \varphi$。记 $[\![\theta]\!]_v := v(\theta)$ 表示赋值 v 下公式 θ 的真值。

为此，先固定本节涉及的原子集合（即课堂板书中老师提到的，将命题拆分成若干子条件 P_i 下的分命题，然后分别证明中 P_i 组成的集合）：

$$\mathrm{At} := \mathrm{At}(\Gamma \cup \{\varphi\}) \tag{2.11}$$

并把赋值理解为函数 $v : \mathrm{At} \to \{0,1\}$。

定义 2.9 (赋值诱导的文字集)

给定赋值 $v : \mathrm{At} \to \{0,1\}$，定义其对应的文字集：

$$\mathcal{V}(v) \;:=\; \{\, P \in \mathrm{At} \mid v(P) = 1 \,\} \cup \{\, \neg P \mid P \in \mathrm{At},\ v(P) = 0 \,\} \tag{2.12}$$

直观地，$\mathcal{V}(v)$ 把 v 的信息语法化为一组前提。我们希望建立如下引理：

引理 2.1

对任意由 At 上原子经连接词构成的公式 φ，有：

$$[\![\varphi]\!]_v = 1 \Rightarrow \mathcal{V}(v) \vdash \varphi, \qquad [\![\varphi]\!]_v = 0 \Rightarrow \mathcal{V}(v) \vdash \neg\varphi. \tag{2.13}$$

对公式 φ 按结构归纳，归纳假设为：对一切严格简单于 φ 的公式 θ，若 $[\![\theta]\!]_v = 1$ 则 $\mathcal{V}(v) \vdash \theta$，若 $[\![\theta]\!]_v = 0$ 则 $\mathcal{V}(v) \vdash \neg\theta$。

笔记 这里的严格简单可以看做定义在 prop 上的序关系。

分三类讨论：

1. **原子情形**：$\varphi \equiv P$。

   若 $[\![P]\!]_v = 1$，则 $P \in \mathcal{V}(v)$，故 $\mathcal{V}(v) \vdash P$；若 $[\![P]\!]_v = 0$，则 $\neg P \in \mathcal{V}(v)$，即 $\mathcal{V}(v) \vdash \neg P$。

   $$\frac{P}{P}\,\text{Ax} \qquad\qquad \frac{\neg P}{\neg P}\,\text{Ax}$$

2. **底元情形**：$\varphi \equiv \bot$。

   由语义 $[\![\bot]\!]_v = 0$。需证 $\mathcal{V}(v) \vdash \neg\bot$。假设 $\bot$，由重述得 $\bot$，出子证明得 $\bot \to \bot$，即 $\neg\bot$。

3. **蕴含情形**：$\varphi \equiv \psi_1 \to \psi_2$。分 $[\psi_1 \to \psi_2]_v$ 的两种值：

   (a). 若 $[\![\psi_1 \to \psi_2]\!]_v = 1$，则（按命题语义）$[\![\psi_1]\!]_v = 0$ 或 $[\![\psi_2]\!]_v = 1$。

   - 若 $[\![\psi_1]\!]_v = 0$，归纳假设给出 $\mathcal{V}(v) \vdash \neg\psi_1$。假设 ψ_1，与 $\neg\psi_1$ 得矛盾 $\bot$，由 $\bot E$ 得 ψ_2，得 $\psi_1 \to \psi_2$。
   - 若 $[\![\psi_2]\!]_v = 1$，归纳假设给出 $\mathcal{V}(v) \vdash \psi_2$。假设 ψ_1，仍得 ψ_2，得 $\psi_1 \to \psi_2$。

   $$\dfrac{\dfrac{\neg\psi_1 \qquad [\psi_1]^1}{\dfrac{\bot}{\psi_2}\,\bot}\,\neg E}{\psi_1 \to \psi_2}\,{\to} I^1 \qquad\qquad \frac{\psi_2 \qquad [\psi_1]^1}{\psi_1 \to \psi_2}\,{\to} I^1$$

   (b). 若 $[\![\psi_1 \to \psi_2]\!]_v = 0$，则必须且仅当 $[\![\psi_1]\!]_v = 1$ 且 $[\![\psi_2]\!]_v = 0$。归纳假设分别给出 $\mathcal{V}(v) \vdash \psi_1$ 与 $\mathcal{V}(v) \vdash \neg\psi_2$。假设 $\psi_1 \to \psi_2$，由 ψ_1 与 $\to E$ 得 ψ_2，与 $\neg\psi_2$ 得 $\bot$，得 $(\psi_1 \to \psi_2) \to \bot$，即 $\neg(\psi_1 \to \psi_2)$。

   $$\dfrac{\dfrac{\neg\psi_2 \qquad \dfrac{\psi_1 \qquad [\psi_1 \to \psi_2]^1}{\psi_2}\,{\to} E}{\bot}\,{\to} E}{\neg(\psi_1 \to \psi_2)}\,\neg I^1$$

至此完备性就被证明了，我们无须引入额外的规则就能利用 ND 推导所有真命题（当然我们也可以引入 $\vee$ 和 $\neg$ 的引入与推导）。这也为我们后续混淆 $\vdash$ 和 $\Vdash$ 提供了理论基础。

我们关心在删减某些规则后，是否仍能保持（相对于合适语义的）完备性。先回顾当前使用的若干自然演绎规则：$\to I$, $\to E$, $\wedge I$, $\wedge E$, $\bot I$, RAA。

事实上，直觉主义逻辑拒绝经典的 RAA，因此经典结论如 $\neg\neg\varphi \to \varphi$ 不再可证，排中律不再成立；但是该体系相对于 Kripke 语义仍然完备。

Minimal Logic 在此基础上进一步去掉了 $\bot$ 的消去规则（即 $\bot \vdash \psi$），从而失去了爆炸律。但 Minimal Logic 对于不爆炸的 Kripke 语义依然完备。

定义 2.10 (直觉主义)

排中律，爬。

在直觉主义里：

$$P \to \neg\neg P, \qquad \neg\neg P \to P \quad ? \tag{2.14}$$

左侧命题是真（因为不需要 RAA），但右侧命题无法被证明。说明这个事情很是不容易。

我们考虑一个新的语义，Kripke model。在这个语义内，$(W, \leq)$ 是一个带有偏序关系的**世界**集。我们认为每个世界都是一组赋值，即存在映射 $v : W \times \text{Prop} \to \{0, 1\}$。

定义 2.11 (Kripke Model)

一个 Kripke 模型是二元组 $(W, \leq)$，其中

- W 是一组世界，配备偏序关系 $\leq$；
- $v : W \times \mathrm{Prop} \to \{0, 1\}$ 是命题变元的赋值函数，满足：

$$\text{若} w \leq w' \text{ 且} v(w, p) = 1, \text{ 则} v(w', p) = 1. \tag{2.15}$$

  即真值在偏序下具有单调性。
- 特别地，$\bot$ 在所有世界中恒为假：对任意 $w \in W$，有 $v(w, \bot) = 0$。

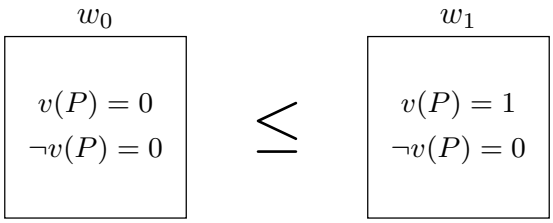


图 2.1: 在 Kripke Model 下，RAA 不再必须。

在 Kripke 语义下，命题公式的解释是相对于世界 $w \in W$ 来定义的。蕴含的语义规定为：

$$v(w, \psi \to \varphi) = \begin{cases} 1, & \forall w' \geq w,\ v(w', \psi) = 1 \Rightarrow v(w', \varphi) = 1, \\ 0, & \text{o.w.} \end{cases} \tag{2.16}$$

这一定义确保了蕴含的真值在偏序结构下具有单调性，并且与直觉主义逻辑的语义一致。

定理 2.2 (完备性)

Kripke 语义与直觉主义逻辑是完备一致的，即

$$\Gamma \vdash_i \varphi \quad \Longleftrightarrow \quad \Gamma \Vdash_{\text{Kripke}} \varphi. \tag{2.17}$$

我们还可以定义公式在所有 Kripke 模型中为真的记号为：

$$\models \varphi \ := \ \forall (W, \leq, v)\, \forall w \in W :\ v(w, \varphi) = 1 \tag{2.18}$$

直觉主义和类型论是有重要联系的。

定义 2.12 (Type)

在类型论中，类型 (Type) 是对项 (term) 的一种分类。记号

$$a : A \tag{2.19}$$

表示项 a 的类型是 A。这里 a 称为 A 的一个构造。

注 直觉主义逻辑与类型论之间存在 Curry–Howard 对应：

$$\text{命题} \longleftrightarrow \text{类型}, \qquad \text{证明} \longleftrightarrow \text{构造} \tag{2.20}$$

- $\varphi \wedge \psi$ 对应于积类型 $A \times B$；
- $\varphi \vee \psi$ 对应于和类型 $A + B$；
- $\varphi \to \psi$ 对应于函数类型 $A \to B$；
- $\bot$ 对应于空类型 0。

在这种意义下，**类型就是命题，程序就是证明**。

以下是一些具体的对应。

Formula	Type-Theoretic Perspective
$P \to \neg P$	$P \to (P \to \bot)$；若 $p : P$ 且 $\varphi : (P \to \bot)$，则 $\varphi(p) : \bot$。
$\neg\neg P \to P$	$((P \to \bot) \to \bot) \to P$；直觉主义下不可证
$\bot \to \varphi$	*ex falso quodlibet*；从空类型 $\bot$ 出发，可以构造到任意类型 φ 的函数。

命题 2.1 (合取)

$$\frac{P \quad Q}{P \wedge Q} \qquad \frac{P \wedge Q}{P} \qquad \frac{P \wedge Q}{Q}$$

Type-Theoretic Perspective: $P \wedge Q$ 对应积类型 $P \times Q$，由 $\mathrm{pair}\langle p, q\rangle$ 构造。

命题 2.2 (析取)

$$\frac{P}{P \vee Q} \qquad \frac{Q}{P \vee Q}$$

Type-Theoretic Perspective: $P \vee Q$ 对应和类型 $P + Q$，由 $\mathrm{inl}(p)$ 或 $\mathrm{inr}(q)$ 构造。

至此，我们已经把逻辑符号解释为类型构造。定义直觉主义推导为 $\vdash_i$，失败类型为 $\bot$，而 $P \to Q$ 被解释为映射类型。在这种框架下，直觉主义逻辑等价于探讨：你允许哪些类型存在，并且是否能够在这些类型中构造出一个实例。例如 $P,\ P \to Q \ \vdash_i\ Q$，我们有构造 $f : P \to Q$ 且 $f(p) = q$。

再举一个例子：公式 $P \to \big((P \to \bot) \to \bot\big)$ 可以理解为一个函数：其中，当输入 $\varphi : P \to \bot$ 时，输出 $\bot$。

Algorithm 2 直觉化解释：$P \to ((P \to \bot) \to \bot)$

```
function f(p : P)
    return λφ. φ(p)
end function
```

再看 $(P \to Q) \to (\neg Q \to \neg P)$，其中 $\neg X := X \to \bot$。它可以解释为：其中，$g : Q \to \bot$，应用 $\varphi(p) : Q$ 得到

Algorithm 3 直觉化解释：$(P \to Q) \to (\neg Q \to \neg P)$

```
function f(φ : P → Q)
    return λg. λp. g(φ(p))
end function
```

矛盾 $g(\varphi(p)) : \bot$，从而得到 $\neg P$。

另一个例子。蕴含：$f : (P \to S) \wedge (Q \to S) \ \to\ (P \vee Q \to S)$

Algorithm 4 构造函数 f

```
function f(u : (P → S) ∧ (Q → S))
    设 u = ⟨v, w⟩，其中 v : P → S, w : Q → S
    return λx. case x of
        inl(p) ↦ v(p)
        inr(q) ↦ w(q)
end function
```

因此，直觉主义可以被解释为：能够在模型下显式构造一个实例 ⇔ 证明了某个命题。

2.2 System K

我们在命题逻辑的基础上引入模态算子，从而得到系统 K 的语言。

定义 2.13 (语法)

- 原子命题 **(atomic proposition)**：设 Prop 是一组命题符号的集合，记作 $p, q, r, \cdots \in \mathrm{Prop}$。它们是最基本的公式，不可再分解。
- 复合公式 **(formula)**：所有公式的集合 $\mathcal{F}$ 按如下归纳方式定义：
  1. 每个原子命题 $p \in \mathrm{Prop}$ 是一个公式。
  2. $\bot$ 是公式，表示假。
  3. 对否定封闭：若 φ 是公式，则 $\neg\varphi$ 也是公式。
  4. 对二元运算符封闭：若 φ, ψ 是公式，则以下都是公式：
  $$(\varphi \wedge \psi) \quad (\varphi \vee \psi) \quad (\varphi \to \psi). \tag{2.21}$$
  它们分别表示合取、析取与蕴涵。
  5. 对必然/可能封闭：若 φ 是公式，则 $\Box\varphi$ 与 $\Diamond\varphi$ 也是公式，分别表示必然 φ 与可能 φ。
- 序列 **(sequent)**：一个序列是形如
$$\Gamma \Rightarrow \Delta \tag{2.22}$$
的表达式，其中 Γ, Δ 是有限（多）集的公式。直观上，Γ 是假设集合，Δ 是结论集合。其意义为，**若 Γ 中的公式都为真，则 Δ 中至少有一个为真**。

♣

公理 2.1 (初始公理)

$$\varphi \Rightarrow \varphi \tag{2.23}$$

♡

公式的形式如下：

$$\varphi ::= p \mid \bot \mid \neg\varphi \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi) \mid (\varphi \to \varphi) \mid \Box\varphi \mid \Diamond\varphi \tag{2.24}$$

一个序列写作：

$$\Gamma \Rightarrow \Delta \tag{2.25}$$

其中 Γ, Δ 是有限公式多集。

基本规则包括恒等规则（**Id**entity Rule）、左（**L**eft）/右（**R**ight）弱化规则（**Weak**ening Rules）：

$$\frac{}{\varphi \Rightarrow \varphi}\ \textsc{Id} \qquad \frac{\Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta}\ \textsc{WeakL} \qquad \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \varphi}\ \textsc{WeakR}$$

联结词规则。首先是左右否定规则：

$$\frac{\Gamma \Rightarrow \Delta, \varphi}{\neg\varphi, \Gamma \Rightarrow \Delta}\ \neg\mathrm{L} \qquad \frac{\varphi, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\varphi}\ \neg\mathrm{R}$$

左右合取规则：

$$\frac{\varphi, \psi, \Gamma \Rightarrow \Delta}{\varphi \wedge \psi, \Gamma \Rightarrow \Delta}\ \wedge\mathrm{L} \qquad \frac{\Gamma \Rightarrow \Delta, \varphi \quad \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \wedge \psi}\ \wedge\mathrm{R}$$

左右析取规则：

$$\frac{\varphi, \Gamma \Rightarrow \Delta \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \vee \psi, \Gamma \Rightarrow \Delta}\ \vee\mathrm{L} \qquad \frac{\Gamma \Rightarrow \Delta, \varphi}{\Gamma \Rightarrow \Delta, \varphi \vee \psi}\ \vee\mathrm{R}_1 \qquad \frac{\Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \vee \psi}\ \vee\mathrm{R}_2$$

左右蕴含规则：

$$\frac{\Gamma \Rightarrow \Delta, \varphi \qquad \psi, \Gamma \Rightarrow \Delta}{\varphi \to \psi, \Gamma \Rightarrow \Delta}\ \to\mathrm{L} \qquad \frac{\varphi, \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \to \psi}\ \to\mathrm{R}$$

除此之外还有表示可能性的模态规则，但这在课程中并没有被涉及。

注 系统 K 是最弱的正规模态逻辑。更强的系统可通过在 K 上加入额外公理得到，例如：

- 系统 T：加入 $\Box A \to A$。
- 系统 S4：加入 $\Box A \to \Box\Box A$。
- 系统 S5：加入 $\Diamond A \to \Box\Diamond A$。

第三章 谓词逻辑 (Predicate Logic)

内容提要

- ❑ 呃
- ❑ 我们先来弥补之前的一个失误

上一讲我们证明了自然推导和自然语义之间的一直完备性，但它们的表达能力是有限的。例如：

例题 3.1 Alice slept well.

注 在这个例子里，slept well 被称作谓词（predicate），而它与 Alice 一起构成了一个命题 Prop.

例题 3.2 $z \neq 1$

如果说自然推导是单一命题对 $\{0,1\}$ 的映射，那 Predicate Logic 可以理解为一组命题对 $\{0,1\}$ 的映射。

首先给出字母表（Alphabet）：

- 常量（Constants）
- 变量（Variables）：$x_i,\ i \in \mathbb{N}$
- 函数符号（Function symbols）：$f_i,\ i \in \mathbb{N}$
- 谓词符号（Predicate symbols）：$\bot,\ =;\ P_i,\ i \in \mathbb{N}$
- 连接词（Connectives）：$\wedge,\ \vee,\ \to,\ \neg,\ \leftrightarrow$
- 辅助符号（Auxiliary symbols）：$(,),$“,”
- 量词（Quantifiers）：$\forall,\ \exists$

定义 3.1 (Term)

术语（Term）是满足以下条件的最小集合 T：

- 任何常量或变量都属于 T；
- 若 $t_1,\dots,t_n \in T$，且 f 是 n 元函数符号，则 $f(t_1,\dots,t_n) \in T$。

♣

定义 3.2 (Formula)

公式（Formula）是满足以下条件的最小集合 F：

- 若 $t_1,\dots,t_n \in T$，且 P 是 n 元谓词符号，则 $P(t_1,\dots,t_n) \in F$；此外，若 $t_1,t_2 \in T$，则 $t_1 = t_2 \in F$；
- 若 $\varphi,\psi \in F$，则 $(\neg\varphi),\ (\varphi \wedge \psi),\ (\varphi \vee \psi),\ (\varphi \to \psi),\ (\varphi \leftrightarrow \psi) \in F$；
- 若 $\varphi \in F$ 且 x 是一个变量，则 $(\forall x\,\varphi)$ 与 $(\exists x\,\varphi)$ 也属于 F。

♣

接下来我们玩一下这些新的定义。

定义 3.3 (结构 (Structure))

考虑宇宙 (Universe) Ω 以及包含其的元组 $\mathfrak{A} := (\Omega;\ f : \Omega \to \Omega;\ P : \Omega^n \to \{0,1\};\ \{c_i\} \subset \Omega)$。即结构由一个宇宙、一个宇宙上的函数、谓词和常量组成。

♣

例题 3.3 考虑结构 $(\mathbb{R};\ \underbrace{\times, \cdot^{-1}}_{\text{Function}};\ \underbrace{=, <}_{\text{Predicate}};\ \underbrace{\{0,1\}}_{\text{Constants}})$.

对于该结构，可以写出其类型为：$\langle 2,1;\ 2,2;\ 2\rangle$。

注 记 $[\cdot]$ 为项在结构 $\mathfrak{A}$ 下的赋值。

$$[c]_{\mathfrak{A}} = c, \quad [x]_{\mathfrak{A}} = x^{\mathfrak{A}}, \quad [f(t_1,t_2)]_{\mathfrak{A}} = f\big([t_1]_{\mathfrak{A}},\ [t_2]_{\mathfrak{A}}\big), \quad [P(t_1,t_2)]_{\mathfrak{A}} = P\big([t_1]_{\mathfrak{A}},\ [t_2]_{\mathfrak{A}}\big) \tag{3.1}$$

以及 $\varphi \in \mathrm{FOR}$ 有 $[\![\varphi \to \psi]\!]_{\mathfrak{A}} = \max(1 - [\![\varphi]\!]_{\mathfrak{A}}, [\![\psi]\!]_{\mathfrak{A}})$。

比较有趣的是量词对应的赋值规则：

$$[\![\forall x\ \varphi(x)]\!]_{\mathfrak{A}} = \min_{c\in\Omega}[\![\varphi(x)]\!]_{\mathfrak{A}}\big|_{x=c} = \min_{c\in\Omega}[\![\varphi(\bar{c})]\!]\big|_{\mathfrak{A}} \tag{3.2}$$

考虑字符串 φ ： $\forall x\exists y,\ x = y$ 与替换 $\varphi[x^2/x]$，我们有 $\forall x^2\exists y,\ x^2 = y$。这是很奇怪的。因为假如考虑替换 $\varphi[0/y]\forall x\exists 0,\ x^2 = 0$，这显然是假的：我们希望替换不会使得命题由真变假，即 $\varphi[t/x] = \varphi$。

事实上，量词里的变量可以被看作哑变量，类似于微积分或张量分析里被缩并掉的自由度。哑变量的名称可以随便被改变而不影响命题的真假。与哑变量（老师给的名字叫 Bounded Variable）对立的概念被称作自由变量（Free Variable）。

考虑自由变量集合 $V(t),\ t \in \mathrm{TERM}$ 与由它生成的公式 $\mathrm{FV}(\phi)$。接下来我们显式归纳出 FV：

- 当 $\phi = P(t_1, t_2)$，有 $\mathrm{FV}(\phi) = \mathrm{V}(t_1) \cup \mathrm{V}(t_2)$;
- 对于谓词 $\square$，当 $\phi = \varphi\square\psi$，有 $\mathrm{FV}(\phi) = \mathrm{FV}(\varphi) \cup \mathrm{FV}(\psi)$;
- 对于量词 Q，当 $\phi = Qx\psi$，有 $\mathrm{FV}(\phi) = \mathrm{FV}(\psi) - \{x\}$，即 x 不再自由.

有了自由变量的定义，我们可以更清晰地给出替换操作 $t'[t/x]$ 的递归规则。

定义 3.4 (替换（Substitution）)

设 t 是一项（term），x 是一个变量。定义 $\varphi[t/x]$ 为将公式 φ 中所有自由出现的 x 替换为 t 所得的公式，递归如下：

- 若 φ 是 TERM：

$$x[t/x] = t, \tag{3.3}$$

$$y[t/x] = y \quad (y \neq x), \tag{3.4}$$

$$f(t_1, \ldots, t_n)[t/x] = f(t_1[t/x], \ldots, t_n[t/x]) \tag{3.5}$$

- 若 $\varphi = P(t_1, \ldots, t_n)$ 是原子公式：

$$\varphi[t/x] = P(t_1[t/x], \ldots, t_n[t/x]) \tag{3.6}$$

- 若 $\varphi = \neg\psi$：

$$\varphi[t/x] = \neg(\psi[t/x]) \tag{3.7}$$

- 若 $\varphi = (\psi_1 \square \psi_2)$，其中 $\square \in \{\wedge, \vee, \to, \leftrightarrow\}$：

$$\varphi[t/x] = \psi_1[t/x] \square \psi_2[t/x] \tag{3.8}$$

- 若 $\varphi = (Qy\,\psi)$，其中 $Q \in \{\forall, \exists\}$：

$$y = x \quad \Rightarrow \quad \varphi[t/x] = \varphi, \tag{3.9}$$

$$y \neq x \quad \Rightarrow \quad \varphi[t/x] = Qy(\psi[t/x]) \tag{3.10}$$

♣

但上述定义还是没有严格限制掉所有不合法的替换。例如：

例题 3.4 $\varphi = \exists x \quad x = y + 1$，如果做替换 $\varphi[x/y]$，变成 $\varphi = \exists x \quad x = x + 1$，则又出现了错误。

命题 3.1

我们要求进行 $\phi[t/x]$ 的替换后，不能改变该自由变量的自由性，即：t is free for x in φ.

♠

为了避免循环表达，我们具体定义一下什么是 free for x in φ：

- 如果 $\phi = P$，t 自然是自由的;
- 如果 $\phi = \varphi\square\psi$，$t$ 是自由的当且仅当在替换 φ 和 ψ 使都是自由的;
- 如果 $\phi = Q_x\varphi$，不替换，故还是自由的;
- 如果 $\phi = Q_y\varphi$，如果 $x \notin \mathrm{FV}(\varphi)$或$y \notin \mathrm{FV}(t)$ 且 t 对 x 在 φ 中是可自由替换的（free for x in φ）

谓词也可以被类似地替换。

下面我们回到语义的部分：

- 如果 $\mathrm{FV}(\varphi)=\varnothing$ 且 $[\![\varphi]\!]_{\mathfrak{A}}$，则我们称 $\mathfrak{A}\models\varphi$；
- 如果 $\mathrm{FV}(\varphi)\neq\varnothing$ 且 $\forall(\forall x\in\mathrm{FV}(\varphi)),[\![\varphi]\!]_{\mathfrak{A}}$，则我们称 $\mathfrak{A}\models\varphi$；
- 对于集合 Γ，若 $\forall\varphi\in\Gamma,\mathfrak{A}\models\varphi$，则我们称 $\mathfrak{A}\models\Gamma$，读作 $\mathfrak{A}$ is a model of Γ；
- $\models\varphi$ 指对于所有具有相同 Type 的结构都有 $\mathfrak{A}\models\varphi$. 我们默认所有结构内的 $=$ 是等价的；
- $\models$ 具有传递性，$\mathfrak{A}\models\Gamma,\Gamma\models\varphi,\to\mathfrak{A}\models\varphi$.

注 上述第四点并不总是成立，等号并不被必须引入。

例如我们可以考虑最简单的一个结构 $(\Omega;\_;=;)$，但就算在这样简单的结构里也存在命题：

$$\varphi_n=\exists x_i,\ i\in[n],\quad\bigwedge_{1\le i<j\le n}\neg(x_i=y_i)\tag{3.11}$$

与命题：

$$\psi_n=\forall x_i,\ i\in[n],\quad\bigvee_{1\le i<j\le n}(x_i=y_i)\tag{3.12}$$

这两个命题分别代表结构中存在 n 个不同的元素或任何 n 个元素都会有碰撞（相同）。有：

$$\models\varphi_n\vee\psi_n\tag{3.13}$$

另一个常用的结构是 Peano 算数。我们先对等号限制结构：

公理 3.1

- $\forall x,\ x=x$；
- $\forall x,\forall y,\ x=y\to y=x$；
- $\forall x,\forall y,\forall z,\ (x=y\wedge y=z)\to(x=z)$；
- Term 等价：$\forall x_i,\forall y_i,\forall i\in[k],\ \bigwedge_{i=1}^{k}(x_i=y_i)\to t(x_1,\cdots,x_t)=t(y_i,\cdots,y_t)$；
- Formula 等价：$\forall x_i,\forall y_i,\forall i\in[k],\ \bigwedge_{i=1}^{k}(x_i=y_i)\to(\varphi(x_1,\cdots,x_t)\leftrightarrow\varphi(y_i,\cdots,y_t))$.

♡

这里等价性更类似于：

$$\varphi\leftrightarrow\varphi[y_1/x_1,\cdots,y_k/x_k]\tag{3.14}$$

这种替换是安全的。

从而：

定义 3.5 (Peano Arithmetic)

Peano Arithmetic 是结构 $(\mathbb{N};+,\cdot,S;=;\bar{0},\bar{1})$，其中 S 为后继函数。

♣

Peano 公理模式满足：

1. $\forall x,y\quad(x+y)\cdot z=x\cdot z+y\cdot z$；
2. $\forall x,y\quad z\cdot(x+y)=x\cdot z+y\cdot z$；
3. $\forall x\quad x\cdot 0=0$；
4. $\forall x\quad x\cdot 1=x$.

定义 3.6 (后继)

后继是满足如下关系的函数：

1. $\forall x,\quad\neg(S(x)=0)$；
2. $\forall x,y\quad S(x)=S(y)\to x=y$；
3. $\forall x,y\quad x+S(y)=S(x+y)$；
4. $\forall x,y\quad xS(t)=x\cdot y+x$；

♣

定义 3.7 (归纳法 (Induction))

归纳法是一种 (比较特殊的) 公理模式:

$$\varphi(0) \land (\forall x,\ \varphi(x) \to \varphi(S(x))) \quad \to \quad \forall x,\ \varphi(x) \tag{3.15}$$

定义 3.8 (自然演绎法)

回忆: 全称引入 ($\forall I$) 全称消去 ($\forall E$)

$$\frac{\dfrac{D}{\varphi(z)}}{\forall x \quad \varphi(x)}\,\forall I \qquad \frac{\forall x \quad \varphi(x)}{\varphi(t)}\,\forall E$$

即, 对于 $\Gamma \vdash \varphi(x)$, 如果 x 不属于 Γ 内任意命题的自由变量, 那么 $\Gamma \vdash \forall x,\ \varphi(x)$.

接下来我们找一些与 Peano 公理等价的命题。他们可以悲用作证明 Peano 算数中的命题的工具。他们被称作推导规则:

$$\frac{}{x = x}\,\mathbb{I}_1$$

$$\frac{x = y}{y = x}\,\mathbb{I}_2$$

$$\frac{x = y \qquad y = z}{x = z}\,\mathbb{I}_3$$

$$\frac{x_1 = y_1 \qquad x_2 = y_2 \qquad \cdots}{t(x_1, x_2, \cdots) = t(y_1, y_2, \cdots) \quad P(x_1, x_2, \cdots) = P(y_1, y_2, \cdots)}\,\mathbb{I}_4$$

定理 3.1

$$\exists \quad = \quad \neg\forall\neg \tag{3.16}$$

证明

$$\frac{\dfrac{[\forall x\, \neg\varphi(x)]^1}{\neg\varphi(x)}\,\forall E \qquad \dfrac{\forall x\, \varphi(x)}{\varphi(x)}\,\forall E}{\dfrac{\bot}{\neg\forall x\, \neg\varphi(x)}\,\to E^1}$$

下面我们试着用这些 Peano 公理证明一些东西:

练习 3.1 试证明 $\mathrm{PA} \vdash \forall x,\ 0 + x = x$.

证明 简记 $\varphi(x) := (0 + x = x)$, 记 $= T$ 为等号传递性,

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x\,(x + 0 = x)}\,\forall E}{0 + 0 = 0}}{\varphi(0)} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\,\varphi(x)\,]^1 \qquad \dfrac{\forall u\,\forall v\,(u = v \to S(u) = S(v))}{(0 + x) = x \to S(0 + x) = S(x)}\,\forall E}{S(0 + x) = S(x)}\,\to E \qquad \dfrac{\forall u\,\forall v\,(u + S(v) = S(u + v))}{0 + S(x) = S(0 + x)}\,\forall E}{0 + S(x) = S(x)}\,= T}{\varphi(Sx)}}{\varphi(x) \to \varphi(Sx)}\,\to I^1}{\forall x\,(\varphi(x) \to \varphi(Sx))}\,\forall I}{\forall x \quad \varphi(x)}\,\mathrm{Ind}$$

一般来说, 我们证明的命题是在一个扩充的字符集上而非最基本的 Peano 的结构上。即我们将常量集由 $\{0, 1\}$ 扩充到 $\mathbb{N}$ 上。

定义 3.9 (定理 (Theorem))

$$\underbrace{T}_{\text{Theorem}} := \{\text{sentence } \varphi,\ s.t.\ \underbrace{\Gamma}_{\text{Axiom Set}} \vdash \varphi\} \tag{3.17}$$

♣

定理集是公理集合在推导操作下的闭包。

定理 3.2

如果 $\Gamma \nvdash \bot$，那么存在 $\mathfrak{A}$ 使得 $\mathfrak{A} \models \Gamma$。

♡

为了找到这个模型，我们引入 Henkin 定理的概念：

定义 3.10 (Henkin 定理)

T 是 Henkin 定理，当且仅当对于任意语句 $\exists x, \varphi(x) \in T$，存在常量符号 c 使得 $\varphi(c) \in T$.

♣

定义 3.11 (扩张 (Extension))

若 $T' \supseteq T$，则 T' 被称作 T 的扩张。

♣

定义 3.12 (保守扩张 (Conservative Extension))

对任意不含新符号的句子 φ，若 $T' \vdash \varphi$ 则必有 $T \vdash \varphi$，则称 T' 是 T 的保守扩张。

♣

定义 3.13 (Henkin 扩张)

设 T 是语言（符号集）L 上的一个理论。我们通过扩展得到理论 T^*，它定义在扩展语言 L^* 上。对于每个公式 $\varphi(x)$，引入一个新的常元符号 c_φ，并添加公理：

$$\exists x\, \varphi(x) \ \rightarrow\ \varphi(c_\varphi) \tag{3.18}$$

则称这是对语言 L 的 Henkin 扩张。c_φ 被称作见证元素。

♣

命题 3.2

Henkin 扩张是保守的。

♠

证明 设 T 是语言 L 上的一个理论。若 $T, \exists x\, \varphi(x) \rightarrow \varphi(c_\varphi) \vdash \psi, \quad \psi \in L$, 则有 $T \vdash \psi$.

证明思路如下。首先我们先只引入一个新公理：

$$\begin{aligned}
&T \vdash (\exists x\, \varphi(x) \rightarrow \varphi(c_\varphi)) \rightarrow \psi \\
&T \vdash \forall y\, ((\exists x\, \varphi(x) \rightarrow \varphi(y)) \rightarrow \psi) \\
&T \vdash (\exists y\, (\exists x\, \varphi(x) \rightarrow \varphi(y))) \rightarrow \psi \\
&T \vdash (\exists x\, \varphi(x) \rightarrow \exists y\, \varphi(y)) \rightarrow \psi \\
&T \vdash \psi
\end{aligned}$$

这里用到了 c_φ 是没有用过的符号这一事实。由此我们可以进一步向上述集合继续添加新公理，做语言的扩张，从而得到了一个定理集列 $T_i = T^*_{i-1}$。记 $T_\varepsilon = \bigcup_{i=0}^{\infty} T_i$。因此任意存在性命题都在某一个 T_i 中有符号对应：

$$\exists x, \varphi(x) \in T_i \tag{3.19}$$

而：

$$\exists x, \varphi(x) \rightarrow \varphi(C_\varphi) \in T_{i+1} \subseteq T_\varepsilon \tag{3.20}$$

在整个扩张中都保持了保守性，从而 Henkin 扩张也是保守的。

至此我们可以回到定理3.2的构造。定义模型 $\mathfrak{A}$:

$$\Omega = \{\text{Closed term } t \in T_\varepsilon\} \tag{3.21}$$

定义 3.14 (封闭项 (Closed Term))

若一个项中不含有任何自由变量，则称其为 封闭项。封闭项只由常量和函数符号生成，不依赖于变量。

对于 Closed term，我们有:

1. $[\![f(t_1,\cdots,t_m)]\!] = f([\![t_1]\!],\cdots,[\![t_m]\!]) = f(t_1,\cdots,t_m)$;
2. $[\![P(t_1,\cdots,t_m)]\!] = \begin{cases} 1 & \text{If } P(t_1,t_2) \in T_\varepsilon \\ 0 & \text{o.w.} \end{cases}$

但这个定义是有坑的，因为它并不能保证排中律——不过现在我们至少已经可以保证他们不能都在里面，否则这个定理集合将不是相容的。下面我们来填补它。

我们进一步扩展 T_ε 至 T_ε^*。为此，我们将所有语句排序，如果一个命题与其逆均不属于 T_ε，那我们就将其中一个语句加入定理集。

注 排序要求可数性，对于不可数集，需要借助 Zorn's Lemma 来保证完全扩张的存在性。

进而定理集几乎被扩充完全了，有:

$$[\![\varphi]\!] = \begin{cases} 1 & \text{If } \varphi \in T_\varepsilon^* \\ 0 & \text{o.w.} \end{cases} \tag{3.22}$$

最后我们给等号打个小补丁。

定义 3.15 (等价关系 (Equivalence Relation))

$$t_1 \sim t_2 \qquad \text{if} \qquad t_1 = t_2 \in T_\varepsilon^* \tag{3.23}$$

我们将宇宙模掉等价关系，得到若干等价类，并要求相同等价类的赋值相等，则可有:

$$[\![t_i = c]\!] = \begin{cases} 1 & \text{If } t_i = c \in T_\varepsilon^* \bmod \sim \\ 0 & \text{o.w.} \end{cases} \tag{3.24}$$

笔记 注意到赋值最大为 1:

$$[\![\exists x\, \varphi(x)]\!]_{\mathfrak{A}} = \max_{c\in\Omega} [\![\varphi(\bar{c})]\!]_{\mathfrak{A}} \tag{3.25}$$

模型的大小与语言的大小是相等的:

证明 我们分两步证明。

(1) 上界. 每个封闭项是由有限个符号（常量、函数符号）构造而成，因此所有封闭项的集合是语言 L 符号的有限串的子集。若 $|L| = \kappa$，则有限串的总数为 $\kappa^{<\omega} = \kappa$。因此有 $|\Omega| \le |L|$。

(2) 下界. Henkin 扩张保证了语言 L 至少含有一个常量符号。对于每个符号（常量或函数），我们都可以构造出相应的封闭项：每个常量符号本身就是一个封闭项；每个函数符号与已有封闭项结合，也生成新的封闭项。因此我们至少可以生成 $|L|$ 个不同的封闭项。所以 $|\Omega| \ge |L|$。

综上，$|\Omega| \le |L|$ 且 $|\Omega| \ge |L|$，于是

$$|\Omega| = |L| \tag{3.26}$$

命题 3.3

存在实数的可数模型。

笔记 我们可以找到一个可数大小的描述实数所有性质的模型。(因为语言满足的公式是有限的或可数的)

笔记 我们也可以找到一个不可数大小的 Peano Based 的模型。

第四章 集合论 (Set Theory)

在集合论里，我们只需要两种谓词：$\in, =$。但为了方便，我们还会引入一些额外的函数，例如 $\varnothing, \cap, \cup$ 等。在之前我们已经学习过了朴素集合论，但朴素集合论会带来一些悖论，例如：

这是一句谎言。

于是我们需要公理化集合论，以规避掉这些潜在的风险。我们并不能认为我们随随便便把几样物品放在一起便产生了一个集合。

假设 S 是一个集合，为 $\varphi(\cdot)$ 是一个单变量的公式，那么：

$$\{x \mid x \in S \wedge \varphi(x)\} \tag{4.1}$$

也是一个集合。我们不能定义一个包含所有集合的集合，但是我们可以定义一个包含所有集合的类，被称作**集合类**。接下来我们公理化集合论。

公理 4.1

- （外延公理）$\forall x \forall y((\forall z\, z \in x \leftrightarrow z \in y) \to x = y)$
  定义等号
- （分离公理）$\forall x \forall w \exists y(\forall z\, z \in y \leftrightarrow z \in x \wedge \varphi(z, w))$
  定义了满足某个条件的子集
- （配对公理）$\forall x \forall y \exists z(x \in z \wedge y \in z)$
  定义了包含两个集合的集合
- （并集公理）$\forall x \exists y \forall z \forall w((z \in x \wedge w \in z) \to w \in y)$
  可以把一个集合的集合取并集
- （幂集公理）$\forall x \exists y \forall z(z \subseteq x \to z \in y)$
  可以取一个集合的幂集
- （无穷公理）$\exists N(\varnothing \in N \wedge (\forall y(y \in N \to y \cup \{y\} \in N))$
  存在归纳集，或者说存在自然数集
- （替代公理）$\forall A \forall w(\forall x\, x \in A \to (\exists! y\, \varphi(y, x, w))) \to (\exists B(\forall x\, x \in A \to (\exists y\, \varphi(y, x, w) \wedge y \in B)))$
  任意集合元素经过一个函数的值可以组成一个集合
- （正则公理）$\forall x\, x \neq \varnothing \to (\exists y\, y \in x \wedge y \cap x = \varnothing)$
  用来排除循环属于关系导致的悖论。考虑一个有向图模型，$x \in y$ 则从 x 向 y 连一条边。假设有循环属于关系，则图里有一个环。使用配对公理，存在一个点 x_0 仅指向环里所有的点。对 x_0 点代入正则公理，则任何环上的点 y 都不满足 $y \cap x = \varnothing$ 与正则公理矛盾。
- （选择公理）$\forall S((\forall x\, x \in S \to x \neq \varnothing) \wedge (\forall x \forall y\, (x \in S \wedge y \in S \wedge x \neq y) \to x \cap y = \varnothing)) \to (\exists T(\forall x\, x \in S \to \exists! y\, y \in x \cap T))$
  定义集合族上可以从每个集合里选一个元素出来组成一个集合

我们接下来定义函数。首先从有序对开始。

定义 4.1

用 $\{\{x\}, \{x, y\}\}$ 作为有序对 (x, y) 的集合论语言。

此后我们一般用惯用记号 (x, y) 来代替严格集合论语言。有了有序对我们定义笛卡尔积。

定义 4.2

定义 S 和 T 的笛卡尔积 $S \times T = \{(x, y) | x \in S \wedge y \in T\}$

首先我们考虑得到所有无序对的集合。对 $S \cup T$ 的幂集使用分离公理得到所有无序对的集合。然后用替代公理把每个无序对映射到有序对。最后再过一次条件为 S 中元素在前面的分离公理得到笛卡尔积。

定义 4.3

称 R 是一个 S 和 T 上的关系，当 $R \subseteq S \times T$。记 aRb 为 $(a,b) \in R$ 的简记。

对一个关系加以各种限制会有不同的定义。我们来定义函数关系。

定义 4.4

称 R 是函数关系若 $\forall x \in S, \exists! y\, xRy$。则根据此关系可定义函数 $f(x) = \cup\{y|xRy\}$。

用函数的形式，选择公理还有一个形式

公理 4.2

$$\forall S((\forall x\, x \in S \to x \neq \varnothing) \wedge (\forall x \forall y\, (x \in S \wedge y \in S \wedge x \neq y) \to x \cap y = \varnothing)) \to (\exists f : S \to \cup S(\forall x\, x \in S \to f(x) \in x))$$

接下来是简化版的哥德尔不完备定理。

我们试图构造一个命题 $\varphi \to \neg\varphi$。这样一个无矛盾系统无法证明出来 φ.

为了创造这个条件，试图让集合论语言本身以字符串操作的形式对命题做推导。定义一个从命题到数的映射, 且保持序列性质。由于集合论本身就可以描述数相关的操作，所以一个命题的编码依然对应一个合法命题。为了简化用双引号表示这一映射。

我们对所有基本符号，分别对应一个从 1 开始的数字。比如说 $\forall$ 对应 1，$\neg$ 对应 2，$\to$ 对应 3，以此类推。

对于一个命题字符串，我们使用 100 进制进行赋值。唯一的变化是变量符号可能很多。我们规定所有变量符号依次对应 19×100^t，且占位 $t+1$ 位的长度进行赋值。

定义一个集合 $TERM$ 表示所有的 term 对应编码的集合。

定义 4.5

- $C_1(X) = \text{"}\varnothing\text{"} \in X$
- $C_2(X) = \text{"1"} \in X$
- $C_3(X) = \forall t \geq 0, \text{"}x_0\text{"} \times 100^t \in X$
- $C_4(X) = \forall \text{"}t_1\text{"}, \text{"}t_2\text{"} \in X, \text{"}f(t_1,t_2)\text{"} \in X$

令 $C = C_1 \wedge C_2 \wedge C_3 \wedge C_4$ 表示以上所有条件全都满足。则定义 $\forall X, C(X) \to TERM \subseteq X$

用类似方法，以满足构造规则的最小集合定义的方法可以构造出来 $FORM$ 表示所有合法命题编码的集合。

我们考虑同样方法定义所有能被证明的命题编码的集合 $PROV$。规则是初始所有公理编码在 X 里，对于自然演绎法的几条规则都放到 X 的规则里，$PROV$ 就是满足所有规则的最小的 X。我们把这个规则显式的记为 $C_p(X)$。

最终利用我们的编码，我们可以构造一个命题使得内部使用有限的编码以及对命题编码的字符串修改得到对命题自身的编码描述。

$$\phi = \forall PROV\, C_p(PROV) \to (\forall x, (x = BLOCK) \to (\forall y, (y \text{ is } x \text{ but replaces the first "z" by } x) \to y \notin PROV))$$

其中

$$BLOCK = \text{"}\forall PROV\, C_p(PROV) \to (\forall x, (x = z) \to (\forall y, (y \text{ is } x \text{ but replaces the first "z" by } x) \to y \notin PROV))\text{"}$$

抛开繁琐的严格集合论语言，实际上 ϕ 定义里的 x 和 y 都是固定好的。x 就是 $BLOCK$。y 把 $BLOCK$ 字符串里的 z 位置替换成了 x，注意此时 x 是 $BLOCK$，替换之后 y 就成了 "ϕ"，那么此时 ϕ 的语义是 "ϕ" $\notin PROV$，产生了矛盾。则 ϕ 是一个不能被证明的命题。证毕。

图灵机视角的哥德尔不完备定理：存在一个验证机 $TM(\phi, proof)$ 可验证对于 ϕ 这个命题，$proof$ 是否是一个合法证明。这个图灵机只需要根据自然演绎法就能写出来。

假设所有命题都可以被证明或证伪，那么对所有命题都存在一个有限长的证明。那么存在一个图灵机 M，枚举所有的 $proof$，运行 TM 来验证是否合法，最终判断命题是否为真。

若存在这样的 M，则对于停机问题 $HALT(TM, x)$，可用集合论语言定义输入 x 的图灵机 TM 所有格局的集合 $S(TM, x)$。用 M 判断是否存在停机格局属于 $S(TM, x)$ 即可。

补充一个停机问题不可判定的证明：

定义 $UC : \{0,1\}^* \to \{0,1\}$ 函数：确定一个从 01 字符串到图灵机的编译器，此后默认用字符串 x 唯一确定一个图灵机 M_x。输入 x 时，若 $M_x(x) = 1$，则 $UC(x) = 0$。否则 $UC(x) = 1$。（M_x 输入 x 输出 0 或者永不停机都算）

假设存在一个图灵机 M 计算 UC 函数，那么 M 输入 M 时，根据 UC 定义 $M(M) \neq UC(M)$，矛盾。我们证明了 UC 函数不可计算。

对于停机问题 $HALT(M, x)$，假设存在一个图灵机 M 计算 $HALT$，那么我们可以构造 M' 计算 UC 函数。M' 输入 x 后，调用 $M(x, x)$。若结果为 0 即不停机，则返回 1。若结果为 1 即停机，那么用通用图灵机运行 $UTM(x, x)$ 翻转结果返回。

由于已知 UC 不可计算，矛盾。证明了 $HALT$ 不可计算。

第五章 初等数论 (Elementary Number Theory)

这一节介绍一些基本数论工具。我们默认 universe 是 $\mathbb{Z}$。

定义 5.1

称 $a|b$，若 $\exists n, b = an$。

有几条性质

命题 5.1

- $a|a$
- $a|b \wedge b|a \to a = b$
- $a|b \wedge b|c \to a|c$

即整除关系是一个偏序关系。

定义 5.2

$\forall a > 0, b$，存在唯一的 $q, r \in \mathbb{Z}$，使得 $r = \{0, 1, \ldots, a-1\}$，且 $b = aq + r$。

称为带余除法。

定义 5.3

定义素数判定函数 $Prime(n) = n \neq 1 \wedge (\forall a > 0, a|n \to (a = 1 \vee a = n))$。

定义 5.4

定义两个数最大公约数为：$gcd(m,n) =$ the greatest positive integer a $s.t.$ $a|m \wedge a|n$

边界条件 $gcd(0,n) = n$。

若 $gcd(a,b) = 1$，称 a 和 b 互质（coprime）

计算 $gcd(m,n)$ 我们使用辗转相除法来实现。

Algorithm 5 最大公约数 gcd

```
function gcd(m, n)
    if m > n then
        return gcd(n, m)
    else if m = 0 then
        return n
    else
        n = mq + n'
        return gcd(n', m)
    end if
end function
```

对于正确性，前两步只是确保 $m \leq n$ 和处理了边界条件。对于 $0 < m \leq n$ 的情况，$n' = n - mq$ 且 $n = mq + n'$。

那么 $\forall a, a|n \wedge a|m \to a|n'$，$\forall a, a|n' \wedge a|m \to a|n$。推出 $gcd(m,n) = gcd(n', m)$

对于可行性，每次 m 是严格递减，一定会终止。

扩展欧几里得算法

再定义另外一个函数 $gcd'(m,n) = \min\{am + bn | a, b \in \mathbb{Z}\}$

首先显然有 $gcd(m,n) | gcd'(m,n)$。接下来我们证明可以在辗转相除法过程中顺便计算出一对解满足 $am + bn = gcd(m,n)$，从而证明 $gcd(m,n) = gcd'(m,n)$。

考虑上面的算法中我们要求额外返回一组解 a,b。则第一种情况 $m>n$，将返回的解翻转一下返回即可。第二种情况 $m=0$，直接返回 $(0,1)$ 即可。对于第三种情况，我们对于子问题得到了 $bn'+am=gcd(n',m)$。由 $n'=n-mq$，得到 $(a-bq)m+bn=gcd(n',m)=gcd(m,n)$，则返回 $(a-bq,b)$ 即可。

由此有一个经典推论 $gcd(m,n)=1\rightarrow\exists a,b\in\mathbb{Z},am+bn=1$。

命题 5.2

$gcd(a,b)=1\wedge gcd(a,c)=1\rightarrow gcd(a,bc)=1$

证明：由于 $am+bn=1$，$am'+cn'=1$，有

$bn=1-am$，$cn'=1-am'$，得 $bcnn'=1-(m+m'+mm'a)a$，即 $nn'bc+(m+m'+mm'a)a=1$，即 $gcd(a,bc)=1$

命题 5.3

若 p 为质数，则

$$gcd(p,a)=\begin{cases}p & p|a\\ 1 & \text{otherwise}\end{cases}$$

定理 5.1

$\forall n$ 存在一个唯一素数分解。证明: 数学归纳法，$n=1$ 或 $PRIME(n)$ 时满足.

假设 $m<n$ 时结论都成立，当 $m=n$ 时：

假设 $n=p_1p_2\dots p_t=q_1q_2\dots q_s$

p_1 是质数，且 $p_1|q_1q_2\dots q_s$，则 $\exists i,p_1=q_s$。等号两侧除掉相等这一项，剩余的由归纳假设都是一样的素数可重集合。则 n 有唯一素数分解。

同余

定义 5.5

$a\equiv b\pmod m$ 称 a 和 b 在模 m 意义下同余，若 $m|a-b$。

命题 5.4

性质里忽略 $\pmod m$，默认都是模同一个数意义下。

- $a\equiv a$
- $a\equiv b\rightarrow b\equiv a$
- $a\equiv b\wedge b\equiv c\rightarrow a\equiv c$

以上三条说明他是个等价条件。

- $a\equiv b\wedge c\equiv d\rightarrow(a+b\equiv c+d,ab\equiv cd)$

对一个等价关系我们可以取一个等价关系代表元的集合，在同余关系下集合为 $\mathbb{Z}_m=\{0,1,\dots,m-1\}$

命题 5.5

若 $gcd(c,m)\neq1$，则 $ac\equiv0$ 不能推出 $a\equiv0$。

证明：设 $d=gcd(c,m)$，则 $\frac{m}{d}\cdot c\equiv0$。

若 $gcd(c,m)=1$，则存在 $ac+bm=1$，即 $\exists c^{-1}=a$ 使得 $cc^{-1}\equiv1$

定义 5.6

$\mathbb{Z}_m^*=\{n\in\mathbb{Z}_m|gcd(n,m)=1\}$

定理 5.2

（费马小定理）若 p 是质数，则 $x^p \equiv x \pmod p$。

证明：当 $gcd(x,p) = p$ 时结论显然。当 $gcd(x,p) = 1$ 时：

$1 \cdot 2 \cdot \ldots \cdot (p-1) = (p-1)!$

$x \cdot 2x \cdot \ldots \cdot (p-1)x = (p-1)!x^{p-1}$

由 $gcd(x,p) = 1$，$a \not\equiv b \to ax \not\equiv bx$。则 $x \cdot 2x \cdot \ldots \cdot (p-1)x \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1)$

$(p-1)! \equiv (p-1)!x^{p-1}$ 推出 $x^{p-1} \equiv 1$。证毕。

♡

对于一般的模数 m 情况下，我们需要用到 $\mathbb{Z}_m^*$。

定义 5.7

欧拉函数定义为 $\phi(m) = |\mathbb{Z}_m^*|$。

♣

那么有新的定理

定理 5.3

（欧拉定理）若 $gcd(x,m) = 1$，则有 $x^{\phi(m)} \equiv 1 \pmod m$。

证明：令 $P = \prod_{i \in \mathbb{Z}_m^*} i$

由 $a, b \in \mathbb{Z}_m^*, a \not\equiv b$ 可知 $ax \not\equiv bx$。则 $\prod_{i \in \mathbb{Z}_m^*} xi = x^{\phi(m)} \prod_{i \in \mathbb{Z}_m^*} i = x^{\phi(m)} P$，且 $\prod_{i \in \mathbb{Z}_m^*} xi \equiv \prod_{i \in \mathbb{Z}_m^*} i = P$

则 $x^{\phi(m)} \equiv 1 \pmod m$

♡

关于欧拉函数还有一些有用的性质

命题 5.6

$m = \sum_{d|m} \phi(d)$

证明：

$$
\begin{aligned}
m &= \sum_{i=1}^{m} 1 \\
&= \sum_{d|m} \sum_{i=1}^{m} [gcd(i,m) = d] \\
&= \sum_{d|m} \sum_{i=1}^{\frac{m}{d}} [gcd(i, \frac{m}{d}) = 1] \\
&= \sum_{d|m} \phi(\frac{m}{d}) \\
&= \sum_{d|m} \phi(d)
\end{aligned}
$$

♠

定理 5.4

（中国剩余定理）若 $n_1, n_2, \ldots, n_t$ 两两互质。令 $N = n_1 n_2 \ldots n_t$。则存在一个从 $\mathbb{Z}_N$ 到 $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_t}$ 的双射。

更具体的，$\pi(a) = (a \mod n_1, a \mod n_2, \ldots, a \mod n_t)$ 就是一个这样的双射。

证明：下证存在一个从右到左的映射且是 π 的逆映射，即证明 π 是满射。

令 $m_i = \frac{N}{n_i}$，则 $gcd(m_i, n_i) = 1$。则存在 $t_i = m_i^{-1}$，即 $t_i m_i \equiv 1 \pmod{n_i}$。

定义 $\pi^{-1}(a_1, a_2, \ldots, a_t) = \sum_{i=1}^{t} a_i t_i m_i \mod N$。

注意到 $\pi^{-1}(a_1, a_2, \ldots, a_t)$ 模 n_i 时，和式里除了第 i 项以外的 m_j 都是 n_i 的倍数，其他项都是 0。剩下 $a_i t_i m_i \mod n_i = a_i$。则构造的映射就是 π 的逆映射。证毕。

由映射两侧的集合大小相等，且是满射，则 π 是一个双射。

命题 5.7

（欧拉函数计算公式）设 $N = p_1^{k_1} \ldots p_t^{k_t}$ 为其唯一分解。令 $n_i = p_i^{k_i}$。

则 $\phi(N) = \prod_{i=1}^{t}(p_i^{k_i} - p_i^{k_i - 1})$。

证明：由中国剩余定理，存在一个从 $\mathbb{Z}_N$ 到 $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_t}$ 的双射 π。

而且，$\forall a$ 若 $gcd(a, N) = 1$，当且仅当 $\forall i \in [t], gcd(a, n_i) = 1$。那么 pi 也是从 $\mathbb{Z}_N^*$ 到 $\mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^* \times \ldots \times \mathbb{Z}_{n_t}^*$ 的双射。即 $\phi(N) = \prod_{i=1}^{t} \phi(n_i)$。易知 $\phi(p_i^{k_i}) = p_i^{k_i} - p_i^{k_i - 1}$。证毕。

欧拉定理一个直接的应用是 RSA 公钥加密。

（非严格）公钥加密的场景是，有一对公钥和私钥 (pk, sk)，其中公钥 pk 公开，所有人都可以用 pk 加密一条消息。私钥 sk 只有部分人有。有私钥的人才能解密这条消息，其他人很难解密。

定理 5.5

（RSA 公钥加密方案）公钥为 (N, e)，私钥为 (p, q)。其中 p, q 为质数，$N = pq$。则 $\phi(N) = (p-1)(q-1)$。$e \in \mathbb{Z}_{\phi(N)}^*$。

加密一条消息 $m \in \mathbb{Z}_N^*$ 时，加密结果为 $c = m^e \mod N$。

解密时，先计算一个 d 使得 $ed \equiv 1 \pmod{\phi(N)}$。然后计算 $c^d \mod N$。

正确性：$c^d \equiv m^{ed} \equiv m \pmod N$

安全性（非严格）：已知 N 很难算出 p, q，也很难算出 $\phi(N)$。也很难算出 m。

二次剩余

定义 5.8

称 r 是模 N 的二次剩余，若 $\exists x, x^2 \equiv r \pmod N$。

由 $x^{p-1} \equiv 1 \pmod p$，则 $r^{\frac{p-1}{2}} \equiv 1 \pmod p$

考虑 $x^{p-1} - 1 \equiv 0 \pmod p$。把式子看成多项式，由于每个元素都满足这个等式，则有 $x^{p-1} - 1 = \prod_{a \in \mathbb{Z}_p^*}(x - a)$。

把其中满足 $x^{\frac{p-1}{2}} - 1 \equiv 0$ 的部分拿出来，那么有 $x^{p-1} - 1 = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1)$。由于所有元素都是这两个因式之一的因子，所以所有元素都满足 $x^{\frac{p-1}{2}}$ 等于 1 或 -1。

定义 5.9

我们定义勒让德符号

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & x = 0 \\ 1 & x \text{ is a QR} \\ -1 & \text{O.W.} \end{cases}$$

考虑映射 $\pi(x) = x^2 \mod p$，则 π 是个二对一的映射 $\pi(x) = \pi(p - x) = x^2$。而且每个元素至多两个根。则 π 映射像集大小为 $\frac{p-1}{2}$。而满足 $x^{\frac{p-1}{2}} = 1$ 的元素一共有 $\frac{p-1}{2}$ 个，则这部分一定是二次剩余，剩下的部分一定是非

二次剩余。则勒让德符号可以直接表示为 $x^{\frac{p-1}{2}}$。

定理 5.6

（二次互反律）对于两个奇素数 p,q，有 $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{(p-1)(q-1)}{4}}$。

第六章 群 (Group)

内容提要

- ❑ 这个我也不是很懂，这个得助教讲。
- ❑ 我有点忘记了。
- ❑ 我们好像什么都没讲。
- ❑ 说明这门课其实没什么可讲的。

6.1 群 (Group)

定义 6.1 (群（Group）)

设 G 是一个非空集合，$*$ 是定义在 G 上的二元运算。若满足以下条件：

1. 封闭性（Closure）：对任意 $a,b\in G$，有 $a*b\in G$；
2. 结合律（Associativity）：对任意 $a,b,c\in G$，有 $(a*b)*c=a*(b*c)$；
3. 单位元（Identity element）：存在 $e\in G$，使得对任意 $a\in G$，有 $e*a=a*e=a$；
4. 逆元（Inverse element）：对任意 $a\in G$，存在 $a^{-1}\in G$，使得 $a*a^{-1}=a^{-1}*a=e$。

则称 $(G,*)$ 为一个群（**group**）。

命题 6.1

一个群内只有一个单位元。

证明

$$e_1=e_1*e_2=e_2 \tag{6.1}$$

命题 6.2

一个群内的一个元素 a 只有一个逆元，记作 a^{-1}。

证明

$$b'=e'b=bab'=be=b \tag{6.2}$$

命题 6.3

群中的元素在两次取逆下不变。

证明

$$(a^{-1})^{-1}=a(a^{-1})(a^{-1})^{-1}=a \tag{6.3}$$

注 其实我们忽略了左单位元，右单位元，左逆，右逆的概念。严格来说，需要经过一些不难的证明去说明左单位元右单位元都等价于单位元，左逆右逆都等价于逆元。

常见的群包括 $(\mathbb{Z},+)$，$(\mathbb{Q}/\mathbb{R}/\mathbb{C},+)$，$(\mathbb{Z}_n,+)$，$(\mathbb{Z}_n^*,\times)$，$(\mathbb{Q}/\mathbb{R}/\mathbb{C}-\{0\},\times)$，$(G,*)$，$(H,\circ)$，$(G\times H,\cdot)$...

定义 6.2 (对称群（Symmetric Group）)

设 X 是一个含有 n 个元素的集合。所有从 X 到 X 的双射（即既单射又满射的映射）在函数复合运算 $\circ$ 下构成一个群，称为 X 上的对称群，记作 S_X。当 $X=\{1,2,\dots,n\}$ 时，记作 $\mathrm{Sym}_n=S_n$，称为 n 阶对称群。S_n 群乘法为映射的复合。

定义 6.3 (子群（Subgroup）)

设 $(G,*)$ 是一个群，H 是 G 的非空子集。若 H 在运算 $*$ 下本身也是一个群，即满足：

1. 对任意 $a,b\in H$，有 $a*b\in H$；
2. 对任意 $a,b,c\in H$，有 $(a*b)*c=a*(b*c)$；
3. 存在 $e_H\in H$ 使得对任意 $a\in H$，有 $e_H*a=a*e_H=a$；
4. 对任意 $a\in H$，存在 $a^{-1}\in H$ 使得 $a*a^{-1}=a^{-1}*a=e_H$，

则称 H 是 G 的一个子群（**subgroup**），记作 $H\leq G$。

定义 6.4 (陪集（Coset）)

设 G 是一个群，$H\leq G$ 是其子群，$a\in G$。定义：

- 左陪集（**Left Coset**）：a 关于 H 的左陪集定义为

$$aH=\{a*h\mid h\in H\};\tag{6.4}$$

- 右陪集（**Right Coset**）：a 关于 H 的右陪集定义为

$$Ha=\{h*a\mid h\in H\}.\tag{6.5}$$

陪集可以看作群 G 在子群 H 作用下的平移所得的子集。

命题 6.4

两元素关于子群 H 的陪集相等，当且仅当二者之间仅相差一次 H 内元素的乘法。

证明 Trivial.

定义 $a\sim b\Leftrightarrow b\sim a$ 当且仅当二者一侧陪集相等。$\sim$ 关系可以被证明为一种等价关系。从而我们可以将任意群 G 看做其内部等价类的不交并。

$$a\sim b\iff a^{-1}b\in H\tag{6.6}$$

命题 6.5

设 G 是一个群，$H\leq G$ 是其子群。对任意 $a\in G$，其左陪集

$$aH=\{ah\mid h\in H\}\tag{6.7}$$

与 H 具有相同的元素个数（即大小相等）。

证明 注意到 $|aH|=|H|$ 即可。

且若 $aH\neq bH$，$aH\cap bH=\varnothing$。反证法若 $\exists h_1,h_2\in H, ah_1=bh_2$，则 $a=bh_2h_1^{-1}$，即 $aH=bH$，矛盾。因此如果 G 是有限群，子群（陪集）的大小一定需要能整除群的大小。

定义 6.5 (正规子群（Normal Subgroup）)

设 G 是一个群，$H\leq G$ 是其子群。若对任意 $g\in G$，都有

$$gHg^{-1}=H\tag{6.8}$$

则称 H 为 G 的一个正规子群（normal subgroup），记作 $H\trianglelefteq G$。等价地，H 为正规子群当且仅当对任意 $g\in G$，左陪集与右陪集相等，即

$$gH=Hg\tag{6.9}$$

正规子群的等价定义为：设 G 是一个群，$N\leq G$。若对任意 $a\in G$ 与 $g\in N$，都有

$$aga^{-1}\in N\tag{6.10}$$

定义 6.6 (交换群（Abelian Group）)

如果群的乘法具有交换律，那么便是一个交换群。 ♣

交换群自然地是正规子群。

考虑 G 的正规子群 N，我们接下来说明 $a, b \in G$, $aN \cdot bN \mapsto (ab)N$ 构成群运算。注意到：

$$\begin{aligned}\{a\}N\{b\}N &= \{a\}(Nb)N \\ &= \{a\}(bN)N \\ &= \{ab\}N = abN\end{aligned}$$

从而剩下的性质是不证自明的，其中 N 是群 $(\{aN : a \in G, \cdot\})$ 的单位元。

定义 6.7 (商群（Quotient Group）)

设 G 是一个群，$H \trianglelefteq G$ 是其正规子群。在这种情况下，所有 H 的左陪集构成的集合

$$G/H = \{\, aH \mid a \in G \,\} \tag{6.11}$$

在如下运算下：

$$(aH) \cdot (bH) = (ab)H \tag{6.12}$$

构成一个群，称为 G 关于 H 的商群（quotient group）。其单位元为 H，逆元为 $(aH)^{-1} = a^{-1}H$。 ♣

例题 6.1 例如对于群 $(\mathbb{Z}, +)$，有 $\{nk : k \in \mathbb{Z}\}L = n\mathbb{Z}$ 上的正规子群，则商群构成同余类。这是显然的。

例题 6.2 $\mathrm{GL}_n(\mathbb{F})$ mod $\mathrm{SL}_n(\mathbb{F})$ 即 $\mathbb{F}$ 上的乘法群。

定义 6.8 (自由群（Free Group）)

设 X 是一个非空集合，称其元素为生成元（generators）。由 X 及其形式逆元 $X^{-1} = \{x^{-1} \mid x \in X\}$ 构成的所有有限字（即由 $X \cup X^{-1}$ 的元素按顺序连接而成的符号串）组成的集合，在以下约化规则下：

$$xx^{-1} = x^{-1}x = e, \tag{6.13}$$

称为自由群，记作 $F(X)$。其群运算是字的等价类的连接并随后约化，单位元是空字 ε。 ♣

自由群元 $\bar{s}_1 \cdots \bar{s}_n$ 的逆为 $\bar{s}_n^{-1} \cdots \bar{s}_1^{-1}$。

注 $F(a)$ 与整数的加法群同构，注意到：

$$F(a) \quad \varepsilon,\ a,\ aa, \cdots;\ a^{-1},\ a^{-1}a^{-1}, \cdots \tag{6.14}$$

换言之，$F(X)$ 是一个满足以下**泛性质**（universal property）的群：对任意群 G 和任意映射 $f : X \to G$，存在唯一的群同态

$$\varphi : F(X) \to G \tag{6.15}$$

使得 $\varphi|_X = f$。

定义 $\langle S \rangle$ 为包含 S 的最小子群，亦被称作**被 S 生成的子群**。

若 X 的基数为 n，则 $F(X)$ 称为 n **生成元自由群**，记作 F_n。

回到对称群。考虑非常简单的一种对称群：置换群。

定义 6.9 (置换群（Permutation Group）)

设 X 是一个非空集合。所有从 X 到自身的双射（即一一且到的映射）在复合运算 $\circ$ 下构成一个群，称为 X 上的置换群（permutation group），记作

$$\mathrm{Sym}(X) = \{\, \sigma : X \to X \mid \sigma \text{ is bijection} \,\} \tag{6.16}$$

当 $X = \{1, 2, \ldots, n\}$ 时，记作 S_n，称为 n 阶对称群（**symmetric group of degree** n）。S_n 的元素称为置换

（**permutations**），群运算为映射的复合：

$$(\sigma \circ \tau)(i) = \sigma(\tau(i)), \quad \forall i \in \{1, 2, \ldots, n\}. \tag{6.17}$$

例题 6.3 在 S_3 中，考虑置换

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \tag{6.18}$$

即 $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$。我们可以将其表示为循环记号 $\sigma = (1\,2\,3)$。

该置换可以拆解为若干个**对换（transpositions）**（即交换两个元素的置换）的复合，例如：

$$(1\,2\,3) = (1\,3)(1\,2). \tag{6.19}$$

验证：

$$\begin{aligned} &(1\,2) : 1 \leftrightarrow 2,\ 3 \text{ 不变;} \\ &(1\,3) : 1 \leftrightarrow 3,\ 2 \text{ 不变.} \end{aligned} \tag{6.20}$$

依次作用可得：

$$1 \xrightarrow{(1\,2)} 2 \xrightarrow{(1\,3)} 2, \quad 2 \xrightarrow{(1\,2)} 1 \xrightarrow{(1\,3)} 3... \tag{6.21}$$

实际上最终结果为

$$1 \mapsto 2, \quad 2 \mapsto 3, \quad 3 \mapsto 1, \tag{6.22}$$

恰好是 $(1\,2\,3)$。

因此，任意置换都可以分解为若干个对换的复合；换句话说，

$$S_n = \langle (i\,j) \mid 1 \le i < j \le n \rangle \tag{6.23}$$

即 S_n 由所有对换生成。

命题 6.6

对换（交错）群是对称群的子群。

练习 6.1 二面体群的半直积结构与置换实现 设 $n \ge 3$。n 边形的二面体群记作 D_{2n}，由旋转 r 与某一条反射 s 生成，满足关系

$$r^n = e, \qquad s^2 = e, \qquad srs = r^{-1}. \tag{6.24}$$

因此

$$D_{2n} \cong C_n \rtimes C_2, \tag{6.25}$$

其中 $C_2 = \langle s \rangle$ 通过共轭作用

$$\varphi(s) : C_n \to C_n, \quad \varphi(s)(r) = r^{-1} \tag{6.26}$$

给出非平凡自同构，从而构成半直积。

令 n 个顶点沿圆周按顺序标号为 $1, 2, \ldots, n$。定义

$$r = (1\,2\,\cdots\,n) \in S_n, \tag{6.27}$$

以及一条轴对称对应的反射 $s \in S_n$。取例如下标准选择：

$$\text{若 } n \text{ 为奇数:} \quad s = (2\,n)(3\,n-1)\cdots\left(\tfrac{n+1}{2}\ \tfrac{n+3}{2}\right), \tag{6.28}$$

$$\text{若 } n \text{ 为偶数:} \quad s = (1\,n)(2\,n-1)\cdots\left(\tfrac{n}{2}\ \tfrac{n}{2}+1\right). \tag{6.29}$$

则 $r, s \in S_n$ 满足

$$r^n = e, \qquad s^2 = e, \qquad srs = r^{-1}, \tag{6.30}$$

故

$$D_{2n} = \langle r, s \rangle \leq S_n. \tag{6.31}$$

其中 r 表示顺时针旋转一格的置换，s 表示关于某条对称轴的反射置换；所有反射均为 sr^k（$0 \leq k < n$）的形式。

命题 6.7

设 $D_n = \langle r, s \mid r^n = e,\ s^2 = e,\ srs = r^{-1} \rangle$，并在 S_n 中实现为

$$r = (1\,2\,\cdots\,n). \tag{6.32}$$

则

$$\langle r \rangle \trianglelefteq D_n. \tag{6.33}$$

证明

$$sr^k s^{-1} = r^{-k} \in \langle r \rangle, \qquad rr^k r^{-1} = r^k \in \langle r \rangle, \tag{6.34}$$

从而

$$g\langle r \rangle g^{-1} = \langle r \rangle, \quad \forall\, g \in D_n, \tag{6.35}$$

这表明 $\langle r \rangle$ 为 D_n 的正规子群。

定义 6.10 (群的中心（Center）)

设 G 是一个群。定义

$$C(G) = \{\, z \in G \mid \forall g \in G,\ zg = gz \,\} \tag{6.36}$$

称为 G 的中心（center）。

换言之，$C(G)$ 由所有与群中每个元素都可交换的元素组成。中心总是 G 的一个**正规子群**，即 $C(G) \trianglelefteq G$。证明是简单的。

定义 6.11 (中心化子（Centralizer）)

设 G 是一个群，$S \subseteq G$ 是其非空子集。定义

$$C_G(S) = \{\, g \in G \mid \forall s \in S,\ gs = sg \,\} \tag{6.37}$$

称为 S 在 G 中的中心化子（centralizer of S in G）。

当 $S = \{a\}$ 仅含一个元素时，记作

$$C_G(a) = \{\, g \in G \mid ga = ag \,\}. \tag{6.38}$$

设 G 是一个群。

群的中心可以表示为所有单个元素子集的中心化子的交集：

$$C(G) = \bigcap_{g \in G} C_G(g), \tag{6.39}$$

其中 $C_G(g) = \{\, x \in G \mid xg = gx \,\}$ 是元素 g 的中心化子。

群的中心等于整个群的中心化子：

$$C(G) = C_G(G) = \{\, x \in G \mid \forall g \in G,\ xg = gx \,\}. \tag{6.40}$$

定义 6.12 (半群（Semigroup）)

设 S 是一个非空集合，$*$ 是定义在 S 上的二元运算。若该运算满足结合律：

$$\forall a,b,c\in S,\quad (a*b)*c=a*(b*c), \tag{6.41}$$

则称 $(S,*)$ 为一个半群（**semigroup**）。

♣

如果半群有幺元，则被被称作幺半群。

交换幺半群可以被**扩张**为一个群。即，我们可以找到单射 $\Pi: S\to G$，使得 $\forall a,b\in S$，有 $\Pi(ab)=\Pi(a)\cdot\Pi(b)$.

定理 6.1 (交换幺半群的 Grothendieck 群)

设 $(M,+,0)$ 为交换幺半群。定义集合 $M\times M$ 上的等价关系

$$(a,b)\sim(c,d)\iff \exists t\in M:\ a+d+t=c+b+t. \tag{6.42}$$

记等价类为 $[a,b]$，在商集 $G(M)=(M\times M)/\sim$ 上定义加法

$$[a,b]+[c,d]:=[a+c,\ b+d],\qquad 0:=[0,0],\qquad -[a,b]=[b,a]. \tag{6.43}$$

则 $(G(M),+)$ 为阿贝尔群，且映射

$$\iota: M\to G(M),\quad \iota(a)=[a,0] \tag{6.44}$$

是半群同态。若 M 具消去律（$a+c=b+c\Rightarrow a=b$），则 ι 为单射。并且 $G(M)$ 具有泛性质：对任意阿贝尔群 A 与半群同态 $f: M\to A$，存在唯一群同态

$$\overline{f}: G(M)\to A,\qquad \overline{f}([a,b])=f(a)-f(b), \tag{6.45}$$

使 $\overline{f}\circ\iota=f$。$G(M)$ 称为 M 的 **Grothendieck** 群。

♡

证明 良定性与群公理均由定义直接验证；若 M 消去，则 $[a,0]=[b,0]\Rightarrow\exists t:\ a+t=b+t\Rightarrow a=b$。泛性质由 $f(a)-f(b)$ 的良定性（利用 $\sim$ 的定义）与同态唯一性给出。

6.2 群同态 (Group Homomorphism)

定义两个群 $K,H\le G$ 的乘法：

$$KH=\{kg\mid k\in K,\ h\in H\} \tag{6.46}$$

我们有：

定理 6.2

对有限群 G 的两个子群 K,H，有

$$|KH|=\frac{|K|\cdot|H|}{|K\cap H|}=|HK|. \tag{6.47}$$

♡

证明 我们希望通过建立一个自然的双射来计算集合 KH 的大小。

因为 $K\cap H\le K$，我们可以把 K 写成不交并：

$$K=\bigsqcup_i k_i(K\cap H). \tag{6.48}$$

同时，KH 可以按 H 的左陪集分解为：

$$KH=\bigsqcup_i k_iH. \tag{6.49}$$

我们的目标是证明这两个块集合之间存在一一对应。

定义映射

$$\Phi: K/(K\cap H)\longrightarrow KH/H,\qquad \Phi(k(K\cap H))=kH. \tag{6.50}$$

若 $k_1(K\cap H)=k_2(K\cap H)$，则 $k_2^{-1}k_1\in K\cap H\subseteq H$。因此

$$k_1H=(k_2(k_2^{-1}k_1))H=k_2H, \tag{6.51}$$

故 Φ 良定义。

若 $\Phi(k_1(K\cap H))=\Phi(k_2(K\cap H))$，即 $k_1H=k_2H$，则 $k_2^{-1}k_1\in H$ 且 $k_2^{-1}k_1\in K$，故 $k_2^{-1}k_1\in K\cap H$。因而

$$k_1(K\cap H)=k_2(k_2^{-1}k_1)(K\cap H)=k_2(K\cap H), \tag{6.52}$$

单射成立。

对任意 $xH\in KH/H$，因为 $x\in KH$，存在 $k\in K,h\in H$ 使 $x=kh$。于是

$$xH=kH=\Phi(k(K\cap H)), \tag{6.53}$$

故满射成立。

因 Φ 为双射，

$$|K/(K\cap H)|=|KH/H|. \tag{6.54}$$

由陪集公式可得

$$\frac{|K|}{|K\cap H|}=\frac{|KH|}{|H|}, \tag{6.55}$$

故

$$|KH|=\frac{|K|\cdot|H|}{|K\cap H|}. \tag{6.56}$$

交换 K,H 的角色即可得

$$|HK|=\frac{|H|\cdot|K|}{|H\cap K|}=|KH|. \tag{6.57}$$

注意 HK 与 KH 的集合不一定相同，但它们的基数必相等。

命题 6.8

设 G 为群，$K,H\leq G$。若 $H\trianglelefteq G$（或对称地 $K\trianglelefteq G$），则

$$HK=KH, \tag{6.58}$$

且 HK 是 G 的一个子群。

证明 先证明集合相等。取任意 $k\in K$。由 $H\trianglelefteq G$，有

$$kHk^{-1}=H. \tag{6.59}$$

等式两边右乘 k 得

$$kH=Hk. \tag{6.60}$$

因而

$$HK=\bigcup_{k\in K}Hk=\bigcup_{k\in K}kH=KH, \tag{6.61}$$

这就证明了 $HK=KH$（作为集合相等）。同理，若 $K\trianglelefteq G$，则对任意 $h\in H$ 有

$$hKh^{-1}=K\quad\Longrightarrow\quad hK=Kh, \tag{6.62}$$

于是同样得到 $HK=KH$。

接着证明 HK 是子群。我们用两步验证闭包与逆元存在。

取 $x_1=h_1k_1\in HK$、$x_2=h_2k_2\in HK$。由 $H\trianglelefteq G$，可将 k_1h_2 换序：

$$k_1h_2=(k_1h_2k_1^{-1})\,k_1\in Hk_1\quad(k_1h_2k_1^{-1}\in H). \tag{6.63}$$

更具体地，存在 $h_3\in H$ 使得

$$k_1h_2=h_3k_1. \tag{6.64}$$

于是

$$x_1x_2 = (h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1h_3(k_1k_2) \in HK, \tag{6.65}$$

闭包成立。

任取 $x = hk \in HK$（$h \in H, k \in K$）。则

$$x^{-1} = k^{-1}h^{-1}. \tag{6.66}$$

利用 $H \trianglelefteq G$，有 $k^{-1}h^{-1} = (k^{-1}h^{-1}k)k^{-1}$，其中

$$k^{-1}h^{-1}k \in H. \tag{6.67}$$

于是存在逆元

$$x^{-1} \in HK. \tag{6.68}$$

综上，HK 对乘法封闭且对取逆封闭，所以 HK 是 G 的子群，并且有集合相等

$$HK = KH. \tag{6.69}$$

推论 6.1

若 $H \trianglelefteq G$ 或 $K \trianglelefteq G$，则

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}, \tag{6.70}$$

且此时 HK 本身为子群。

♡

定义 6.13 (群同态)

设 $(G, \cdot)$ 与 $(G', *)$ 为两个群。若存在映射

$$\varphi : G \to G' \tag{6.71}$$

使得对任意 $a, b \in G$，恒有

$$\varphi(a \cdot b) = \varphi(a)\varphi(b), \tag{6.72}$$

则称 φ 为从 G 到 G' 的群同态（**group homomorphism**）。

♣

定义 6.14 (群同构)

若群同态的映射还是双射，则称 φ 为群同构（**group isomorphism**），并记作

$$G \cong G' \tag{6.73}$$

♣

定义 6.15 (像集（Image）)

设 $\varphi : G \to G'$ 是两个群之间的同态映射。定义 φ 的像集为：

$$\mathrm{Im}(\varphi) = \{\, \varphi(g) \mid g \in G \,\} \subseteq G' \tag{6.74}$$

它表示 G' 中所有可以由 G 中元素经 φ 映射得到的元素集合。

♣

定义 6.16 (核（Kernel）)

设 $\varphi : G \to G'$ 是群同态映射。定义 φ 的核为：

$$\ker(\varphi) = \{\, g \in G \mid \varphi(g) = e_{G'} \,\} \tag{6.75}$$

其中 $e_{G'}$ 为 G' 的单位元。

♣

我们指出，像集与核都是子群。核甚至是正规子群。

命题 6.9

对于 h_1, h_2，有充要关系：

$$h_1, h_2 \in \mathrm{Im}(\varphi) \leftrightarrow h_1 h_2^{-1} \in \mathrm{Im}(\varphi) \tag{6.76}$$

♠

先证明像集是子群。

证明 **(1)** 非空. 因为 G 是群，存在单位元 e_G。同态保持运算，故

$$\varphi(e_G) = e_{G'} \tag{6.77}$$

因此 $e_{G'} \in \mathrm{Im}(\varphi)$，像集非空。

(2) 乘法封闭性. 任取 $a', b' \in \mathrm{Im}(\varphi)$，则存在 $a, b \in G$ 使得

$$a' = \varphi(a), \quad b' = \varphi(b) \tag{6.78}$$

于是

$$a'b' = \varphi(a)\varphi(b) = \varphi(ab) \tag{6.79}$$

而 $ab \in G$，故 $\varphi(ab) \in \mathrm{Im}(\varphi)$。因此乘法封闭。

(3) 逆元封闭性. 任取 $a' \in \mathrm{Im}(\varphi)$，存在 $a \in G$ 使 $a' = \varphi(a)$。由同态性质：

$$\varphi(a^{-1}) = \varphi(a)^{-1} = (a')^{-1} \tag{6.80}$$

因为 $a^{-1} \in G$，故 $(a')^{-1} \in \mathrm{Im}(\varphi)$。于是像集对取逆封闭。

$\mathrm{Im}(\varphi)$ 非空、对群运算与取逆均封闭，因此它是 G' 的一个子群。

再来证明核是正规子群。

证明 先证明 $\ker(\varphi)$ 是子群. **(i)** 非空：由于 $\varphi(e_G) = e_{G'}$，故 $e_G \in \ker(\varphi)$。

(ii) 闭包：任取 $a, b \in \ker(\varphi)$，则

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = e_{G'} e_{G'}^{-1} = e_{G'} \tag{6.81}$$

故 $ab^{-1} \in \ker(\varphi)$，从而 $\ker(\varphi)$ 是子群。

(2) 共轭封闭性. 任取 $x \in \ker(\varphi)$ 与 $g \in G$，计算：

$$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(g) e_{G'} \varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e_{G'} \tag{6.82}$$

因此 $gxg^{-1} \in \ker(\varphi)$，即

$$g \ker(\varphi) g^{-1} \subseteq \ker(\varphi) \tag{6.83}$$

由对称性，反向包含也成立，于是

$$g \ker(\varphi) g^{-1} = \ker(\varphi), \quad \forall g \in G \tag{6.84}$$

因此 $\ker(\varphi)$ 在 G 中对共轭不变，故为 G 的正规子群：

$$\ker(\varphi) \trianglelefteq G \tag{6.85}$$

定理 6.3 (第一群同构定理)

对于群 G, H，若二者之间存在群同态，则 G 对核的商群与像群之间存在同构。

♡

$$\begin{array}{ccc} G & \xrightarrow{\phi} & H \\ {\scriptstyle\eta}\downarrow & & \uparrow{\scriptstyle\tau} \\ G/\ker\phi & \underset{\psi^{-1}}{\overset{\psi}{\rightleftarrows}} & \mathrm{Im}\phi \end{array}$$

证明 定义映射

$$\psi : G/\ker\phi \longrightarrow \operatorname{Im}\phi, \qquad \psi(g\,\ker\phi) := \phi(g) \tag{6.86}$$

首先验证良定义：若 $g_1\ker\phi = g_2\ker\phi$，则 $g_2^{-1}g_1 \in \ker\phi$，于是

$$\phi(g_1) = \phi(g_2)\,\phi(g_2^{-1}g_1) = \phi(g_2)\,e_H = \phi(g_2) \tag{6.87}$$

故 ψ 良定义。

验证同态性：对任意 $g_1, g_2 \in G$，

$$\psi\big((g_1\ker\phi)(g_2\ker\phi)\big) = \psi(g_1g_2\ker\phi) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \psi(g_1\ker\phi)\,\psi(g_2\ker\phi) \tag{6.88}$$

证明满射到 $\operatorname{Im}\phi$ 显然：任取 $y \in \operatorname{Im}\phi$，存在 $g \in G$ 使 $y = \phi(g) = \psi(g\ker\phi)$。

证明单射：设 $\psi(g\ker\phi) = e_H$，则

$$\phi(g) = e_H \quad\Longrightarrow\quad g \in \ker\phi \quad\Longrightarrow\quad g\ker\phi = \ker\phi \tag{6.89}$$

即 $G/\ker\phi$ 的单位元。故 $\ker\psi = \{\ker\phi\}$，同态为单射。

综上，ψ 是从 $G/\ker\phi$ 到 $\operatorname{Im}\phi$ 的双射同态，即同构。最后，对任意 $g \in G$，

$$(\tau\circ\psi\circ\eta)(g) = \tau\big(\psi(g\ker\phi)\big) = \tau\big(\phi(g)\big) = \phi(g) \tag{6.90}$$

因而图表可换。若有另一个同构 $\psi' : G/\ker\phi \to \operatorname{Im}\phi$ 满足同一可换条件，则对每个 g

$$\psi'(g\ker\phi) = \phi(g) = \psi(g\ker\phi) \tag{6.91}$$

故 $\psi' = \psi$，唯一性成立。

定理 6.4 (第二群同构定理)

设 G 为群，$H \le G$，$K \trianglelefteq G$。则

$$HK \le G, \qquad K \trianglelefteq HK, \qquad H\cap K \trianglelefteq H \tag{6.92}$$

且存在群同构

$$\theta : H/(H\cap K) \xrightarrow{\cong} HK/K, \qquad \theta(h(H\cap K)) = hK. \tag{6.93}$$

♡

证明 首先证明 HK 为子群。

- 非空性：由于 H 和 K 是子群，$e_G \in H$ 且 $e_G \in K$，故

$$e_G = e_Ge_G \in HK. \tag{6.94}$$

- 乘法封闭性：任取 $h_1k_1, h_2k_2 \in HK$（其中 $h_1, h_2 \in H$，$k_1, k_2 \in K$）。由于 $K \trianglelefteq G$，有

$$h_2^{-1}k_1h_2 \in K, \tag{6.95}$$

即存在 $k' \in K$ 使得 $h_2^{-1}k_1h_2 = k'$，从而

$$k_1h_2 = h_2k'. \tag{6.96}$$

于是

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(h_2k')k_2 = (h_1h_2)(k'k_2) \in HK. \tag{6.97}$$

- 逆元封闭性：任取 $hk \in HK$（其中 $h \in H$，$k \in K$）。其逆元为

$$(hk)^{-1} = k^{-1}h^{-1}. \tag{6.98}$$

由于 $K \trianglelefteq G$，有

$$hk^{-1}h^{-1} \in K, \tag{6.99}$$

即存在 $k'' \in K$ 使得 $hk^{-1}h^{-1} = k''$，从而

$$k^{-1}h^{-1} = h^{-1}k''. \tag{6.100}$$

因此

$$(hk)^{-1} = h^{-1}k'' \in HK, \tag{6.101}$$

因为 $h^{-1} \in H$ 且 $k'' \in K$。

故 HK 是 G 的子群。

其次证明 $K \trianglelefteq HK$。由于 $K \trianglelefteq G$，且 $HK \subseteq G$，对任意 $x \in HK$ 和 $k \in K$，有

$$xkx^{-1} \in K, \tag{6.102}$$

故 $K \trianglelefteq HK$。

再证明 $H \cap K \trianglelefteq H$。任取 $h \in H$ 和 $k \in H \cap K$。由于 $K \trianglelefteq G$，有

$$hkh^{-1} \in K, \tag{6.103}$$

又因 H 是子群，

$$hkh^{-1} \in H. \tag{6.104}$$

故

$$hkh^{-1} \in H \cap K, \tag{6.105}$$

所以 $H \cap K \trianglelefteq H$。

定义映射

$$\phi : H \longrightarrow HK/K, \qquad \phi(h) = hK. \tag{6.106}$$

此映射良定义，因为 $h \in H$ 蕴含 $hK \in HK/K$。它是同态，因为对任意 $h_1, h_2 \in H$，

$$\phi(h_1h_2) = (h_1h_2)K = h_1K \cdot h_2K = \phi(h_1)\phi(h_2). \tag{6.107}$$

计算核：

$$\ker\phi = \{h \in H \mid hK = K\} = \{h \in H \mid h \in K\} = H \cap K. \tag{6.108}$$

计算像：

$$\operatorname{Im}\phi = \{hK \mid h \in H\} = HK/K, \tag{6.109}$$

因为 HK 中任意元素可写为 hk $(h \in H, k \in K)$，且

$$hkK = hK. \tag{6.110}$$

由第一同构定理，有

$$H/\ker\phi \cong \operatorname{Im}\phi, \tag{6.111}$$

即

$$H/(H \cap K) \cong HK/K. \tag{6.112}$$

令 θ 为 ϕ 诱导的同构，即

$$\theta\big(h(H \cap K)\big) = \phi(h) = hK, \tag{6.113}$$

这就完成了证明。

定理 6.5 (第三群同构定理)

设 G 为群，$N \trianglelefteq G$，$K \trianglelefteq G$ 且 $N \leq K$。则

$$K/N \trianglelefteq G/N \tag{6.114}$$

且商群同构

$$(G/N)\big/(K/N) \;\cong\; G/K \tag{6.115}$$

♡

证明 先证 $K/N \trianglelefteq G/N$。对任意 $gN \in G/N$ 与 $kN \in K/N$，

$$(gN)(kN)(gN)^{-1} = gkg^{-1}N \in K/N \tag{6.116}$$

因为 $K \trianglelefteq G$ 蕴含 $gkg^{-1} \in K$。故 K/N 为 G/N 的正规子群。

定义满同态

$$\pi : G/N \longrightarrow G/K, \qquad \pi(gN) = gK \tag{6.117}$$

良定义性：若 $g_1N = g_2N$，则 $g_2^{-1}g_1 \in N \leq K$，从而

$$g_1K = g_2(g_2^{-1}g_1)K = g_2K \tag{6.118}$$

同态性直接由乘法相容得到。像显然为 G/K，故 π 满射。

计算核：

$$\ker\pi = \{\, gN \in G/N :\ gK = K \,\} = \{\, gN :\ g \in K \,\} = K/N \tag{6.119}$$

由第一同构定理，

$$(G/N)\big/\ker\pi \ \cong\ \mathrm{Im}\,\pi = G/K \tag{6.120}$$

代入 $\ker\pi = K/N$ 即得

$$(G/N)\big/\,(K/N) \ \cong\ G/K \tag{6.121}$$

定理 6.6 (第四群同构定理)

设 G 为群，$N \trianglelefteq G$。则存在以下双射对应：

$$\Big\{ H \mid N \leq H \leq G \Big\} \ \leftrightarrow\ \Big\{ \widetilde{H} \mid \widetilde{H} \leq G/N \Big\}, \qquad H \ \mapsto\ H/N \tag{6.122}$$

此对应满足：

$$H_1 \subseteq H_2 \ \Leftrightarrow\ H_1/N \subseteq H_2/N \tag{6.123}$$

$$(H_1H_2)/N = (H_1/N)(H_2/N), \qquad (H_1 \cap H_2)/N = (H_1/N) \cap (H_2/N) \tag{6.124}$$

且正规性被保持与反映：

$$H \trianglelefteq G \ \Leftrightarrow\ H/N \trianglelefteq G/N \tag{6.125}$$

并且在 $H \trianglelefteq G$ 时有商群同构：

$$(G/N)\big/(H/N) \ \cong\ G/H \tag{6.126}$$

♡

证明 定义映射

$$\Phi : \{H \mid N \leq H \leq G\} \ \to\ \{\, \widetilde{H} \leq G/N \,\}, \qquad \Phi(H) = H/N \tag{6.127}$$

若 $N \leq H$，则 $N \trianglelefteq H$，则 $H/N \leq G/N$，故 Φ 良定义。

若 $\Phi(H_1) = \Phi(H_2)$，即 $H_1N = H_2N$，则 $\forall h_1 \in H_1, \exists h_2 \in H_2, h_1N = h_2N$，即 $h_2^{-1}h_1 \in N \subseteq H_2$，即 $h_1 \in H_2$。可知 $H_1 \subseteq H_2$。反之亦然。所以 $H_1 = H_2$，即 Φ 是单射。

对任意 $\widetilde{H} \leq G/N$，令

$$\Psi(\widetilde{H}) = \{g \mid g \in G \wedge gN \in \widetilde{H}\} \tag{6.128}$$

则易证 $\Psi(\widetilde{H})$ 为 G 的子群，且包含 N。且 $\forall h_1N \in \Phi(\Psi(\widetilde{H})), \exists h_2 \in \Psi(\widetilde{H}), h_1N = h_2N$。由 Ψ 定义可知 $h_1N \in \widetilde{H}$。反过来 $\forall hN \in \widetilde{H}, h \in \Psi(\widetilde{H})$，则 $hN \in \Phi(\Psi(\widetilde{H}))$。即

$$\widetilde{H} = \Phi(\Psi(\widetilde{H})) \tag{6.129}$$

即任意 $\widetilde{H} \in \{\widetilde{H} \leq G \leq N\}$，都存在 $\Psi(\widetilde{H})$ 过 Φ 映射得到他，则 Φ 是个满射。综上 Φ 是双射。

保序性：若 $H_1 \subseteq H_2$，则显然 $H_1/N \subseteq H_2/N$；反之，若 $H_1/N \subseteq H_2/N$，则对任意 $h \in H_1$，有 $hN \in H_1/N \subseteq H_2/N$，故存在 $h_2 \in H_2$ 使 $hN = h_2N$，即 $h_2^{-1}h \in N \subseteq H_2$，所以 $h \in H_2$，从而 $H_1 \subseteq H_2$。

对于交与积：

$$(H_1 \cap H_2)/N = \{\, hN \mid h \in H_1 \cap H_2 \,\} = (H_1/N) \cap (H_2/N) \tag{6.130}$$

$$(H_1H_2)/N = \{\, h_1h_2N \mid h_1 \in H_1, h_2 \in H_2 \,\} = (H_1/N)(H_2/N) \tag{6.131}$$

其中最后一个等式是因为 H_1/N 和 H_2/N 的乘积由形如 $(h_1N)(h_2N) = h_1h_2N$ 的元素组成。

正规性对应：若 $H \trianglelefteq G$，则对任意 $gN \in G/N$ 与 $hN \in H/N$，

$$(gN)(hN)(gN)^{-1} = ghg^{-1}N \in H/N \tag{6.132}$$

故 $H/N \trianglelefteq G/N$。反之，若 $H/N \trianglelefteq G/N$，则对任意 $g \in G$ 与 $h \in H$，

$$ghg^{-1}N = (gN)(hN)(gN)^{-1} \in H/N \tag{6.133}$$

故存在 $h' \in H$ 使 $ghg^{-1}N = h'N$，即 $h'^{-1}ghg^{-1} \in N \subseteq H$，所以 $ghg^{-1} \in H$，从而 $H \trianglelefteq G$。

最后，当 $H \trianglelefteq G$ 时，定义 $\tilde{\pi} : G/N \to G/H$，$\tilde{\pi}(gN) = gH$。此映射良定义：若 $g_1N = g_2N$，则 $g_2^{-1}g_1 \in N \subseteq H$，故 $g_1H = g_2H$。它是同态且满射。核为

$$\ker\tilde{\pi} = \{\, gN \in G/N \mid gH = H \,\} = \{\, gN \mid g \in H \,\} = H/N \tag{6.134}$$

由第一同构定理，

$$(G/N)\big/(H/N) \;\cong\; G/H \tag{6.135}$$

定义 6.17 (阶 (Order))

一个群的阶等于其大小。 ♣

例题 6.4 严格上三角矩阵 $N_n(\mathbb{F})$ 是上三角矩阵 $B_n(\mathbb{F})$ 的正规子群，而它们都是线性群 $GL_n(\mathbb{F})$ 的子群。存在 $B_n \mapsto (\mathbb{F}^*)^n$ 的映射 ϕ，其中 $(\mathbb{F}^*)^n$ 是数域 $\mathbb{F}$ 上的乘法群。我们有：

$$B_n/N_n \cong (\mathbb{F}^*)^n \tag{6.136}$$

例题 6.5 考虑多项式环上的元素 $\mathbb{F}[x]$，其中 a_0 是其常数项系数。定义映射：

$$\phi : \mathbb{Z}[x] \to \mathbb{Z}_p \quad = \quad (a_0, a_1, \cdots) \mapsto a_0 \tag{6.137}$$

则这可说明：

$$\mathbb{Z}_p \cong \mathbb{Z}[x]/\{f(x) : p \mid a_0\} \tag{6.138}$$

定义 6.18 (单群（Simple Group）)

若群 G 为非平凡群（即 $G \neq \{e\}$），并且 G 不存在除 $\{e\}$ 与 G 自身以外的非平凡正规子群，则称 G 为一个单群（simple group）。 ♣

注

- 单群在群论中起到基本构件的作用，类似于整数分解中的质数。
- 所有有限阿贝尔单群都同构于某个素数阶循环群 $\mathbb{Z}_p$。
- 非阿贝尔单群的最小例子是交替群 A_5。

定理 6.7 (有限单群分类定理 *（Classification of Finite Simple Groups）)

每一个有限单群都属于以下四类之一：

1. 循环群（**Cyclic Groups**）：

$$G \cong \mathbb{Z}_p, \quad p \text{ 为素数}. \tag{6.139}$$

这是所有有限阿贝尔单群。

2. 交替群（**Alternating Groups**）：
$$G \cong A_n, \quad n \geq 5, \tag{6.140}$$
其中 A_n 表示 n 个元素的偶置换所成的群。
3. 李型群（**Groups of Lie Type**）：这是一大类有限单群，源于有限域上的连通单李型代数群的群论结构，包括：
$$\text{经典型：} \quad A_n(q),\ B_n(q),\ C_n(q),\ D_n(q); \tag{6.141}$$
$$\text{扭曲型：} \quad {}^2A_n(q),\ {}^2D_n(q),\ {}^3D_4(q),\ {}^2E_6(q),\ {}^2F_4(q),\ {}^2G_2(q); \tag{6.142}$$
$$\text{例外型：} \quad E_6(q),\ E_7(q),\ E_8(q),\ F_4(q),\ G_2(q). \tag{6.143}$$
4. **26** 个散在群（**Sporadic Groups**）：这些不属于任何连续族的“例外”有限单群，共 26 个，包括：
$$\text{Mathieu 群：} \quad M_{11},\ M_{12},\ M_{22},\ M_{23},\ M_{24}; \tag{6.144}$$
$$\text{Janko 群：} \quad J_1,\ J_2,\ J_3,\ J_4; \tag{6.145}$$
$$\text{Conway 群：} \quad Co_1,\ Co_2,\ Co_3; \tag{6.146}$$
$$\text{Fischer 群：} \quad Fi_{22},\ Fi_{23},\ Fi'_{24}; \tag{6.147}$$
$$\text{其他：} \quad HS,\ McL,\ He,\ Ru,\ Suz,\ O'N,\ HN,\ Ly,\ Th,\ B,\ M. \tag{6.148}$$
♡

该分类定理的完整证明耗时超过半个世纪（约 1950s–2004）。

定理 6.8 (中国剩余定理（Chinese Remainder Theorem）)

设 $m_1, m_2, \ldots, m_n$ 为两两互素的正整数，记
$$M = m_1 m_2 \cdots m_n. \tag{6.149}$$
对任意整数 $a_1, a_2, \ldots, a_n$，同余方程组
$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases} \tag{6.150}$$
有解，且在模 M 意义下唯一。

更具体地，设
$$M_i = \frac{M}{m_i}, \qquad M_i y_i \equiv 1 \pmod{m_i}, \tag{6.151}$$
则方程组的通解为
$$x \equiv \sum_{i=1}^{n} a_i M_i y_i \pmod{M}. \tag{6.152}$$
♡

中国剩余定理的代数形式表述为：
$$\mathbb{Z}/M\mathbb{Z} \ \cong\ \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}, \tag{6.153}$$
这是一个群同构，同时是个环同构，保留加法与乘法结构。

定义 6.19 (有限生成阿贝尔群（Finitely Generated Abelian Group）)

设 A 是一个阿贝尔群。若存在有限个元素 $a_1, a_2, \ldots, a_n \in A$，使得 A 中的任意元素都可以表示为这些生成元的整数线性组合：

$$\forall a \in A, \quad \exists k_1, \ldots, k_n \in \mathbb{Z}, \quad a = k_1 a_1 + k_2 a_2 + \cdots + k_n a_n \tag{6.154}$$

则称 A 为一个有限生成阿贝尔群（finitely generated abelian group）。

♣

换言之，A 可以写成这些生成元生成的群：

$$A = \langle a_1, a_2, \ldots, a_n \rangle \tag{6.155}$$

注 对于阿贝尔群，我们一般使用 $+$ 符号作为群运算，数乘 kx 表示 x 元素自作用 k 次。用 0 来表示单位元。用 $-a$ 来表示元素 a 的逆元。

定义 6.20 (外直积（External Direct Product）)

设 $G_1, G_2, \ldots, G_n$ 为一族群。它们的外直积（external direct product）定义为集合

$$G_1 \times G_2 \times \cdots \times G_n = \{ (g_1, g_2, \ldots, g_n) \mid g_i \in G_i \}, \tag{6.156}$$

并在其上定义分量乘法运算：

$$(g_1, g_2, \ldots, g_n) \cdot (h_1, h_2, \ldots, h_n) = (g_1 h_1,\ g_2 h_2,\ \ldots,\ g_n h_n). \tag{6.157}$$

在该运算下，$G_1 \times G_2 \times \cdots \times G_n$ 构成一个群，称为 $G_1, G_2, \ldots, G_n$ 的外直积，记作

$$G_1 \times G_2 \times \cdots \times G_n. \tag{6.158}$$

♣

定义 6.21 (内直积（Internal Direct Product）)

设 G 为一个群，$H_1, H_2, \ldots, H_n$ 是 G 的若干子群。若满足以下三个条件：

1. 每个 H_i 在 G 中正规：

$$H_i \trianglelefteq G, \quad \forall i = 1, \ldots, n; \tag{6.159}$$

2. 群 G 由这些子群生成：

$$G = H_1 H_2 \cdots H_n; \tag{6.160}$$

3. 任意不同子群的交集仅含单位元：

$$H_i \cap \left(\prod_{j \neq i} H_j \right) = \{e\}, \quad \forall i. \tag{6.161}$$

则称 G 是 $H_1, H_2, \ldots, H_n$ 的内直积，记作

$$G = H_1 \times H_2 \times \cdots \times H_n. \tag{6.162}$$

♣

定理 6.9 (内直积与外直积的关系)

若 G 是 $H_1, H_2, \ldots, H_n$ 的内直积，则存在自然的群同构

$$\Phi : H_1 \times H_2 \times \cdots \times H_n \to G, \qquad \Phi(h_1, h_2, \ldots, h_n) = h_1 h_2 \cdots h_n, \tag{6.163}$$

且 Φ 为双射。

♡

定理 6.10

若 G 为有限生成阿贝尔群，则 G 本身同构于若干个循环群的直和：

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}, \tag{6.164}$$

其中 $r \geq 0$，$k \geq 0$，且 $\forall i, n_i = p_i^{t_i}$，$p_i$ 为质数。 ♡

证明

设 G 是一个有限生成阿贝尔群，有生成元

$$G = \langle a_1, a_2, \ldots, a_t \rangle. \tag{6.165}$$

假设 G 不能被少于 t 个元素生成。

使用数学归纳法。对 $t = 1$ 的 G，结论显然成立。

归纳假设：$m < t$ 的群 G 结论都成立，当 $m = t$ 时：

定义群同态

$$\varphi : \mathbb{Z}^t \longrightarrow G, \quad \varphi(m_1, m_2, \ldots, m_t) = \sum_{i=1}^{t} m_i a_i. \tag{6.166}$$

设其核为

$$K = \ker \varphi = \{(m_1, \ldots, m_t) \in \mathbb{Z}^t \mid \sum_{i=1}^{t} m_i a_i = 0\}. \tag{6.167}$$

对群 G 的所有的生成元组 $(a_1, \ldots, a_t)$ 对应的所有的核空间内元素 $(c_1, \ldots, c_t)$。我们取一个“模长”最小的非零解 $(c_1, c_2, \ldots, c_t)$，及其对应的生成元 $(a_1, a_2, \ldots, a_t)$。定义模长为 $\sum_{i=1}^{t} |c_i|$。

第一种情况，若核空间里只有全零解，则无法取出这样的一个 $\vec{c}$。这种情况说明 $\ker \phi = \{e\}$，ϕ 是单射。由生成元的定义，则 ϕ 也是满射。则存在一个从 $\mathbb{Z}^t$ 到 G 的双射，即 G 同构于 $\mathbb{Z}^t$，归纳假设成立。

第二种情况，我们能取出这样的一个 $\vec{c}$。根据定义有 $\sum_{i=1}^{t} c_i a_i = 0$。我们证明这个 $\vec{c}$ 至多有一个非零分量。

假设存在两个位置非零，不妨设 $|c_1| \geq |c_2| > 0$。则有：

$$c_1 a_1 + c_2 a_2 + \sum_{i=3}^{t} c_i a_i = 0 \tag{6.168}$$

变形可得：

$$(c_1 - c_2) a_1 + c_2 (a_2 + a_1) + \sum_{i=3}^{t} c_i a_i = 0 \tag{6.169}$$

或有

$$(c_1 + c_2) a_1 + c_2 (a_2 - a_1) + \sum_{i=3}^{t} c_i a_i = 0 \tag{6.170}$$

易知 $(a_1, a_2 + a_1, \ldots, a_t)$ 和 $(a_1, a_2 - a_1, \ldots, a_t)$ 都是生成元组。且 $(c_1 - c_2, c_2, \ldots, c_t)$ 和 $(c_1 + c_2, c_2, \ldots, c_t)$ 的模长必有一个比 $(c_1, c_2, \ldots, c_t)$ 小。与 $\vec{c}$ 最小矛盾。

则 $\vec{c}$ 中至多有一个非零分量。不妨假设这个位置的生成元是 a_1，系数是 c_1。则 G 有一个子群同构于 $\mathbb{Z}^{c_1}$。由归纳假设，$\langle a_2, a_3, \ldots, a_t \rangle$ 是 $t-1$ 个生成元的阿贝尔群，则同构于一系列循环群的直积。下证 G 是 $\langle a_1 \rangle$ 和 $\langle a_2, a_3, \ldots, a_t \rangle$ 的内直积。反证法，假设存在一个非单位元 $g \in G$，$g \in \langle a_1 \rangle$ 且 $g \in \langle a_2, a_3, \ldots, a_t \rangle$。则存在一组系数 $(d_1, d_2, \ldots, d_t)$ 满足，

$$g = d_1 a_1 = \sum_{i=2}^{t} d_i a_i \tag{6.171}$$

那么也满足

$$d_1 a_1 - \sum_{i=2}^{t} d_i a_i = 0 \tag{6.172}$$

那么重复上面证明 $\vec{c}$ 最多只有一个非零分量的步骤，对 $(d_1, -d_2, \ldots, -d_t)$ 做辗转相减，可以得到最终 $d = gcd(d_1, d_2, \ldots, d_t)$，且在某个生成元组的唯一一个分量 a' 上，满足 $da' = 0$。则有 $d \leq \min_{i=1}^{t} d_i \leq d_1$。由 g 是 $\langle a_1 \rangle$

中元素且此子群阶为 c_1，则 $d < c_1$ 且 $da' = 0$，为一个模长更小的 kernel 空间元素，与 c_1 最小矛盾。

则可证明 $\langle a_1\rangle$ 和 $\langle a_2, \dots, a_t\rangle$ 交集只有单位元。即 $G = \langle a_1\rangle \oplus \langle a_2, \dots, a_t\rangle$。综合归纳假设，得到 $G \cong \mathbb{Z}^r \oplus \mathbb{Z}_{t_1} \oplus \dots \oplus \mathbb{Z}_{t_k}$。由每个 t_i，由中国剩余定理，都可将其拆成其唯一分解的每个质数幂大小的循环群。

定理 6.11 (内直积与外直积的关系)

若 G 是 $H_1, H_2, \dots, H_n$ 的内直积，则存在自然的群同构

$$\Phi : H_1 \times H_2 \times \cdots \times H_n \longrightarrow G, \qquad \Phi(h_1, h_2, \dots, h_n) = h_1 h_2 \cdots h_n, \tag{6.173}$$

且 Φ 为双射。因此，内直积可以视为外直积在 G 中的实现。 ♡

注[记号] 设 G, H 为群，则我们有以下常用记号与定义：

1. **群同态集 (Hom set)**
$$\mathrm{Hom}(G, H) = \{\, \varphi : G \to H \mid \varphi(ab) = \varphi(a)\varphi(b),\ \forall a, b \in G \,\}. \tag{6.174}$$
2. **群同构集 (Iso set)**
$$\mathrm{Iso}(G, H) = \{\, \varphi \in \mathrm{Hom}(G, H) \mid \varphi \text{ 为双射} \,\}. \tag{6.175}$$
3. **自同态半群 (Endomorphism semigroup)** 当 $G = H$ 时，群到自身的所有同态构成一个半群：
$$\mathrm{End}(G) := \mathrm{Hom}(G, G). \tag{6.176}$$
4. **自同构群 (Automorphism group)** 当 $G = H$ 且映射为双射时，所有自同构构成一个群，记作：
$$\mathrm{Aut}(G) := \mathrm{Iso}(G, G), \tag{6.177}$$
运算为映射复合。
5. **内自同构群 (Inner automorphism group)** 对于任意 $g \in G$，定义映射：
$$\varphi_g : G \to G, \quad \varphi_g(a) = gag^{-1}. \tag{6.178}$$
所有这样的映射构成的集合称为 G 的内自同构群：
$$\mathrm{Inn}(G) = \{\, \varphi_g : a \mapsto gag^{-1} \mid g \in G \,\}. \tag{6.179}$$
容易验证：
$$\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G). \tag{6.180}$$

6.3 群作用 (Group Action)

定义 6.22 (（左）群作用)

群作用 $\star$ 是群 G 与集合 X 到集合 X 的映射：

$$G \times X \to X \tag{6.181}$$

其中，群作用满足：

$$\forall g, h \in G, \quad x \in X, \quad h \star (g \star x) = hg \star x \tag{6.182}$$

♣

例如对称群 $\mathrm{Sym}(\Omega) \times \Omega \to \Omega$，考虑群元 σ, τ 有：

$$\sigma \star x := \sigma(x) \tag{6.183}$$

$$\tau \star (\sigma \star x) = (\tau \cdot \sigma) \star x \tag{6.184}$$

定义群对自己的**左平移** $G \times G \to G$：

$$g \star h = gh \tag{6.185}$$

左平移是群作用是显然的。类似地有右平移：

$$g \star h = hg^{-1} \tag{6.186}$$

证明 我们简单验证一下右平移也是群作用：

$$g_1 \star (g_2 \star h) = hg_2^{-1}g_1^{-1} = h(g_1g_2)^{-1} = g_1g_2 \star h \tag{6.187}$$

注 特别值得注意的是，如果处于直观地把右平移中的取逆去掉，得到的新运算为一个**右群作用**而非左群作用。但我们一般不做考虑。

平移作用有一些比较有趣的性质。由于 $G \times X \to X$ 可以被看作 $G \to (X \to X)$（类似于张量面面观），一个群元可以决定一个 X 到自身的映射。也就是说对于 X 上的一个群作用 G，存在群同态 $\mathrm{Hom}(G, \mathrm{Sym}(X))$。

我们采用记号 $\phi_j \in \mathrm{Sym}(X)$ 代表群元 j 代表的群同构，有：

$$(\phi_j)^{-1} = \phi_{j^{-1}} \tag{6.188}$$

$$\phi_e = \mathrm{id} \tag{6.189}$$

如果上式中的第二条当前仅当对应群元为单位元，那么我们称这个群作用为**忠实的**。

定义 6.23 (忠实的)

一个群作用 G 被称作忠实的，当且仅当：

$$\forall g \neq e, \exists x, \quad g \star x \neq x \tag{6.190}$$

♣

定理 6.12

任何一个群都同构于一个对称群的子群。

♡

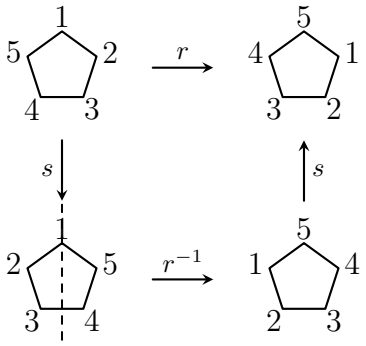
我们最关心的一个群作用是**共轭作用** (Conjugation Action)：$G \times G \to G$。其中，群作用被定义为：

$$g \star h = ghg^{-1} \tag{6.191}$$

即 $\phi_g(h) = ghg^{-1}$。我们指出，ϕ_g 是一个群同构。也就是说，$g \mapsto \phi_g$ 实际上是 $G \to \mathrm{Aut}(G)$ 的同态。

注 对于完备群，即当中心 $C(G) = \{e\}$ 是平凡的且 $\mathrm{Aut}(G) = \mathrm{Inn}(G)$ 时，上述同态升级为同构。

再来举个群作用的例子。考虑二面体群 $D_n := \langle r, s \mid r^n = s^2 = 1, srs = r^{-1} \rangle$。我们可以将其作用于 $[n] := \{1, 2, \cdots, n\}$ 上。其中对于正多边形点群，r 的几何意义可以被解释为顺时针旋转 $2\pi/n$，而 s 为沿任意一条固定对称轴做翻转。从而有：



接下来我们额外引入一些概念。

定义 6.24 (轨道)

轨道 $\mathrm{orbit}(x) := Gx$ 被定义为点集：

$$Gx := \{g \star x \mid g \in G\} \tag{6.192}$$

♣

我们指出：

$$x \in Gx \tag{6.193}$$

这是显然的。且：

$$\forall x, y \quad Gx = Gy \text{ or } Gx \cap Gy = \varnothing \tag{6.194}$$

这也是显然的，只需考虑如果有公共元素，两个轨道内必可通过群变换连接。

我们通常记 X/G 为 X 中所有点在 G 变换下轨迹的集合。

定义 6.25 (稳定子 (Stabilizer))

$\mathrm{Stab}(x)$ 被定义为所有群作用中没有移动 x 的群元构成的集合：

$$\mathrm{Stab}(x) = \{g \mid g \star x = x\} \tag{6.195}$$

♣

定理 6.13

稳定子是原变换群的子群。

♡

证明 考虑 $g, h \in \mathrm{Stab}(x)$，从而有 $\phi_g(x) = \phi_h(x) = \phi_{h^{-1}}(x) = x$，从而 $\phi_{gh^{-1}}(x) = \phi_g \cdot \phi_{h^{-1}}(x) = x$，也即 $gh^{-1} \in G$。

定理 6.14

如果两个元素之间差一个群作元素用 g，那么它们的稳定子互为 g 导出的共轭：

$$y = gx \quad \Rightarrow \quad \mathrm{Stab}(y) = g\mathrm{Stab}(x)g^{-1} \tag{6.196}$$

♡

证明 设 $h \in \mathrm{Stab}(x)$，则：

$$\begin{aligned}&(ghg^{-1}) \star y\\ =&ghx\\ =&gx = y\end{aligned}$$

因此 ghg^{-1} 总属于 y 的稳定子，即 $\mathrm{Stab}(y) \subseteq g\mathrm{Stab}(x)g^{-1}$。反过来的证明是用一样的方法去证明 $\mathrm{Stab}(x) \subseteq g^{-1}\mathrm{Stab}(x)g$。两边共同得到 $\mathrm{Stab}(y) = g\mathrm{Stab}(x)g^{-1}$。

定义 6.26 (共轭类（Conjugation Class）)

设 G 是一个群。对于任意元素 $h \in G$，h 的共轭类是指所有与 h 共轭的元素构成的集合，即：

$$C(h) = \{ghg^{-1} \mid g \in G\} \tag{6.197}$$

♣

换句话说，h 的共轭类就是 h 在群 G 的共轭作用下的轨道。

例如，对于相抵变换 $(\mathrm{GL} \times \mathrm{GL}) \times \mathrm{Mat} \mapsto \mathrm{Mat}$，$M \to AMB^{-1}$，其轨道即所有秩相同的矩阵，因为任意两个秩相同的矩阵可以被可逆矩阵相互相抵变换。

再举例，对于基变换（相似变换）$\mathrm{GL} \times \mathrm{Mat} \to \mathrm{Mat}$，$M \mapsto AMA^{-1}$，其共轭类是所有相似的矩阵。

再举例，在对称群上的共轭作用 $\mathrm{Sym}(n) \times \mathrm{Sym}(n) \to \mathrm{Sym}(n)$，$\tau \mapsto \sigma\tau\sigma^{-1}$。

定义一个置换的形状是这个置换形成的轮换大小可重集合。下证共轭的置换的形状相同。

任意 τ, σ，则 $\sigma\tau\sigma^{-1} \star (\sigma(i)) = \sigma\tau \star (i) = \sigma(\tau \star i)$，即将任意 $\sigma(i)$ 映射到 $\sigma(\tau \star i)$。对比 τ 这个置换，将 i 映射到 $\tau \star i$。那么对于任意一个 τ 置换里的轮换 $(a_1, a_2, \cdots, a_k)$ 将会变成 $(\sigma(a_1), \sigma(a_2), \cdots, \sigma(a_k))$。即所有轮换大小都不变，则两个置换形状相同。

共轭的稳定子是：

$$\{g \mid gxg^{-1} = x\} \tag{6.198}$$

即 x 的中心化子 $C(x)$。

定理 6.15

设群 G 作用在集合 X 上，$x \in X$。令 $Gx = \{g \star x \mid g \in G\}$ 为 x 的轨道，$\mathrm{Stab}(x) = \{g \in G \mid g \star x = x\}$ 为稳定化子。则存在双射：

$$\varphi : G/\mathrm{Stab}(x) \to Gx, \quad g\,\mathrm{Stab}(x) \mapsto g \star x \tag{6.199}$$

特别地，当 G 为有限群时，有：

$$|Gx| = [G : \mathrm{Stab}(x)] = \frac{|G|}{|\mathrm{Stab}(x)|} \tag{6.200}$$

♡

证明 我们逐步证明映射 φ 是良定义的双射。

良定义性：设 $g\,\mathrm{Stab}(x) = h\,\mathrm{Stab}(x)$，即存在 $k \in \mathrm{Stab}(x)$ 使得 $h = gk$。则

$$h \star x = (gk) \star x = g \star (k \star x) = g \star x \tag{6.201}$$

故 φ 的定义与代表元选择无关，是良定义的。

单射性：若 $\varphi(g\,\mathrm{Stab}(x)) = \varphi(h\,\mathrm{Stab}(x))$，即 $g \star x = h \star x$，则

$$h^{-1}g \star x = h^{-1} \star (g \star x) = h^{-1} \star (h \star x) = (h^{-1}h) \star x = e \star x = x \tag{6.202}$$

故 $h^{-1}g \in \mathrm{Stab}(x)$，即 $g\,\mathrm{Stab}(x) = h\,\mathrm{Stab}(x)$。

满射性：对任意 $y \in Gx$，存在 $g \in G$ 使得 $y = g \star x$，即 $y = \varphi(g\,\mathrm{Stab}(x))$。

因此 φ 是双射。当 G 有限时，左陪集个数 $[G : \mathrm{Stab}(x)] = |G/\mathrm{Stab}(x)| = |Gx|$，即

$$|Gx| = \frac{|G|}{|\mathrm{Stab}(x)|} \tag{6.203}$$

为了直观，作为例子，我们给出 S_5 的共轭类分类。

表 6.1: S_5 的共轭类分类

循环型	代表元	类大小	稳定子大小	稳定子结构
1^5	(1)	1	120	S_5
$1^3, 2$	$(1\,2)$	$\binom{5}{2} = 10$	12	$S_2 \times S_3$
$1^2, 3$	$(1\,2\,3)$	$2! \cdot \binom{5}{3} = 20$	6	$\mathbb{Z}_3 \times S_2$
$1, 2^2$	$(1\,2)(3\,4)$	$\frac{1}{2!} \cdot \binom{5}{2} \cdot \binom{3}{2} = 15$	8	$\mathbb{Z}_2^2 \times \mathbb{Z}_2$
$1, 4$	$(1\,2\,3\,4)$	$3! \cdot \binom{5}{4} = 30$	4	$\mathbb{Z}_4$
$2, 3$	$(1\,2)(3\,4\,5)$	$\binom{5}{2} \cdot 2! = 20$	6	$S_2 \times \mathbb{Z}_3$
5	$(1\,2\,3\,4\,5)$	$4! = 24$	5	$\mathbb{Z}_5$

由于群可以写成其共轭类的不交并：

$$|G| = \sum_{\text{ConjugationClass}} |Gg| = \sum_{\text{ConjugationClass}} [G : C(g)] \tag{6.204}$$

有些时候，共轭类中只有一个元，即中心中的元素，我们可以将其从上述求和中拆出。同时，取每个大小大于一的共轭类中的一个代表元。有：

$$|G| = |C(G)| + \sum_{c_i \text{ not in center}} [G : C(c_i)] \tag{6.205}$$

这被称作共轭类方程。

定义 6.27 (p-群)

设 G 是有限群，p 为素数。若 G 的阶是 p 的幂，即

$$|G| = p^n, \qquad n \in \mathbb{N}, \tag{6.206}$$

则称 G 为一个 p-群（p-group）。 ♣

命题 6.10

若 G 是有限 p-群，即

$$|G| = p^n, \qquad p \text{ 为素数}, n \in \mathbb{N}, \tag{6.207}$$

则 G 的中心 $C(G)$ 必为非平凡的，即

$$C(G) \neq \{e\}. \tag{6.208}$$

♠

证明 令 G 作用在自身上，由共轭定义：

$$g \cdot x = gxg^{-1}, \qquad \forall g, x \in G. \tag{6.209}$$

该作用的轨道与稳定子满足：

$$|G| = \sum_{x \in \mathcal{R}} [G : C_G(x)], \tag{6.210}$$

其中 $\mathcal{R}$ 是各共轭类代表元集合，$C_G(x)$ 为中心化子。

注意到共轭类方程：

- 对 $x \in C(G)$，有 $C_G(x) = G$，其共轭类大小为 1；
- 对 $x \notin C(G)$，$|C_G(x)| < |G|$，因此 $|C_G(x)|$ 为 p^k 的某个真子幂，故对应的共轭类大小 $|G : C_G(x)|$ 为 p 的倍数。

因此可得

$$|G| = |C(G)| + p \cdot m \tag{6.211}$$

对某个整数 m。由于 $|G| = p^n$，可知 $|C(G)| \equiv 0 \pmod{p}$，即 $|C(G)|$ 是 p 的倍数。

因此 $|C(G)| \geq p > 1$，从而 $C(G)$ 非平凡。

命题 6.11

若有限群 G 的阶为

$$|G| = p^2, \qquad p \text{ 为素数} \tag{6.212}$$

则 G 必为 Abelian。 ♠

证明 由 p-群中心非平凡的命题可知

$$1 < |C(G)| \tag{6.213}$$

故

$$|C(G)| \in \{p, p^2\} \tag{6.214}$$

若

$$|C(G)| = p^2 \tag{6.215}$$

则 $C(G) = G$，显然 G 阿贝尔。

若

$$|C(G)| = p \tag{6.216}$$

则商群

$$|G/C(G)| = \frac{|G|}{|C(G)|} = p \tag{6.217}$$

阶为素数的群必循环，故 $G/C(G)$ 循环。已知若 $G/C(G)$ 循环，则 G Abelian（因为存在 $g \in G$ 使得 $G = \langle g, C(G)\rangle$，

任何元素可写成 $g^i z$，从而两两可交换）。于是 G Abelian。

注 阶为 p^2 的阿贝尔群只有两种同构类型：

$$G \cong \mathbb{Z}_{p^2} \quad \text{或} \quad G \cong \mathbb{Z}_p \times \mathbb{Z}_p \tag{6.218}$$

定义 6.28 (p-子群)

设 G 是有限群，p 为素数。若 $H \leq G$ 且其阶为 p 的幂，即

$$|H| = p^k, \qquad k \in \mathbb{N}, \tag{6.219}$$

则称 H 为 G 的一个 p-子群（p-subgroup）。

♣

定义 6.29 (Sylow p-子群)

设有限群 G，若 $P \leq G$ 且

$$|P| = p^n, \tag{6.220}$$

同时该子群最大，即：

$$p^{n+1} \nmid |G| \tag{6.221}$$

则称 P 为 G 的一个 *Sylow* p-子群（Sylow p-subgroup）。

♣

G 中所有 Sylow p-子群的集合记作 $\mathrm{Syl}_p(G)$。

定理 6.16 (Sylow I (存在性))

设有限群 G 的阶为

$$|G| = p^r m, \qquad \gcd(p, m) = 1. \tag{6.222}$$

则 G 至少存在一个阶为 p^r 的子群，即存在 Sylow p-子群。

♡

证明 我们对 $|G|$ 归纳。

当 $|G| = p$ 时，结论显然成立（群自身即 Sylow p-子群）。

设命题对一切阶小于 $|G|$ 的群成立。对 G：

(1) 若 $p \nmid |C(G)|$：考虑共轭类方程，由总和是 p 的倍数，第一项不是 p 倍数，则一定存在某个共轭类使得其代表元 c_i 满足

$$p \nmid [G : C_G(c_i)] = \frac{p^r m}{|C_G(c_i)|} \tag{6.223}$$

则 G 存在一个子群使得 $p^r \mid |C_G(c_i)|$，且 $p^{r+1} \nmid |C_G(c_i)|$。由归纳假设，阶更小的群都存在 Sylow p-子群，则 $C_G(c_i)$ 存在一个子群大小为 p^r，这个子群自然也是 G 的子群，归纳假设成立。

(2) 若 $p \mid |C(G)|$：

由群的中心定义，$C(G)$ 是阿贝尔群。由阿贝尔群分解定理，$C(G)$ 一定存在一个阶为 p^t 的循环子群，则 $C(G)$ 一定存在一个阶为 p 的子群 $\langle g \rangle$。且 $\langle g \rangle \trianglelefteq G$。

由归纳假设，$G/\langle g \rangle$ 存在一个 p-Sylow 子群 $S/\langle g \rangle$，大小为 p^{r-1}。由第四同态定理，$G/\langle g \rangle$ 的这个子群 K 对应一个包含 $\langle g \rangle$ 的 G 的子群 S 且满足 $K = S/\langle g \rangle$。

那么由拉格朗日定理，可得

$$|S| = |K| \cdot |\langle g \rangle| = p^r \tag{6.224}$$

归纳假设成立。

定理 6.17 (Sylow II)

设 G 为有限群，$P \le G$ 为 Sylow p-子群，$Q \le G$ 为任意 p-子群。则存在 $g \in G$ 使

$$Q \le gPg^{-1}. \tag{6.225}$$

♡

证明 令 Q 作用在左陪集的集合 G/P 上（注意：G/P 这里指所有左陪集的集合，不一定是商群）：

$$Q \times G/P \longrightarrow G/P, \qquad q \cdot (gP) := (qg)P. \tag{6.226}$$

由轨道–稳定子定理，有

$$|G/P| \;=\; \sum_i |\mathrm{Orbit}_i|, \tag{6.227}$$

其中

$$|\mathrm{Orbit}(gP)| \;=\; [\,Q : \mathrm{Stab}_Q(gP)\,], \qquad \mathrm{Stab}_Q(gP) := \{\, q \in Q \mid qgP = gP \,\}. \tag{6.228}$$

注意到

$$|G/P| \;=\; [\,G : P\,] \tag{6.229}$$

与 p 互素（因为 P 是 Sylow p-子群），故 $|G/P|$ 不是 p 的倍数。因此在各个轨道大小的和中，必存在某个轨道大小不是 p 的倍数。于是存在 $g \in G$ 使

$$p \nmid |\mathrm{Orbit}(gP)| \;=\; [\,Q : \mathrm{Stab}_Q(gP)\,]. \tag{6.230}$$

然而 Q 是 p-群，故 $[\,Q : \mathrm{Stab}_Q(gP)\,]$ 只能是 p 的幂。与“不是 p 的倍数”合并，唯一可能是

$$[\,Q : \mathrm{Stab}_Q(gP)\,] \;=\; 1, \qquad \text{即} \quad Q \;=\; \mathrm{Stab}_Q(gP). \tag{6.231}$$

于是对一切 $q \in Q$ 有

$$qgP \;=\; gP \quad\Longrightarrow\quad g^{-1}qg \in P \quad\Longrightarrow\quad q \in gPg^{-1}. \tag{6.232}$$

故 $Q \le gPg^{-1}$，证毕。

推论 6.2

1. 任意两个 p-Sylow 子群都共轭；
2. 任意 p-子群都被某个 p-Sylow 子群包含；
3. p-Sylow 子群唯一 $\Longleftrightarrow$ 该 p-Sylow 子群正规于 G。

♡

命题 6.12

设 P 是 G 的一个 Sylow p-子群，则 P 是 $N_G(P)$ 的唯一 Sylow p-子群。

♠

证明 显然 $P \le N_G(P)$，因此 P 是 $N_G(P)$ 的一个 p-子群。根据正规化子的定义，

$$N_G(P) := \{\, g \in G \mid gPg^{-1} = P \,\}. \tag{6.233}$$

由此知 $P \trianglelefteq N_G(P)$。因为 P 的阶已经是 p 在 $|G|$ 中的最高次幂，所以 $N_G(P)$ 不可能再有比 P 更大的 p-子群。故 P 是 $N_G(P)$ 的唯一 Sylow p-子群。

定理 6.18 (Sylow III)

记 $n_p = |\mathrm{Syl}_p(G)|$。则：

$$n_p = [G : N_G(P)], \qquad n_p \equiv 1 \pmod{p}, \qquad n_p \mid m. \tag{6.234}$$

若 $n_p = 1$，则该唯一 Sylow p-子群正规。

♡

证明 [证明] 由前述共轭作用，轨道大小为

$$n_p = [G : N_G(P)] = \frac{|G|}{|N_G(P)|}. \tag{6.235}$$

由于 $P \leq N_G(P)$，设 $|N_G(P)| = p^n k$，其中 $k \mid m$。则：

$$n_p = \frac{p^n m}{p^n k} = \frac{m}{k}, \tag{6.236}$$

从而 $n_p \mid m$。

接下来证明 $n_p \equiv 1 \pmod{p}$。固定一个 p-Sylow 子群 P。考虑 P 对 $\mathrm{Syl}_p(G)$ 的共轭作用：

$$P \times \mathrm{Syl}_p(G) \longrightarrow \mathrm{Syl}_p(G), \qquad g * P_i := gP_ig^{-1}. \tag{6.237}$$

设每个轨道选取一个代表元 P_i，由轨道–稳定子定理：

$$n_p = |\mathrm{Syl}_p(G)| = \sum_i |\mathrm{Orbit}_i| = \sum_i [\, P : \mathrm{Stab}_P(P_i) \,]. \tag{6.238}$$

对每个轨道代表元 P_i 分情况讨论：

- 若 $\mathrm{Stab}_P(P_i) < P$，则 $[P : \mathrm{Stab}_P(P_i)]$ 为 p 的倍数；
- 若 $\mathrm{Stab}_P(P_i) = P$，则 $[P : \mathrm{Stab}_P(P_i)] = 1$。且易知 $P_i \subseteq \mathrm{Stab}_P(P_i) = P$，由 $|P_i| = |P|$，则 $P_i = P$。因此恰有一个轨道大小为 1（对应 $P_i = P$），其余轨道大小均为 p 的倍数。故

$$n_p = \sum_i |\mathrm{Orbit}_i| \equiv 1 \pmod{p}. \tag{6.239}$$

第七章 环 (Ring)

7.1 基本定义

定义 7.1

一个环是一个有序三元组 $(R,+,\cdot)$，其中 R 是一个集合，$+$ 和 $\cdot$ 是 R 上的两个二元运算，满足以下公理：

1. $(R,+)$ 构成一个阿贝尔群：
   (a). 加法结合律：$\forall a,b,c\in R,\ (a+b)+c=a+(b+c)$
   (b). 加法单位元（零元）：$\exists 0\in R,\ \forall a\in R,\ a+0=0+a=a$
   (c). 加法逆元（负元）：$\forall a\in R,\ \exists -a\in R,\ a+(-a)=(-a)+a=0$
   (d). 加法交换律：$\forall a,b\in R,\ a+b=b+a$
2. $(R,\cdot)$ 构成一个半群：
   (e). 乘法结合律：$\forall a,b,c\in R,\ (a\cdot b)\cdot c=a\cdot(b\cdot c)$
3. 分配律（乘法对加法的分配律）：
   (f). 左分配律：$\forall a,b,c\in R,\ a\cdot(b+c)=(a\cdot b)+(a\cdot c)$
   (g). 右分配律：$\forall a,b,c\in R,\ (a+b)\cdot c=(a\cdot c)+(b\cdot c)$

如果环 R 包含乘法单位元，即 $\exists 1\in R, 1\neq 0,\ \forall a\in R,\ a\cdot 1=1\cdot a=a$，则称 R 为含幺环。

以上是环基本定义，我们大多数情况默认环是含幺环。接下来我们需要研究满足某些性质的环，有些新的定义。

定义 7.2

如果环 R 满足乘法交换律，即 $\forall a,b\in R,\ a\cdot b=b\cdot a$，则称 R 为交换环（**Commutative Ring**）。

如果环 R 无零因子，其中零因子定义为 z 使得 $z\neq 0, \exists a\neq 0, za=0\vee az=0$，则称 R 为整环 **(Integral Ring)**。

如果一个环同时满足以上两个条件称为整区 **(Integral Domain)**。

如果环 R，$\forall a\neq 0, \exists a^{-1}\in R, a\cdot a^{-1}=a^{-1}\cdot a=1$，则称为除环 **(Division Ring)**。

容易发现，若 R 是除环，则 R 一定是整环。由 $ab=0$ 可知 $a=0\vee b=0$。

如果环 R 同时是除环和整区，则称 R 为域 **(Field)**。

一些具体的例子：

域：$\mathbb{Q},\mathbb{R},\mathbb{C}$。

环：$\mathbb{Z},\mathbb{Z}_n$。

任意阿贝尔群 M 上的自同态集 $\mathrm{End}(M)$ 作为元素，加法定义为两个函数点加，乘法定义为映射复合，构成一个环。

任意环 R，由 R 中元素组成的 n 阶方阵 $M_n(R)$ 在矩阵加法和矩阵乘法下构成环。

定义 7.3

四元数 **(Quaternion)** 由生成元

$$\{1,-1,i,-i,j,-j,ij,-ij\} \tag{7.1}$$

生成。满足 $(-1)\cdot a=-a$，$ab=-ba$，$i^2=j^2=(ij)^2=-1$。可以对某个环 R 定义四元数环

$$\{x+yi+zj+wij \mid x,y,z,w\in R\} \tag{7.2}$$

定义环的直积 $R=R_1\times R_2\times\cdots\times R_n$ 为 n 元组，第 i 个分量为 R_i 元素。加法和乘法都是按位分别做环上加

法乘法。则 R 也是环。

或者更一般的函数环。定义从集合 X 到环 R 的函数 $f : X \to R$，定义加法为 $(f_1 + f_2)(x) = f_1(x) + f_2(x)$，乘法为 $(f_1 f_2)(x) = f_1(x) f_2(x)$。则此函数集合和加法乘法也构成环。

定义 7.4

给定一个交换环 R，定义 $R[x]$ 表示系数为 R 元素，变元为 x 的所有有限次多项式，称为多项式环 **(polynomial ring)**。

$$R[x] = \{\sum_{i=0}^{d} a_i x^i \mid d \in \mathbb{N}, a_i \in R\} \tag{7.3}$$

更一般的，可以定义多变元多项式环

$$R[x, y] = \{\sum_{i=0}^{d_1}\sum_{j=0}^{d_2} a_{i,j} x^i y^j \mid d_1, d_2 \in \mathbb{N}, a_{i,j} \in R\} \tag{7.4}$$

把 x_i 看成是一个单独的形式符号，按照多项式的加法乘法定义，可证明多项式环构成环。

♣

定义 7.5

更一般的，可以在一个半群 G 和交换环 R 上定义群环 **(group ring)**。

$$R[G] = \{\sum_{g \in G} a_g g \mid a_g \in R\} \tag{7.5}$$

也可以看作是一个从 G 到 R 的映射集合。

运算定义为

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g \tag{7.6}$$

$$(\sum_{g \in G} a_g g)(\sum_{g \in G} b_g g) = \sum_{k \in G} (\sum_{gh=k} a_g b_h) k \tag{7.7}$$

♣

若用 x_i 来代替 $\mathbb{Z}$ 中的 i，则容易证明 $R[x] \cong R[\mathbb{Z}]$。

7.2 环同态

接下来试图定义环同态。

定义 7.6

一个从环 R 到环 S 的映射 ϕ 被称为环同态映射若

- $\phi(a + b) = \phi(a) + \phi(b)$
- $\phi(ab) = \phi(a)\phi(b)$
- $\phi(1_R) = 1_S$

定义像为 $Im(\phi) = \phi(R)$。

定义核为 $Ker(\phi) = \phi^{-1}(0_S)$

♣

分析 $Ker(\phi)$ 的性质，我们给出理想的定义。

定义 7.7

环 R 的一个子集 I 称为 R 的理想 **(Ideal)**，若

- $(I, +) \leq (R, +)$

- $\forall a \in I, \forall x \in R$，满足 $ax, xa \in I$

可以看出任意 R 到某个环的环同态 ϕ,$Ker(\phi)$ 是 R 的理想。
具体例子：考虑从 $\mathbb{Z}$ 到 $\mathbb{Z}_n$ 的环同态映射 ϕ，定义 $\phi(x) = x \mod n$。容易验证 ϕ 是一个环同态。
可以看出 $Ker(\phi) = n\mathbb{Z}$，是 $\mathbb{Z}$ 的理想。
环 R 上的矩阵环 $M_n(R)$，设 I 是 R 的理想，则 $M_n(I)$ 是 $M_n(R)$ 的理想。
接下来是一些理想相关的定义

定义 7.8

任意环 R，$\{0\}$ 是零理想，R 是单位理想。都称为平凡理想。
对 R 里的一个子集 $S \subseteq R$，定义 S 的生成理想 **(generated ideal)** 是包含 S 的最小理想，记作 (S)。
若 S 是由单个元素 s 构成的集合，称其生成理想为主理想 **(principal ideal)**。也可以记作 (s)。
对于 $S \subseteq R$，可以认为

$$(S) = \{\sum_{i=1}^{t} a_i s_i b_i \mid a_i, b_i \in R, s_i \in S\} \tag{7.8}$$

若 R 是交换环，则可以化简为

$$(S) = \{\sum_{i=1}^{t} a_i s_i \mid a_i \in R, s_i \in S\} \tag{7.9}$$

命题 7.1

交换环 R 是域当且仅当 R 没有非平凡理想。

证明 (1)“⇒”：若 R 是域，则任意非零理想 I，$\exists a \neq 0, a \in I$。则存在 $a^{-1} \in R, a \cdot a^{-1} = 1 \in I$，则 $\forall x \in R, x \cdot 1 = x \in I$。则 $I = R$。即 R 只有平凡理想。

(2)“⇐”：若 R 只有平凡理想，则 $\forall s \in R, s \neq 0$，有 $(s) = \{sr \mid r \in R\} = R$，即存在 s^{-1} 使得 $s \cdot s^{-1} = 1$。则 R 是域。

定义 7.9

若环 R 无非平凡理想，则称 R 是单环 **(simple ring)**。

定义 7.10

定义两个理想 I, J 间的运算为

$$I + J = \{i + j \mid i \in I, j \in J\} \tag{7.10}$$

$$IJ = (\{ij \mid i \in I, j \in J\}) \tag{7.11}$$

容易证明 $+$ 和 $\cdot$ 运算结果依然是理想。且易看出 $IJ \subseteq I \cap J$。

定义 7.11

称环 R 的理想 I 是极大的，若任意理想 J 若满足 $I \subseteq J \subseteq R$ 则 $J = I$ 或 $J = R$。

例子：p 是质数，则 $p\mathbb{Z}$ 是 $\mathbb{Z}$ 的极大理想。

定义 7.12

称环 R 的两个理想 I 和 J 是互素 **(coprime)** 的，若

$$I + J = R \tag{7.12}$$

例子：$a\mathbb{Z}+b\mathbb{Z}=\gcd(a,b)\mathbb{Z}$。则当 $\gcd(a,b)=1$ 时，$a\mathbb{Z}$ 和 $b\mathbb{Z}$ 互素。

命题 7.2

对交换环 R，若 $I+J=R$，则 $IJ=I\cap J$。

♠

证明 无条件满足 $IJ\subseteq I\cap J$。

存在 $a\in I,b\in J$，有 $a+b=1$。则 $\forall c\in I\cap J$，有 $c=c(a+b)=ca+cb\in IJ$。即 $I\cap J\subseteq IJ$。

综上 $IJ=I\cap J$。

定义 7.13

对于环 R 的非单位理想 I，可以定义

$$R/I=\{a+I\mid a\in R\} \tag{7.13}$$

为 R 对 I 的商环。

由 $I\neq R$，则 $1\notin I$，则 $1+I\neq 0+I$。

具体的如下定义环上运算。

$$(a+I)+(b+I)=a+b+I \tag{7.14}$$

$$(a+I)(b+I)=ab+I \tag{7.15}$$

易证以上定义是良定义的。

♣

定义 7.14

自然环同态：$\phi:R\to R/I$

满足

$$\phi(r)=r+I \tag{7.16}$$

♣

定理 7.1

环同态定理：考虑从环 R 到环 S 的环同态映射 ϕ，令 $I=Ker(\phi)$，$Im(\phi)=\phi(R)$。有以下定理

- 令 $\hat{\phi}:R/I\to\phi(R)$ 定义为 $\hat{\phi}(a+I)=\phi(a)$。则 $\hat{\phi}$ 是环同构映射。
- 令 A 是 R 子环，B 是 R 理想，则 $A+B$ 是 R 子环，$A\cap B$ 是 A 理想，且

$$(A+B)/B\cong A/(A\cap B) \tag{7.17}$$

- I 和 J 都是 R 理想，且 $I\subseteq J$，则

$$R/J\cong(R/I)/(J/I) \tag{7.18}$$

- 设 I 是 R 理想，则 $\{J \text{ is ideal of } R\mid I\subseteq J\subseteq R\}$ 和 $\{J \text{ is ideal of } R/I\}$ 之间存在双射 ψ。$\psi(J)=J/I$ 就是这个双射。

♡

证明 第二定理证明：对同态映射 $\phi:A+B\to A/(A\cap B)$，定义 $\phi(a+b)=a+A\cap B$。

则可看出若 $\phi(a+b)=A\cap B$，则 $a\in B$。若 $a\in B$，则 $a+A\cap B=A\cap B$。即 $Ker(\phi)=B$。且 $Im(\phi)=A/(A\cap B)$，由第一定理 $(A+B)/B\cong A/(A\cap B)$。

同态定理证明和群同态非常相似。其他的略去。

下面是同态定理的应用

命题 7.3

设 I 是交换环 R 的非平凡理想。则 I 是极大理想 $\Leftrightarrow$ R/I 是域。

♠

证明 由同态定理，所有包含 I 的理想和 R/I 的理想存在双射。则若 R/I 是域，即无非平凡理想，即包含 I 的理

想只有 I 和 R，即 I 是极大的。反之亦然。

定理 7.2

中国剩余定理：交换环 R 的若干理想 I_i 两两互素，则有如下环同构：

$$R/I_1 \times \ldots \times R/I_t \cong R/(I_1 I_2 \ldots I_t) \tag{7.19}$$

♡

证明 考虑从 R 到 $R/I_1 \times R/I_2 \times \ldots \times R/I_t$ 的同态映射 ϕ，定义

$$\phi(r) = (r + I_1, r + I_2, \ldots, r + I_t) \tag{7.20}$$

易证 ϕ 是同态映射。

若 $\phi(r + I_1 I_2 \ldots I_t) = 0$，则 $r \in I_1 I_2 \ldots I_t$。反之亦然。则 $Ker(\phi) = I_1 I_2 \ldots I_t$。

下证 $\forall (a_1 + I_1, a_2 + I_2, \ldots, a_t + I_t)$，存在一个 $r \in R$ 使得 $\phi(r) = \vec{a}$

固定一个 I_j，则对于任意 $j \neq i$，有 $I_j + I_i = R$，则 $\exists u_i \in I_j, v_i \in I_i$ 使得 $u_i + v_i = 1$，则 $v_i + I_j = 1 + I_j$。则令 $e_j = \prod_{i \neq j} v_i$。则 $e_j + I_j = 1 + I_j$，且有 $e_j \in I_1 I_2 \ldots I_{j-1} I_{j+1} \ldots I_t$

令 $r = e_1 a_1 + e_2 a_2 + \ldots + e_t a_t$，则有 $\phi(r) = (a_1 + I_1, a_2 + I_2, \ldots, a_t + I_t)$。

以上可证 $Im(\phi) = R/I_1 \times R/I_2 \times \ldots \times R/I_t$，由环同态定理 $R/Ker(\phi) = Im(\phi)$ 可得中国剩余定理。

商环的例子：

域 $\mathbb{F}$ 上的多项式环 $\mathbb{F}[x]$。有 $\mathbb{F}[x]/(x) \cong \mathbb{F}$。

考虑 $(x-1)$。由 $\forall k, (x-1) \mid (x^k - 1^k)$，且 $f(x) - f(1)$ 就是所有 $x^k - 1^k$ 的线性组合，则 $(x-1) \mid f(x) - f(1)$。任何多项式 $f(x)$ 和 $f(1)$ 在商环里属于同一元素。即 $\mathbb{F}[x]/(x-1) \cong \mathbb{F}$

$\mathbb{Z}[x]/(x^2+5) = \{a + bx \mid a, b \in \mathbb{Z}\}$

同理，任何一个至少 2 次多项式可以通过多项式带余除法得到一次多项式的代表元。

直观理解上，在商环里，我们相当于要求了 $x^2 + 5 = 0$，即形式化的要求 $x = \sqrt{-5}$。定义 $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$，直观理解 $\mathbb{Z}[x]/(x^2+5) \cong \mathbb{Z}[\sqrt{-5}]$。具体验算发现同构成立。

或者，定义从 $\mathbb{Z}[x]$ 到 $\mathbb{Z}[\sqrt{-5}]$ 的同态映射 $\phi(f) = f(\sqrt{-5})$。由环同态定理得到结论。

7.3 从环到域

接下来从 Integral Domain 到 Field 定义，逐步细化定义。

定义 7.15

环 R，若 $u \in R, \exists u^{-1} \in R, uu^{-1} = 1$，则称 u 是单位 **(unit)**。

定义 $R^* = \{u \in R \mid u \text{ is a unit}\}$。在乘法运算下 R^* 构成群。

♣

定义 7.16

若 R 是整区，定义 R 的分式域 **(fraction field)** 是 $R \times (R \setminus \{0\})/\sim$。

其中 $\sim$ 是一个等价关系，$(a,b) \sim (c,d) \Leftrightarrow ad = bc$。

运算为

$$(a,b) + (c,d) = (ad + bc, bd) \tag{7.21}$$

$$(a,b)(c,d) = (ac, bd) \tag{7.22}$$

♣

定义 7.17

环 R 的特征定义为最小的正整数 c 使得 c 个 1 相加得到 0。若无这样的正整数定义特征为 0。记作 $char(R)$。

♣

命题 7.4

若 R 是整区，则 $char(R)$ 是素数或 0。

证明 假设 $char(R) = c = mn$，其中 $m,n \neq 1$，则定义 M 为 m 个 1 相加，N 为 n 个 1 相加。由环的分配律有 $MN = 0$。由整区定义，$M = 0$ 或 $N = 0$，与特征定义矛盾。

命题 7.5

若整区 R 的特征为 p，则存在一个子环与 $\mathbb{Z}_p$ 同构。若特征为 0，则存在一个子环与 $\mathbb{Z}$ 同构。

证明 考虑从 $\mathbb{Z}$ 到 R 的同态映射 ϕ。定义 $\phi(n)$ 为

$$\begin{cases} n\text{个}1\text{相加} & n > 0 \\ 0 & n = 0 \\ -n\text{个}-1\text{相加} & n < 0 \end{cases}$$

容易验证 ϕ 是同态映射。由定义 $Im(\phi)$ 是 R 的子环。

当 $Char(R) = 0$ 时，$Ker(\phi) = \{0\}$。由环同态定理，$\mathbb{Z} \cong Im(\phi)$。

当 $Char(R) = p$ 时，$Ker(\phi) = p\mathbb{Z}$。由环同态定理，$\mathbb{Z}/(p\mathbb{Z}) = \mathbb{Z}_p \cong Im(\phi)$。

定理 7.3

对整区 R，若存在从 R 到域 $\mathbb{F}$ 的单同态映射 f，则存在从 $Frac(R)$ 到域 $\mathbb{F}$ 的同态映射 $\hat{f}$，且 $\hat{f}$ 限制在 $(R,1)$ 上等于 f。

证明 令 $\hat{f}(a,b) = \frac{f(a)}{f(b)}$。由单同态，$f(b) \neq 0$，可如上定义。简单的运算可验证其良定义，同态性，以及限制后和 f 相同。

接下来是一些构造域有用的定义。

定义 7.18

称一个环 R 的理想 I 是素理想若 $a,b \in R, ab \in I$，则 $a \in I$ 或 $b \in I$

命题 7.6

对交换环 R，若 I 是素理想，则 R/I 是整区。

证明 若 $(a+I)(b+I) = I$，即 $ab \in I$，由素理想定义，则 $a \in I \vee b \in I$，即 $a + I = I \vee b + I = I$。即 R/I 是整区。

定义 7.19

对交换环 R:

- 称 $a \mid b$，若 $\exists u \in R, b = ua$。
- 称 a 和 b 相伴，若 $a \mid b \wedge b \mid a$。记作 $a \sim b$。
- 称 $a \in R$ 不可约，若 $a \neq 0 \wedge a \nmid 1$ 且 $p|a \to p \sim 1 \vee p \sim a$。
- 称 $p \in R$ 是素元，若 $p \neq 0 \wedge p \nmid 1$，$p|ab \to p|a \vee p|b$。

定义 7.20 (主理想环)

称 R 为主理想环 (Principal Ideal Ring, PID)，若所有理想 I 都是某个元素 s 的主理想 (s)。

命题 7.7

主理想环 R 里，不可约元 a 生成的主理想 (a) 是极大理想。素元 p 生成的主理想 (p) 是素理想。且 I 是极大理想等价于 I 是素理想。

证明 任意 R 中不可约元 a。若 $(a)\subseteq I\subseteq R$，则 $\exists u\in R, I=(u)$。则 $a\in(u), u\mid a$。则 $u\sim 1\vee u\sim a$，即 $I=R\vee I=(a)$。即 (a) 是极大理想。

若 a 可约，则 $a=xy$，x,y 都不是单位。则 $(a)\subseteq(x)\subseteq R$。其中 $x\in(x)$ 但 $x\notin(a)$。由 x 不是单位则 $(x)\neq R$。则 (a) 不是极大理想。

任意 R 中素元 p。若 $ab\in(p)$，即 $p\mid ab$，则 $p\mid a\vee p\mid b$，即 $a\in(p)\vee b\in(p)$。即 (p) 是素理想。

若 p 不是素元，同理可证 (p) 不是素理想。

下证素元等价于不可约元。

若 s 可约，$s\in R, s=ab$，且 a,b 都不是单位。则 $s\mid ab$，但 $s\nmid a, s\nmid b$。则 s 不是素元。

若 s 不可约，若 $s\mid ab$。考虑 (s,a) 生成的理想，由主理想环，则 $(s,a)=(d), d\in R$。则 $d\mid s$。

若 $d\sim s$，则 $(s,a)=(s)$，即 $s\mid a$。

若 $d\sim 1$，则 $\exists\alpha,\beta\in R, \alpha s+\beta a=1$。

同理考虑 (s,b) 生成的理想 (d')。则 $s\mid b$ 或 $\exists\alpha',\beta'\in R, \alpha' s+\beta' b=1$。

可知 $\beta\beta' ab=(1-\alpha s)(1-\alpha' s)\in 1+(s)$

由 $\beta\beta' ab\in(s)$，则 $1\in(s)$。与 s 是不可约元（非单位）矛盾。

则不可能 $s\nmid a\wedge s\nmid b$，即 s 是素元。

综上，素元等价于不可约元。则极大理想等价于素理想。

注 最后也可以直接 $\alpha sb+\beta ab=\alpha sb+\beta sc=b$，即 $s\mid b$。直接证明 s 是素元。

主理想环具体例子：$\mathbb{Z}$，域 $\mathbb{F}$ 的多项式环 $\mathbb{F}[x]$。

证明 任意 $\mathbb{F}[x]$ 里的理想 I，取其中次数最小的非零多项式 f。假设 $I\neq(f)$，则存在一个 $g\in I\setminus(f)$，做对 f 的带余除法 $g=fh+r$，其中 $r\neq 0$。但 r 的次数低于 f，且 $r\in I$，与 f 定义矛盾。则 I 是主理想。

定义 7.21 (欧式整区)

称环 R 是欧式整区 (Euclidean Domain)，若存在一个从 R 到 $\mathbb{N}$ 的映射，称为范数，满足如下条件：

- $|x|=0\Leftrightarrow x=0$
- $\forall a\in R, b\neq 0$，存在 $q,r\in R$ 使得 $a=bq+r$，且 $|r|<|b|$。

♣

定理 7.4

每个欧式整区都是主理想整环。

♡

证明 设 R 是欧几里得整环，φ 是其范数。设 I 是 R 的任意理想。

如果 $I=\{0\}$，则 $I=(0)$ 是主理想。

如果 $I\neq\{0\}$，考虑集合：

$$S=\{\varphi(x)\mid x\in I,\ x\neq 0\} \tag{7.23}$$

由于 S 是非负整数集的非空子集，则 S 有最小元。设 $a\in I$，$a\neq 0$，使得 $\varphi(a)$ 是 S 的最小元。

我们断言 $I=(a)$。

首先，显然有 $(a)\subseteq I$，因为 $a\in I$ 且 I 是理想。

反之，任取 $b\in I$。由欧几里得整环的定义，存在 $q,r\in R$ 使得：

$$b=aq+r\quad 且\quad r=0\text{ 或 }\varphi(r)<\varphi(a) \tag{7.24}$$

由于 $b\in I$ 且 $a\in I$，有 $r=b-aq\in I$。

如果 $r\neq 0$，则 $\varphi(r)<\varphi(a)$，但 $\varphi(a)$ 是 S 的最小元，矛盾。因此 $r=0$，从而 $b=aq\in(a)$。

故 $I\subseteq(a)$。

综上，$I=(a)$ 是主理想。由于 I 是任意理想，R 是主理想整环。

欧式整区具体例子：$\mathbb{Z}, \mathbb{Z}[i]$。

对 $a+bi\in\mathbb{Z}[i]$，定义范数为 a^2+b^2。性质第一条显然满足。

考虑第二条性质。对于 $a,b\in\mathbb{Z}[i],b\neq 0$，考虑商环元素 $a+(b)$，相当于在二维平面上过 a 点，以 b 向量为边长生成的正方形格。那么考虑离 0 最近的格点 $a+bq$，这个距离一定小于正方形边长。则 $|a-bq|<|b|$。性质第二条满足。则是欧式整区。

定义 7.22 (唯一分解环)

设 R 是一个整区。如果 R 满足以下两个条件，则称 R 为唯一分解环（Unique Factorization Domain, UFD）：

1. （存在性）对于 R 中的每一个非零非单位元素 a，都存在有限个不可约元 $p_1,p_2,\dots,p_n\in R$，使得

$$a=p_1p_2\cdots p_n \tag{7.25}$$

2. （唯一性）如果 a 有两个这样的分解：

$$a=p_1p_2\cdots p_n=q_1q_2\cdots q_m \tag{7.26}$$

其中 p_i 和 q_j 都是不可约元，那么：

- $n=m$
- 存在一个置换 $\sigma\in S_n$，使得对于每个 i，p_i 与 $q_{\sigma(i)}$ 相伴（即存在单位 $u_i\in R^\times$，使得 $p_i=u_iq_{\sigma(i)}$）

♣

定义 7.23

对一个整区 R，定义两种可能的性质。

因子链条件：不存在无限长的序列 $\{a_i\}$ 使得 $\forall i,a_{i+1}\mid a_i\wedge a_i\nmid a_{i+1}$。

素性条件：$\forall s\in R$，s 不可约等价于 s 是素元。

♣

定理 7.5

唯一分解环 R 满足因子链条件和素性条件。

♡

证明 素性条件：任意不可约元 s，假设 $s\mid ab\wedge s\nmid a\wedge s\nmid b$。

则对 ab 有两种分解方式。

$$ab=decomp(a)\cdot decomp(b) \tag{7.27}$$

$$ab=s\cdot decomp(\frac{ab}{s}) \tag{7.28}$$

由 $s\nmid a\wedge s\nmid b$，则 $decomp(a)$ 和 $decomp(b)$ 中都没有 s。则 ab 有两种不同分解，矛盾。

若 a 可约，则 a 一定不是素元。则唯一分解环满足素性条件。

证明 因子链条件：设 R 是唯一分解环，假设存在真因子链

$$a_1,a_2,a_3,\dots \tag{7.29}$$

其中 $a_{i+1}\mid a_i$ 且 $a_i\nmid a_{i+1}$。

考虑 a_i 的不可约因子分解。由于 a_{i+1} 是 a_i 的真因子，a_{i+1} 的不可约因子分解要么比 a_i 少一个不可约因子，要么某些不可约因子的重数减少。

定义函数 $\varphi:R\setminus\{0\}\to\mathbb{N}$ 如下：

- 对于单位 u，定义 $\varphi(u)=0$
- 对于非零非单位元素 $a=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$（其中 p_i 是互不相伴的不可约元），定义

$$\varphi(a)=e_1+e_2+\cdots+e_k \tag{7.30}$$

如果 b 是 a 的真因子，则 $\varphi(b)<\varphi(a)$。因此在真因子链中：

$$\varphi(a_1)>\varphi(a_2)>\varphi(a_3)>\cdots \tag{7.31}$$

这是一个严格递减的自然数序列，不可能无限长。矛盾。

因此，唯一分解环中不存在无限长的真因子链，即满足因子链条件。

定理 7.6

设 R 是整区。如果 R 满足因子链条件和素性条件，则 R 是唯一分解环。 ♡

证明 我们需要证明 R 满足唯一分解环的两个条件：分解的存在性和唯一性。

存在性：设 $a \in R$ 是非零非单位元素。我们需要证明 a 可以分解为有限个不可约元的乘积。

假设存在某个非零非单位元素 a 不能分解为有限个不可约元的乘积。我们将构造一个无限真因子链，与因子链条件矛盾。

由于 a 不能分解为有限个不可约元的乘积，特别地 a 本身不是不可约元（否则 $a = a$ 就是一个分解）。因此 a 可约，即存在真因子分解：

$$a = a_1 b_1 \tag{7.32}$$

其中 a_1, b_1 都是 a 的真因子（即 $a_1 \mid a$，$b_1 \mid a$，但 $a \nmid a_1$，$a \nmid b_1$）。

由于 a 不能分解为有限个不可约元的乘积，至少 a_1 和 b_1 中有一个也不能分解为有限个不可约元的乘积（否则 a 就可以分解了）。不妨设 a_1 不能分解为有限个不可约元的乘积。

对 a_1 重复上述论证：由于 a_1 不能分解为有限个不可约元的乘积，特别地 a_1 不是不可约元，因此存在真因子分解：

$$a_1 = a_2 b_2 \tag{7.33}$$

其中 a_2 是 a_1 的真因子，且 a_2 也不能分解为有限个不可约元的乘积。

继续这个过程，我们得到一个无限序列：

$$a, a_1, a_2, a_3, \ldots \tag{7.34}$$

其中每个 a_{i+1} 都是 a_i 的真因子。这与因子链条件矛盾！

因此，我们的假设错误，每个非零非单位元素都可以分解为有限个不可约元的乘积。

唯一性：设 $a \in R$ 是非零非单位元素，有两个不可约分解：

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n \tag{7.35}$$

其中 p_i 和 q_j 都是不可约元。

我们对 m 进行数学归纳法来证明分解的唯一性。

归纳基础：当 $m = 1$ 时，$a = p_1$ 是不可约元。那么 $p_1 = q_1 q_2 \cdots q_n$。由于 p_1 是不可约元，n 必须为 1（否则 p_1 可约），且 q_1 与 p_1 相伴。唯一性成立。

归纳假设：假设对于所有可以写成 $m-1$ 个不可约元乘积的元素，分解是唯一的（在相伴和重排意义下）。

归纳步骤：考虑 $a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$。

由于 p_1 是不可约元，且 R 满足素性条件，p_1 是素元。考虑 $p_1 \mid q_1 q_2 \cdots q_n$。由于 p_1 是素元，存在某个 j 使得 $p_1 \mid q_j$。

重排 q_j 使得 $p_1 \mid q_1$。由于 q_1 也是不可约元，$p_1 \mid q_1$ 意味着 p_1 与 q_1 相伴，即存在单位 u 使得 $q_1 = u p_1$。

代入原等式：

$$p_1 p_2 \cdots p_m = (u p_1) q_2 \cdots q_n \tag{7.36}$$

由于 R 是整环，可以消去 p_1（非零）：

$$p_2 \cdots p_m = (u q_2) q_3 \cdots q_n \tag{7.37}$$

注意 $u q_2$ 也是不可约元（因为 q_2 不可约且 u 是单位）。

现在左边的乘积有 $m-1$ 个不可约元，由归纳假设，$m - 1 = n - 1$（即 $m = n$），且存在置换 σ 使得对于 $i = 2, \ldots, m$，p_i 与对应的不可约元相伴。

结合 p_1 与 q_1 相伴，我们得到整个分解的唯一性。

由数学归纳法，分解的唯一性得证。

定理 7.7

任意主理想环 R 一定是唯一分解环。 ♡

证明 由前面证明，主理想环符合素性条件。

设 R 是主理想环，假设存在真因子链：

$$a_1, a_2, a_3, \dots \tag{7.38}$$

其中 $a_{i+1} \mid a_i$ 且 $a_i \nmid a_{i+1}$。

考虑由这些元素生成的主理想：

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots \tag{7.39}$$

现在考虑这些理想的并集：

$$I = \bigcup_{i=1}^{\infty} (a_i) \tag{7.40}$$

我们证明 I 是 R 的一个理想：

- 对任意 $x, y \in I$，存在 m, n 使得 $x \in (a_m)$，$y \in (a_n)$。取 $N = \max\{m, n\}$，则 $x, y \in (a_N)$，因此 $x - y \in (a_N) \subseteq I$。
- 对任意 $x \in I$ 和 $r \in R$，存在 m 使得 $x \in (a_m)$，因此 $rx \in (a_m) \subseteq I$。

由于 R 是主理想环，存在 $a \in R$ 使得 $I = (a)$。

由于 $a \in I = \bigcup_{i=1}^{\infty} (a_i)$，存在某个 k 使得 $a \in (a_k)$，即 $a_k \mid a$。

另一方面，由于 $I = (a)$，对于任意 i，我们有 $a_i \in (a)$，即 $a \mid a_i$。

特别地，取 $i = k + 1$，我们有 $a \mid a_{k+1}$。

但 $a_{k+1} \mid a_k \mid a$，因此 $a_{k+1} \mid a$ 且 $a \mid a_{k+1}$，这意味着 a 与 a_{k+1} 相伴，即 $(a) = (a_{k+1})$。

现在考虑 a_k：由于 $a \mid a_k$ 且 $a_k \mid a$（因为 $a_k \in I = (a)$），我们有 a 与 a_k 相伴，即 $(a) = (a_k)$。

但 $(a_k) = (a) = (a_{k+1})$，这与 a_{k+1} 是 a_k 的真因子矛盾（因为真因子意味着 $(a_k) \subsetneq (a_{k+1})$）。

因此，我们的假设错误，主理想环中不存在无限长的真因子链，即满足因子链条件。

非唯一分解环例子：$\mathbb{Z}[\sqrt{-5}]$。其中 $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$。其中 3 和 $2 + \sqrt{-5}$ 和 $2 - \sqrt{-5}$ 都是不可约元素，且不相伴。则 $\mathbb{Z}[\sqrt{-5}]$ 不是唯一分解环。

用以上所有工具，我们来通过域的多项式环 $\mathbb{F}[x]$ 来构造一个域。

已知命题 1.3，则我们试图用 $\mathbb{F}/I$，其中 I 是极大理想。由多项式环是主理想环，则 $I = (f)$。

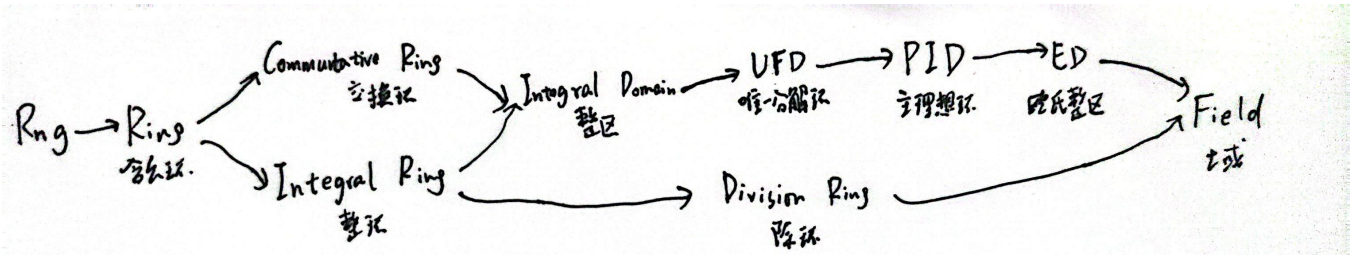
由素性条件和命题 1.6，若 f 是不可约多项式，则 I 是极大理想。则 $\mathbb{F}[x]/(f)$ 是一个域。

考虑域 $\mathbb{F} = \mathbb{Z}_p$ 和一个 d 次不可约多项式 f。那么代表元是所有系数在 $\mathbb{Z}_p$ 中，次数小于 d 的多项式：

$$\mathbb{Z}_p[x]/(f) = \{\sum_{i=0}^{d-1} a_i x^i \mid a_i \in \mathbb{Z}_p\} \tag{7.41}$$

可以看到这个域的大小为 p^d。则任意素数 p，任意幂次 d，都存在一个大小为 p^d 的有限域。

最终，综合我们以上证明的所有性质的环之间的规约关系，我们有以下这张图


Rng
Ring
含幺环
Commutative Ring
交换环
Integral Ring
整环
Integral Domain
整区
UFD
唯一分解环
PID
主理想环
ED
欧氏整区
Field
域
Division Ring
除环

第八章 域 (Field)

8.1 域扩张

定义 8.1 (子域)

设 F 和 K 都是域。如果 F 是 K 的子集，且 F 在 K 的运算下构成域，则称 F 是 K 的子域，记作 $F \leq K$。

定义 8.2 (域扩张)

设 F 是 K 的子域，则称 K 是 F 的域扩张（或扩域），记作 K/F（读作"K over F"）。称 F 是基域。

1. 如果 K/F 是域扩张，则 K 可以自然地视为 F 上的向量空间。
2. 域扩张的**次数**定义为向量空间的维数：$[K:F] = \dim_F K$。
3. 如果 $[K:F] < \infty$，则称 K/F 为**有限扩张**，否则称为**无限扩张**。

定理 8.1

若域 F 特征为 p，则 $\mathbb{Z}_p$ 同构于某子域。

若域 F 特征为 0，则 $\mathbb{Q}$ 同构于某子域。

证明 特征为 p 时结论已知。

特征为 0 时，由环特征的定理，存在 $\mathbb{Z}$ 和某子域同构。由分式环到域同态映射定理可知存在 $\mathbb{Q}$ 和某子域同构。

命题 8.1

任意有限域大小为质数的幂次。

证明 设 $char(F) = p$，则存在一个子群 K 和 F_p 同构是 F 的子域。设 $[F:K] = d$，则 $|F| = p^d$。

定理 8.2 (域扩张次数的乘法公式)

设 $F \subset E \subset K$ 是域的塔扩张，则

$$[K:F] = [K:E][E:F] \tag{8.1}$$

其中 $[K:F]$ 表示 K 作为 F 上向量空间的维数。

证明 我们分两种情况证明：

情况一：$[E:F]$ 或 $[K:E]$ 无限

如果 $[E:F] = \infty$ 或 $[K:E] = \infty$，则 $[K:F]$ 也必然无限，因为：

- 如果 $[E:F] = \infty$，则存在 E 中无限多个 F-线性无关的元素，这些元素在 K 中也是 F-线性无关的
- 如果 $[K:E] = \infty$，则存在 K 中无限多个 E-线性无关的元素，这些元素在 K 中也是 F-线性无关的

因此在这种情况下，等式两边都是 ∞，公式成立。

情况二：$[E:F]$ 和 $[K:E]$ 都有限

设：

- $[E:F] = m$，取 E 在 F 上的一组基：$\{e_1, e_2, \ldots, e_m\}$
- $[K:E] = n$，取 K 在 E 上的一组基：$\{k_1, k_2, \ldots, k_n\}$

我们证明集合

$$B = \{e_i k_j \mid 1 \leq i \leq m,\ 1 \leq j \leq n\} \tag{8.2}$$

是 K 在 F 上的一组基。

第一步：证明 B 是 F-线性生成集

对任意 $x \in K$，由于 $\{k_1, \ldots, k_n\}$ 是 K 在 E 上的基，存在 $a_1, \ldots, a_n \in E$ 使得

$$x = a_1 k_1 + a_2 k_2 + \cdots + a_n k_n \tag{8.3}$$

又因为 $\{e_1, \ldots, e_m\}$ 是 E 在 F 上的基，对每个 $a_j \in E$，存在 $b_{1j}, \ldots, b_{mj} \in F$ 使得

$$a_j = b_{1j} e_1 + b_{2j} e_2 + \cdots + b_{mj} e_m \tag{8.4}$$

代入得：

$$\begin{aligned} x &= \sum_{j=1}^{n} a_j k_j \\ &= \sum_{j=1}^{n} \left(\sum_{i=1}^{m} b_{ij} e_i \right) k_j \\ &= \sum_{i=1}^{m} \sum_{j=1}^{n} b_{ij} (e_i k_j) \end{aligned}$$

因此 x 可以表示为 B 中元素的 F-线性组合，即 B 生成 K 作为 F-向量空间。

第二步：证明 B 是 F-线性无关的

假设存在 $c_{ij} \in F$ 使得

$$\sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} (e_i k_j) = 0 \tag{8.5}$$

整理得：

$$\sum_{j=1}^{n} \left(\sum_{i=1}^{m} c_{ij} e_i \right) k_j = 0 \tag{8.6}$$

令 $d_j = \sum_{i=1}^{m} c_{ij} e_i \in E$，则上式变为：

$$\sum_{j=1}^{n} d_j k_j = 0 \tag{8.7}$$

由于 $\{k_1, \ldots, k_n\}$ 是 K 在 E 上的基，E-线性无关，所以对每个 j，$d_j = 0$，即

$$\sum_{i=1}^{m} c_{ij} e_i = 0 \quad \text{对每个} j = 1, \ldots, n \tag{8.8}$$

又因为 $\{e_1, \ldots, e_m\}$ 是 E 在 F 上的基，F-线性无关，所以对每个 i, j，$c_{ij} = 0$。

因此 B 是 F-线性无关的。

第三步：计算维数

由于 B 是 K 在 F 上的一组基，且 $|B| = mn$，所以

$$[K : F] = mn = [K : E][E : F] \tag{8.9}$$

做域扩张的几种方式：

1. 域 F，则系数为 F 的不可约 d 次多项式 f，有 $F[x]/(f)$ 是域。所有 0 次多项式是 F。且 $[F[x]/f : F] = d$。则 $F[x]/(f)$ 是 F 的域扩张。
2. 域 F 的分式域 $Frac(F[x])$ 记为 $F(x)$，其中分母为常数的是 $F[x]$。度数为无穷。则 $F(x)$ 是 F 的域扩张。
3. 令 F 是 K 的子域。其中 $u \in K$ 不是 F 的元素。令 $F(u)$ 为包含 F 和 u 最小的子域。显然 $F(u)$ 是 F 的域扩张。

接下来考虑域之间的同态。

命题 8.2

域 F 到域 F' 的同态映射如果不是零同态就是单射。

证明 如果 φ 不是单射，则 $\ker(\varphi) \neq \{0\}$。由于 F 是域，它的理想只有 $\{0\}$ 和 F，所以 $\ker(\varphi) = F$，即 φ 是零同态。

命题 8.3

域 F 到 F' 的同态映射 ϕ，$\phi(F)$ 也是域。

具体例子：

1. 已知 $\mathbb{R}[i] = \mathbb{C}$。域 $\mathbb{R}[x]/(x^2+1)$ 到 $\mathbb{C}$ 有一个同构映射 $\phi(ax+b) = ai + b$。$\psi(ax+b) = -ai + b$ 也是同构映射。
2. 更一般的，令 K/F，$u \in K$。$f \in F[x]$ 不可约，且 $f(u) = 0$。则 $F[x]/(f) \cong F(u)$。此时称 u 为 F 上的代数数。

   证明 我们通过构造显式的同构来证明这个定理。

   第一步：定义环同态

   定义映射：

   $$\varphi : F[x] \to F(u), \quad g(x) \mapsto g(u) \tag{8.10}$$

   容易验证 φ 是环同态.

   第二步：计算同态的核

   设 $g(x) \in \ker(\varphi)$，则 $g(u) = 0$。考虑 $f(x)$ 和 $g(x)$ 的最大公因式 $d(x) = \gcd(f(x), g(x))$。由于 $f(x)$ 不可约，$d(x)$ 要么是常数，要么是 $f(x)$ 的相伴元。

   $d(x)$ 是 $f(x)$ 和 $g(x)$ 的 $F[x]$ 线性组合，所以 $d(u) = 0$。如果 $d(x)$ 是常数，则 $d(u) \neq 0$，矛盾。因此 $d(x)$ 是 $f(x)$ 的相伴元，即 $f(x) \mid g(x)$。则 $\ker(\varphi) = (f)$。

   第三步：证明同态是满射

   我们需要证明 φ 是满射，即对任意 $y \in F(u)$，存在 $g(x) \in F[x]$ 使得 $g(u) = y$。

   由于 $F(u)$ 是 F 通过添加 u 得到的域，$F(u)$ 中的元素都可以表示为 u 的多项式（系数在 F 中）。更精确地说，由于 $f(x)$ 是 u 的极小多项式且 $\deg f = n$，则 $F(u)$ 中每个元素可以唯一表示为：

   $$a_0 + a_1 u + a_2 u^2 + \cdots + a_{n-1} u^{n-1}, \quad a_i \in F \tag{8.11}$$

   因此，对任意 $y \in F(u)$，存在多项式 $g(x) \in F[x]$ 且 $\deg g < n$ 使得 $g(u) = y$。特别地，取这个 $g(x)$，我们有 $\varphi(g(x)) = g(u) = y$。

   那么由环同态基本定理，我们有：

   $$F[x]/(f(x)) \cong F(u) \tag{8.12}$$

3. 若 $\forall f \in F[x], f(u) \neq 0$，那么有 $Frac(F[x]) \cong F(u)$。此时称 u 为 F 上的超越数。

   证明 第一步：定义分式域的同态

   考虑分式域：

   $$\mathrm{Frac}(F[x]) = \left\{ \frac{g(x)}{h(x)} \,\middle|\, g(x), h(x) \in F[x],\ h(x) \neq 0 \right\} \tag{8.13}$$

   定义映射：

   $$\varphi : \mathrm{Frac}(F[x]) \to F(u), \quad \frac{g(x)}{h(x)} \mapsto \frac{g(u)}{h(u)} \tag{8.14}$$

   第二步：证明 φ 是良定义的

   我们需要证明：

   - 分母不为零：由于 $h(x) \neq 0$ 且 u 是超越元，$h(u) \neq 0$，所以 $\frac{g(u)}{h(u)}$ 在 $F(u)$ 中有意义。

- 与表示无关：如果 $\frac{g_1(x)}{h_1(x)} = \frac{g_2(x)}{h_2(x)}$ 在 $\mathrm{Frac}(F[x])$ 中，则存在非零多项式 $k(x) \in F[x]$ 使得

$$g_1(x)h_2(x)k(x) = g_2(x)h_1(x)k(x) \tag{8.15}$$

特别地，在 $x = u$ 处有：

$$g_1(u)h_2(u)k(u) = g_2(u)h_1(u)k(u) \tag{8.16}$$

由于 $k(u) \neq 0$（u 是超越元），我们得到：

$$g_1(u)h_2(u) = g_2(u)h_1(u) \tag{8.17}$$

因此：

$$\frac{g_1(u)}{h_1(u)} = \frac{g_2(u)}{h_2(u)} \tag{8.18}$$

且显然 φ 是同态。

第三步：证明 φ 是单射

假设 $\varphi\left(\frac{g(x)}{h(x)}\right) = 0$，则：

$$\frac{g(u)}{h(u)} = 0 \Rightarrow g(u) = 0 \tag{8.19}$$

由于 u 是超越元，$g(x)$ 必须是零多项式，所以 $\frac{g(x)}{h(x)} = 0$ 在 $\mathrm{Frac}(F[x])$ 中。

因此 $\ker(\varphi) = \{0\}$，φ 是单射。

第四步：证明 φ 是满射

对任意 $y \in F(u)$，由 $F(u)$ 的定义，存在多项式 $g(x), h(x) \in F[x]$，$h(x) \neq 0$，使得：

$$y = \frac{g(u)}{h(u)} \tag{8.20}$$

那么：

$$y = \varphi\left(\frac{g(x)}{h(x)}\right) \tag{8.21}$$

因此 φ 是满射。

命题 8.4

有限扩张一定是代数扩张。超越扩张一定是无限扩张。

从定义就可以直接看出结论。注意无限扩张有可能也是代数扩张。因为可以扩张一个无穷集。比如 $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \ldots]$。

定理 8.3

平面上给定单位长度的尺规作图，无法做出三等分角和倍立方体 (体积为已知立方体 2 倍的立方体)。

证明 考虑我们可以做出长度的集合。

- 首先可以做出 x 轴所有整点。做垂线后可以做出 y 轴所有整点。再做垂线可以做平面上所有整点。
- 用相似三角形法可以做出所有有理数点。
- 所有已知长度的根号可以得出。把 $l-1$ 放到 y 轴上，和 $(1,0)$ 连线，可得到 $\sqrt{l}$。
- 已有长度 a, b，直接拼接得到 $a+b$。
- 已有长度 a, b，通过相似三角形 $1 : a = b : ab$ 可得到 ab。
- 已有长度 a，通过相似三角形可得到 $\frac{1}{a}$。

则所有可得到集合是一个域。且是 $\mathbb{Q}$ 不断进行二次扩张得到的域，称第 i 次操作后的集合为 F_i。除了上面提到的以外，可以证明直线相交，直线与圆相交，两圆相交操作得到的新长度都属于二次扩张。则 $\forall i, [F_i : \mathbb{Q}] = 2^k, k \in \mathbb{N}$。

但若可以三等分角，那么由三倍角公式和正弦定理，可以得到一个已有长度的 $\frac{1}{3}$ 次方。那么这是一个三次扩张。由 $[\mathbb{Q}[l^{\frac{1}{3}}] : \mathbb{Q}] \mid [F_i, \mathbb{Q}]$，但 3 不能整除 2 的幂次，矛盾。

倍立方体同理。

8.2 分裂域

注 这里讨论的多项式默认指首一多项式。

定义 8.3

域 F 上的多项式首一 $f \in F[x]$，称 f 在 K 上分裂，若

$$f(x) = \prod (x - \alpha_i) \tag{8.22}$$

其中 $\alpha_i \in K$。

定义 8.4

称 K 为 $f \in F[x]$ 的分裂域 (splitting field of f)，若

1. f 在 K 上分裂。
2. $K = F(\alpha_1, \ldots, \alpha_d)$

定理 8.4

任意 $f \in F[x]$，存在唯一分裂域 K，且 $[K : F] \leq (\deg f)!$

证明 先证存在性。对 $n = \deg f$ 进行归纳。

基础情况：当 $n = 1$ 时，$K_1 = F$，结论显然成立。

归纳步骤：假设对次数小于 n 的多项式结论成立。

设 $g(x)$ 是 $f(x)$ 的一个不可约因子。考虑域扩张 $F_1 = F[z]/(g)$，有 $[F_1 : F] = \deg(g)$。且元素 $z \in F_1$ 满足 $g(z) = 0$。则 $f(z) = g(z) \cdot (\frac{f}{g})(z) = 0$。则 $(x - z) \mid f$。考虑在域 F_1 上，多项式 $\frac{f(x)}{x-z} \in F_1[x]$，由归纳假设有分裂域 K。则 f 也有分裂域 K。归纳假设成立。

且容易发现每次归纳，多项式的次数都 -1，每次归纳时的扩域维数不超过多项式次数，则总扩域维数不超过 $(\deg f)!$。

证明 第一种唯一性指的是，域 F 的多项式 f 的任何分裂域 K 都和归纳证明构造出来的分裂域同构。

任意 f 的分裂域 K，归纳过程中 $f = g \cdot (\frac{f}{g})$ 其中 g 不可约。那么 g 也在 K 中分裂。假设一个根是 u_1，那么由前面的定理，有 $F_1 = F[z]/(g(z)) \cong F(u_1)$，同态映射为 ϕ。

对于第二层归纳类似进行，令 $f_1 = \frac{f}{x-z}$，则 $f_1 = g_1(\frac{f_1}{g_1})$，其中 g_1 不可约。则 g_1 在 K 中分裂，且存在 u_2 使得 $\phi(g_1)(u_2) = 0$，由定理有 $F_2 \cong F(u_1, u_2)$。可以往下归纳。

到最后就是归纳法构造出来的分裂域同构于 $F(u_1, u_2, \ldots, u_d)$。由分裂域定义，任意 f 的分裂域同构于 $F(u_1, \ldots, u_d)$。

证明 第二种唯一性指的是，有域扩张 K/F，且 $f \in F[x]$ 在 K 上分裂。则若 K 的子域 E_1, E_2 是 f 的分裂域，则 $E_1 = E_2$。这种唯一性是显然的，因为加入的根都是同一个 K 里的元素。

8.3 有限域

定理 8.5

任意质数 p，正整数 d，存在大小为 p^d 的有限域，且同构意义下唯一，记为 $\mathbb{F}_{p^d}$ 或 $GF(p^d)$。

命题 8.5

(费马小定理) 大小为 p^d 的有限域 F，任意非零元素 $x \in F, x \neq 0$ 有 $x^{p^d-1} = 1$。

证明方法和数论章节里的 $\mathbb{Z}_p$ 版本完全相同。

定理 1.5 证明：

证明

假设有大小为 p^d 的域 $\mathbb{F}_{p^d}$，则由费马小定理 $\forall x \in \mathbb{F}_{p^d}, x^{p^d} = x$，则 $\forall a \in \mathbb{F}_{p^d}, (x-a) \mid x^{p^d} - x$。

那么 $\mathbb{F}_{p^d}$ 所有元素都是 $f(x) = x^{p_d} - x \in \mathbb{F}_p[x]$ 的根。有

$$\prod_{\alpha \in \mathbb{F}_{p^d}} (x - \alpha) = x^{p^d} - x \tag{8.23}$$

设 K 是多项式 $f(x) = x^{p^d} - x$ 在 $\mathbb{F}_p$ 上的分裂域。由于 $\mathbb{F}_p$ 是有限域，$f(x)$ 是有限次多项式，其分裂域 K 存在且是有限扩张。

下证 f 无重根。

计算形式导数：

$$f'(x) = p^d x^{p^d - 1} - 1 = -1 \quad (\text{因为} p^d \equiv 0 \pmod{p}) \tag{8.24}$$

由于 $f'(x) = -1 \neq 0$，$f(x)$ 与 $f'(x)$ 互质，因此 $f(x)$ 无重根。

接下来我们开始构造这个域。

$R = \{\alpha \in K \mid f(\alpha) = 0\} = \{\alpha \in K \mid \alpha^{p^d} = \alpha\}$

我们证明 R 构成一个域：

- 加法封闭性：对任意 $\alpha, \beta \in R$，

$$(\alpha + \beta)^{p^d} = \sum_{i=0}^{p^d} \binom{p^d}{i} \alpha^i \beta^{p^d - i} \tag{8.25}$$

注意其中 α 和 β 幂次之间是域乘法，前面的数乘不是域乘法，是后面的元素自加常数次。不难证明当 $i \neq 0 \wedge i \neq p^d$ 时 $p \mid \binom{p^d}{i}$，则由域特征为 p，除了首尾项都是 0。则

$$(\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d} = \alpha + \beta \in R \tag{8.26}$$

所以 $\alpha + \beta \in R$。

- 乘法封闭性：对任意 $\alpha, \beta \in R$，

$$(\alpha\beta)^{p^d} = \alpha^{p^d} \beta^{p^d} = \alpha\beta \tag{8.27}$$

所以 $\alpha\beta \in R$。

- 加法逆元：若 F 特征为 2，则 $-\alpha = \alpha \in R$ 。

若 F 特征不为 2，则 $(-\alpha)^{p^d} = -\alpha^{p^d} = -\alpha$。第一个等号因为 p^d 是奇数。

因此 $-\alpha \in R$。

- 乘法逆元：对任意非零 $\alpha \in R$，

$$(\alpha^{-1})^{p^d} = (\alpha^{p^d})^{-1} = \alpha^{-1} \tag{8.28}$$

所以 $\alpha^{-1} \in R$。

因此 R 是 K 的子域。

由于 $f(x)$ 无重根且次数为 p^d，R 中恰有 p^d 个元素。

由于 R 包含 $f(x)$ 的所有根且是域，而 K 是 $f(x)$ 的分裂域（即包含所有根的最小域），我们有 $K \subseteq R$。

但 $R \subseteq K$，所以 $K = R$。

因此 K 是大小为 p^d 的有限域。

接下来我们通过一系列定理来说明，通过 $\mathbb{F}_q[x]/(f)$ 其中 f 是不可约多项式，这种方式来生成任意素数幂次大小的域的方式可行。

引理 8.1

$$\gcd(x^{q^a}-x, x^{q^b}-x) = x^{q^{\gcd(a,b)}}-x \tag{8.29}$$

♡

证明 设 $\phi(n) = x^{q^n}-x$。

不妨设 $a \geq b$，则

$$x^{q^b}-x \equiv 0 \pmod{\phi(b)} \tag{8.30}$$

$$x^{q^b} \equiv x \pmod{\phi(b)} \tag{8.31}$$

$$x^{q^a} = (x^{q^b})^{q^{a-b}} \equiv x^{q^{a-b}} \pmod{\phi(b)} \tag{8.32}$$

则根据欧几里得算法，有

$$\gcd(\phi(a), \phi(b)) = \gcd(\phi(b), \phi(a-b)) \tag{8.33}$$

可得出引理内容。

命题 8.6

大小为 q 的域 $\mathbb{F}_q$，若 $f \in \mathbb{F}_q[x]$ 不可约次数为 d，则

$$f \mid x^{q^d}-x \tag{8.34}$$

♠

证明 令 $F_1 = \mathbb{F}_q[x]/(f)$，则存在 $u \in F_1$ 使得 $f(u) = 0$。

则 $(x-u) \mid f$ 且 $(x-u) \mid (x^{q^d}-x)$，则 $\gcd(f, x^{q^d}-x) \neq 1$。

由 $f, x^{q^d}-x \in \mathbb{F}_q[x]$，且在 $\mathbb{F}_q[x]$ 里 f 不可约，则 $f \mid (x^{q^d}-x)$。

定理 8.6

大小为 q 的域 $\mathbb{F}_q$，$\mathbb{F}_q[x]$ 上 d 次不可约多项式 f 的分裂域为 K，有 $[K:F] = d$。

♡

证明 取 α 为 f 的一个根。则分裂域 K 满足 $F(\alpha) \subseteq K$。其中 f 是 α 的极小多项式，则 $F(\alpha) = F[x]/(f)$，有 $[F(\alpha):F] = d$。

由命题 1.6 可知 $f \mid x^{q^d}-x$，且 $x^{q^d}-x$ 在 $F(\alpha) \cong \mathbb{F}_{q^d}$ 上分裂。则 $F(\alpha)$ 是 f 的分裂域。

则 $[K:F] = d$。

定理 8.7

大小为 q 的域 $\mathbb{F}_q$，有

$$x^{q^d}-x = \prod_{d' \mid d,\ \text{不可约多项式} f \in \mathbb{F}_q[x]} f(x) \tag{8.35}$$

♡

证明 当 $d' \mid d$ 时，d' 次不可约多项式 f，由命题 1.6 可知 $f \mid (x^{q^{d'}}-x)$。再由引理 1.1 可知 $(x^{q^{d'}}-x) \mid (x^{q^d}-x)$。则有 $f \mid (x^{q^d}-x)$。

当 $d' \nmid d$ 时，d' 次不可约多项式 $f \mid (x^{q^{d'}}-x)$。

假设 $f \mid (x^{q^d}-x)$，则有

$$f \mid \gcd(x^{q^{d'}}-x, x^{q^d}-x) = x^{q^{\gcd(d,d')}}-x \tag{8.36}$$

记 $d'' = \gcd(d, d')$。则 f 在 $\mathbb{F}_{q^{d''}}$ 上分裂，由定理 1.7 可知 $\deg f \leq d''$。与 $d' \nmid d$ 和 $\deg f = d'$ 矛盾。

则 $f \nmid (x^{q^d}-x)$。

由 $x^{q^d}-x$ 无重根，则可约多项式分解为更低次不可约多项式考虑过了，不可能再次出现。则等式成立。

定理 8.8

在 $\mathbb{F}_q[x]$ 中，任意次数 d，存在一个 d 次不可约多项式。

♡

证明 比较定理 1.7 里的等式两边的次数，有

$$q^d = \sum_{d'|d} d' \cdot N(d') \tag{8.37}$$

其中 $N(d')$ 表示 d' 次不可约多项式个数。对次数 d' 使用定理 1.7 可知所有次数整除 d' 的不可约多项式相乘等于 $x^{q^{d'}} - x$，则 $d' \cdot N(d') \le q^{d'}$。则右侧次数有：

$$\le d \cdot N(d) + \sum_{d'|d \wedge d' \neq d} q^{d'}$$

$$\le dN(d) + q^{\frac{d}{2}+1} - q$$

当 $d \ge 2$ 时，$q^d > q^{\frac{d}{2}+1} - q$，则 $dN(d) > 0$ 才能满足上式。即任意次数 d 存在一个不可约多项式。

以上我们证明了，任意质数 p 任意幂次 d 都存在一个大小为 p^d 的有限域且可以通过多项式商掉不可约多项式的主理想得到。

接下来是有限域的一个应用。

定理 8.9

可以高效分解一个域 F 上的多项式 $f \in F[x]$。设 $|F| = q$。

♡

我们给出当域大小是奇数时的算法：

1. 先计算 $\gcd(f, f')$ 找到重因子并去掉。对这些重因子重新调用算法分解。则目前 f 无重因子。
2. 拆分所有不同次数的不可约因子。使用定理 1.7 的式子，从小到大分别把 f 和 $x^{q^d} - x$ 做 gcd 提取同次数的不可约因子。做 gcd 的第一步需要计算 $(x^{q^d} - x) \mod f(x)$，这里考虑把 $f(x)$ 当成模数，用快速幂计算 x^{q^d}。

   那么我们接下来认为 f 的所有不可约因子同次数。
3. 现在 $f = f_1 \cdot f_2 \cdot \ldots \cdot f_k$。我们已知 f 的次数 kd 和每个 f_i 的次数 d。则由中国剩余定理有

   $$F[x]/(f) \cong F[x]/(f_1) \times F[x]/(f_2) \times \ldots \times F[x]/(f_k) \tag{8.38}$$

   那么均匀随机 sample 一个 $g \in F[x]/(f)$ 对应均匀随机一个 $(g_1, g_2, \ldots g_k)$。考虑 $g_1^{q^d-1} = 1$。由 q 为奇数，则 $g_1^{\frac{q^d-1}{2}} = 1 \text{ or } -1$。

   那么我们考虑 sample g 之后计算 $g^{\frac{q^d-1}{2}} + 1$，则每个分量有一半概率为 0，即 $f_i \mid g$。

   则我们重复 sample g 然后计算 $\gcd(f, g^{\frac{q^d-1}{2}} + 1)$，就能把部分因子提取出来。反复尝试差不多就可以提取出来每一个。

第九章 组合计数

9.1 基本计数原理

	公式	例子
加法原理	若 $A \cap B = \varnothing$，则 $\lvert A + B\rvert = \lvert A\rvert + \lvert B\rvert$	选一个学生的方法数 = 在男生中选一个 + 在女生中选一个学生的方法数
乘法原理	若事件 A, B 独立，则总方法数为 $\lvert A\rvert \cdot \lvert B\rvert$	选一男一女学生的方法数 = 在男生中选一个 × 在女生中选一个
阶乘 (Factorial)	$n(n-1)(n-2)\cdots 1 = n!$	共有 $n!$ 种排列方式
排列数	$n(n-1)\cdots(n-k+1) = \dfrac{n!}{(n-k)!}$	从 n 个物体中选 k 个排列
组合数	$\dbinom{n}{k} = \dfrac{n!}{k!(n-k)!}$	二项式系数 (Binomial Coefficient)

9.2 组合数的性质

$$
\begin{aligned}
\binom{n}{k} &= \binom{n}{n-k}, \\
(x+y)^n &= \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}, \\
\binom{n}{k} &= \binom{n-1}{k} + \binom{n-1}{k-1}, \quad \text{直观：选第一个或不选第一个}, \\
\binom{n}{k} &= \frac{n}{k}\binom{n-1}{k-1}, \\
\binom{n}{k} &= \frac{k+1}{n-1}\binom{n}{k+1}.
\end{aligned}
\tag{9.1}
$$

组合数可以用**帕斯卡三角形**表示：

$$
\begin{array}{ccccccc}
 & & & \binom{0}{0} & & & \\
 & & \binom{1}{0} & & \binom{1}{1} & & \\
 & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & \\
\binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3}
\end{array}
$$

9.3 二项式定理的例子

$$
\begin{aligned}
\sum_{k=0}^{n} k\binom{n}{k} &= \sum_{k=0}^{n} k \cdot \frac{n}{k}\binom{n-1}{k-1} \\
&= n\sum_{k=1}^{n} \binom{n-1}{k-1} \\
&= n\sum_{k=0}^{n-1} \binom{n-1}{k} \\
&= n \cdot 2^{n-1}.
\end{aligned}
\tag{9.2}
$$

另一个常见恒等式：

$$\sum_{k=0}^{m}\binom{n+k}{n}=\binom{n+m+1}{n+1} \tag{9.3}$$

证明 一方面，可以直接用数学归纳证明. 另一方面，考虑其组合意义：$n+m$ 个人中需要选出 $m+1$ 个人，左侧和式相当于在枚举最后一个未选中的人是哪个.

9.4 卡特兰数 (Catalan Numbers)

卡特兰数定义为：

$$C_n=\binom{2n}{n}-\binom{2n}{n-1}=\frac{1}{n+1}\binom{2n}{n}. \tag{9.4}$$

例 1 $(0,0)\to(n,n)$ 的，不经过 $x<y$ 部分的最短路径数为 C_n.

证明 总方案数为组合数 $\binom{2n}{n}$.
对于每一个不合法路径，其一定与 $y=x+1$ 有交点. 考虑映射 ϕ，其将不合法路径的第一个与 $y=x+1$ 的交点之前的部分沿 $y=x+1$ 翻转. 容易证明 ϕ 形成了从不合法路径，到 $(-1,1)\to(n,n)$ 路径的双射.
于是不合法路径数为 $\binom{2n}{n-1}$.

$$C_n=\binom{2n}{n}-\binom{2n}{n-1}=\frac{1}{n+1}\binom{2n}{n} \tag{9.5}$$

递推关系：

$$C_n=\sum_{k=1}^{n}C_{k-1}C_{n-k}. \tag{9.6}$$

直观：在 $0+1+2+\cdots+n$ 中插入括号的可能数记为 A_n，则

$$A_n=\sum_{k=0}^{n-1}A_kA_{n-k-1}=\sum_{k=1}^{n}A_{k-1}A_{n-k}. \tag{9.7}$$

9.5 Balls & Bins

n 个桶放 m 个球。

Balls \ Bins	可区分	不可区分
可区分	n^m	$\sum_{i=1}^{n}S_2(m,i)$
不可区分	插板 可有空桶：$\binom{m+n-1}{n-1}$ 无空桶：$\binom{m-1}{n-1}$	$\sum_{k=1}^{n}p(m,k)$ 其中 $p(m,k)=p(m-1,k-1)+p(m-k,k)$

9.6 多项式推广

$$\binom{m}{m_1,m_2,m_3} \tag{9.8}$$

$$(x+y+z)^n=\sum_{i,j}\binom{n}{i,j,n-i-j}x^iy^jz^{n-i-j}. \tag{9.9}$$

9.7 容斥原理 (Inclusion-Exclusion Principle)

$$
\begin{aligned}
|A \cup B| &= |A| + |B| - |A \cap B|, \\
|A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|, \\
\left|\bigcup_{i=1}^{n} A_i\right| &= \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \cdots .
\end{aligned} \tag{9.10}
$$

证明 考虑每个 $x \in \bigcup A_k$ 在右式中的出现次数 f_x

$$f_x = \sum_{T \subseteq [n], T \neq \varnothing} (-1)^{|T|-1} [x \in \bigcap_{k \in T} A_k]$$

注意到只要 $\exists k, x \notin A_k$，求和项就会变成 0. 于是令 S 为 $A_1, \ldots, A_n$ 中所有包含 x 的集合，即 $S = \{i | x \in A_i\}$，于是有

$$f_x = \sum_{T \subseteq S, T \neq \emptyset} (-1)^{|T|-1} = 1 - \sum_{T \subseteq S} (-1)^{|T|} = 1$$

这是因为 $\sum_{T \subseteq S} (-1)^{|T|} = \sum_k (-1)^k \sum_{T \subseteq S, |T|=k} 1 = \sum_k (-1)^k \binom{|S|}{k} = 0.$

9.8 鸽笼原理

例 1. 对于 $S \subseteq [2n]$，$|S| \geq n+1$，则

(a). $\exists i \neq j \in S$，i, j coprime.

证明 令第 i 个 hole 为 $\{2i-1, 2i\}$，则一定存在一个 hole 有两个元素同时在 S，于是互素.

(b). $\exists i \neq j \in S$，$i | j$.

证明 令第 i 个 hole 为 $\{(2i-1) \times 2^k\}$，则一定存在一个 hole 有两个元素同时在 S，这两个元素的商为 2 的幂次.

例 2. 对于序列 $a_1, \ldots, a_n$. 对于 $r \times s < n$，有：要么存在长 $r+1$ 的非升子序列（即 LNIS $> r$），要么存在长 $s+1$ 的非降子序列（即 LNDS $> s$）.

证明 令 r_i 表示 a_i 结尾的最长非降子序列，s_i 表示 a_i 结尾的最长非升子序列.

若 LNIS $\leq r$ 且 LNDS $\leq s$，则 $(r_i, s_i) \in [r] \times [s]$. 则考虑所有的 (r_i, s_i)，由鸽笼原理知一定存在 $i \neq j$ 使得 $(r_i, s_i) = (r_j, s_j)$.

不妨设 $i < j$. 由于 $r_i = r_j$ 所以 $a_i < a_j$. 由于 $s_i = s_j$ 所以 $a_i > a_j$. 矛盾.

例 3. Short-Integer Solution (SIS)：对于 $M \in \mathbb{M}_p^{n \times m}$，令在模 p 意义下 $Mx = 0$ 的一个 SIS 为满足 $x_i \in \{-1, 0, 1\}$ 的解. 证明：$M > n \log P$ 时，SIS 一定存在.

证明 考虑 $\{0,1\}^m \to \mathbb{Z}_p^n$ 的映射，将 x 映成 Mx.

则由鸽笼原理知，存在 $x \neq x' \in \{0,1\}^m$ 使得 $Mx = Mx'$，于是 $M(x - x') = 0$. 故 $x - x'$ 为一个 SIS.

9.9 生成函数

定义 9.1

给定数列 $\{a_n\}_{n=0}^{+\infty}$，定义该数列的 生成函数 **(Generating Function)** 为形式幂级数

$$A(x) = \sum_{n=0}^{+\infty} a_n x^n$$

为方便，若已知形式幂级数 $A(x)$，将其 n 次项系数记作 $[x^n](A(x))$。

我们可以给出一些简单的生成函数的例子：

$$\{1,0,0,0,\dots\} \longleftrightarrow 1$$
$$\{0,0,\dots,\alpha,0,0,\dots\} \longleftrightarrow \alpha x^t (\text{第 } t \text{ 位为 } \alpha)$$
$$\{1,1,1,\dots\} \longleftrightarrow 1+x+x^2+\cdots=\frac{1}{1-x}$$
$$\{1,\alpha,\alpha^2,\dots\} \longleftrightarrow 1+\alpha x+\cdots=\frac{1}{1-\alpha x}$$
$$\{1,0,0,\dots,0,1,0,0,\dots\ 0,\dots\} \longleftrightarrow 1+x^p+x^{2p}+\cdots=\frac{1}{1-x^p} (1 \text{ 出现在 } kp \text{ 位})$$
$$\left\{\binom{k}{n}\right\}_n \longleftrightarrow (1+x)^k$$
$$\left\{\alpha^n\binom{k}{n}\right\}_n \longleftrightarrow (1+\alpha x)^k=\sum_{i=0}^{k}\binom{k}{i}x^i$$
$$\{a_n+b_n\}_n \longleftrightarrow A(x)+B(x)$$
$$\left\{\sum_{i=0}^{n}a_ib_{n-i}\right\}_n \longleftrightarrow A(x)B(x)$$
$$\{\alpha^n a_n\}_n \longleftrightarrow A(\alpha x)$$
$$\alpha_0,0,\alpha_2,0,\alpha_4,0,\cdots \longleftrightarrow \frac{A(x)+A(-x)}{2}$$
$$\{a_1\}\{b_1\} \longleftrightarrow A(x)\,B(x)$$
$$\{0,\alpha_0,\alpha_1,\alpha_2,\alpha_3,\dots\} \longleftrightarrow xA(x) (\text{向右移位})$$
$$\left\{\sum_{i=0}^{n}a_n\right\}_n \longleftrightarrow A(x)\frac{1}{1-x}$$
$$\left\{\binom{n-k+1}{k-1}\right\}_n \longleftrightarrow \frac{1}{(1-x)^k}$$
$$\left\{\alpha^n\binom{n-k+1}{k-1}\right\}_n \longleftrightarrow \frac{1}{(1-\alpha x)^k}$$

注：最后这个式子用来消除所有的奇数项。实际上消除所有 $\bmod n$ 余特定余数的项都能以类似的手段做到。下面是展示乘法公式用途的例子。

- 考虑我们有若干 1 元的硬币，我们需要凑出 n 元钱，将凑钱的方法数以 a_n 记。显然 $a_n=1$，对应的生成函数是 $\frac{1}{1-x}$。
- 如果我们有若干 2 元的纸币，凑法数以 b_n 记，那么 $b_{2n}=1, b_{2n-1}=0$，对应的生成函数是 $\frac{1}{1-x^2}$。
- 现在如果我们有足量的 1 元硬币和 2 元纸币，想要凑出 n 元，那么我们考虑把 n 分成 $i+(n-i)$，用 1 元硬币凑 i 元，2 元纸币凑 $n-i$ 元。于是凑法数就是 $\sum_i a_ib_{n-i}$，这正好与乘法公式对应上，于是此时的生成函数就是前两者的乘积，$\frac{1}{(1-x^2)(1-x)}$。

推而广之，假设我们有：

- ∞ 张 2 元纸币（生成函数 $\frac{1}{1-x^2}$）
- 1 个 1 元硬币（生成函数 $1+x$）
- ∞ 张 5 元纸币（生成函数 $\frac{1}{1-x^5}$）
- 4 张 1 元纸币（生成函数 $1+x+x^2+x^3+x^4=\frac{1-x^5}{1-x}$）

那么就可以把所有生成函数相乘，得到 $\frac{1}{(1-x)^2}$，它的 n 次项系数就是凑出 n 元的方法数。这个结果与直觉相符，相当于拿着无穷多的 1 元硬币和 1 元纸币去凑。

一般地，对于 $\frac{1}{(1-x)^k}$，它的 n 次项系数相当于有序组 $(i_1,\dots,i_k), i_j\ge 0, \sum i_j=n$ 的数量，也即 $\binom{n+k-1}{k-1}$，进而

$$[x^n]\frac{1}{(1-\alpha x)^k}=\alpha^n\binom{n+k-1}{k-1}$$

。

在学习积分时我们知道，所有有理函数总能写成 $R(x)+\sum_i \frac{c_i}{(x-a_i)^{k_i}}$ 的形式，其中 $R(x)$ 是多项式。再利用上面的式子，就可以计算出所有有理函数作为生成函数对应的数列。

下面是 Finonacci 数列的例子。已知 $f_0=1, f_1=1, f_n=f_{n-1}+f_{n-2}$。于是生成函数为：

$$\begin{aligned}
F(x) &= f_0 + f_1 x + f_2 x^2 + f_3 x^3 + \dots \\
&= f_0 + f_1 x + (f_0+f_1)x^2 + (f_1+f_2)x^3 + \dots \\
&= 1 + f_0 x + f_1 x^2 + f_2 x^3 + \dots \\
&\quad + f_0 x^2 + f_1 x^3 + \dots \\
&= 1 + xF(x) + x^2 F(x) \\
\Rightarrow F(x) &= \frac{1}{1-x-x^2} \\
&= \frac{1}{\sqrt{5}}\left(\frac{\alpha_+}{1-\alpha_+ x} - \frac{\alpha_-}{1-\alpha_- x}\right), \alpha_\pm = \frac{1\pm\sqrt{5}}{2}
\end{aligned}$$

这样就能求出 Fibonacci 数列的通项公式 $f_n=(\alpha_+^{n+1}-\alpha_-^{n+1})/\sqrt{5}$。

下面是 Catalan 数的例子，回忆 Catalan 数 C_n 由 $C_0=1, C_n=\sum_{i=0}^{n-1} C_i C_{n-1-i}$ 确定，那么它的生成函数：

$$\begin{aligned}
C(x) &= \sum_n C_n x^n \\
&= 1 + \sum_{n=1}^{\infty}\sum_{i=0}^{n-1} C_i C)n-1-i x^n \\
&= 1 + x\sum_{n=1}^{\infty}\sum_{i=0}^{n-1} C_i C_{n-1-i} x^{n-1} \\
&= 1 + x\sum_{n=0}^{\infty}\sum_{i=0}^{n} C_i C_{n-i} x^n \\
&= 1 + xC(x)C(x)
\end{aligned}$$

于是 $xC^2(x)-C(x)+1=0$，解这个二次方程，舍去在 $x=0$ 处发散的解，得到：

$$\begin{aligned}
C(x) &= \frac{1-(1-4x)^{\frac{1}{2}}}{2x} \\
&= \frac{1}{2x}\left(1-\sum_{n=0}^{\infty}\binom{\frac{1}{2}}{n}(-4x)^n\right) \\
&= \frac{1}{2x}\left(-\sum_{n=1}^{\infty}\binom{\frac{1}{2}}{n}(-4x)^n\right) \\
&= \frac{1}{2x}\left(-\sum_{n=1}^{\infty}\frac{\frac{1}{2}(-\frac{1}{2})\dots(-\frac{2n-3}{2})}{n!}(-1)^n 2^{2n}x^n\right) \\
&= \frac{1}{2x}\left(\sum_{n=1}^{\infty}\frac{(2n-3)!!}{n!}2^n x^n\right) \\
&= \frac{1}{2x}\left(\sum_{n=1}^{\infty}\frac{(2n-2)!}{n!(n-1)!}2x^n\right) \\
&= \sum_{n=1}^{\infty}\frac{(2n-2)!}{n!(n-1)!}x^{n-1} \\
&= \sum_{n=0}^{\infty}\frac{(2n)!}{n!(n+1)!}x^n \\
&= \sum_{n=0}^{\infty}\frac{1}{n+1}\binom{2n}{n}x^n
\end{aligned}$$

还有一个小例子是把 n 个球放到无穷个桶里，球和桶皆不可区分，将桶按照放球的多少排序，可以看出这就是 $(a_1,a_2,\dots),a_i\geq a_{i+1},a_i\geq 0,\sum a_i=n$ 的数量，其生成函数就是

$$\prod_{k=1}^{\infty}\frac{1}{1-x^k}$$

下面考虑生成函数的一种推广，称为指数生成函数：

定义 9.2

给定数列 $\{a_n\}_{n=0}^{\infty}$，定义形式幂级数 $\widetilde{A}(x)=\sum_n \frac{a_n}{n!}x^n$，称为原数列的 指数生成函数 **(Exponential Generating Function)**。

♣

同样先来考虑简单的例子：

$$\begin{aligned}
\{1,1,1,\dots\} &\longleftrightarrow \mathrm{e}^x \\
\{1,\alpha,\alpha^2,\dots\} &\longleftrightarrow \mathrm{e}^{\alpha x} \\
\{0,1,2,3,\dots\} &\longleftrightarrow x\mathrm{e}^x \\
\left\{1,\frac{1}{2},\frac{1}{3},\dots\right\} &\longleftrightarrow \frac{\mathrm{e}^x-1}{x} \\
\{\alpha^n a_n\}_n &\longleftrightarrow \widetilde{A}(\alpha x) \\
\left\{\sum_{i=0}^{n}\binom{n}{i}a_i b_{n-i}\right\}_n &\longleftrightarrow \widetilde{A}(x)\widetilde{B}(x) \\
\{a_1,a_2,\dots\} &\longleftrightarrow \widetilde{A}(x)'
\end{aligned}$$

乘法是由于

$$\begin{aligned}\widetilde{A}(x)\widetilde{B}(x) &= \sum \frac{1}{n!}a_n \frac{1}{m!}b_m x^{m+n} \\ &= \sum \frac{a_n b_m}{n!m!}x^{m+n} \\ &= \sum \frac{1}{(m+n)!}\binom{m+n}{n}a_m b_n x^{m+n}\end{aligned}$$

它的组合意义是说，有 n 个可区分元素，用排列方式 A 排列的方法数为 a_n，用排列方法 B 排列的方法数为 b_n。如果一部分用 A 排列，另一部分用 B，那么方法数数列所对应的指数生成函数就是 $\widetilde{S}(x) = \widetilde{A}(x)\widetilde{B}(x)$。进一步，把这 n 个元素分成若干不相交的子集，每一个内部用排列方式 A 排列，那么方法数所对应的指数生成函数就是 $\widetilde{E}(x) = \exp(\widetilde{A}(x))$，这里规定 $\widetilde{E}(0) = 1, \widetilde{A}(0) = 0$。参见下面的例子：

考虑所有 n 元置换，共有 $n!$ 个，对应到生成函数 $\widetilde{S}(x) = \frac{1}{1-x}$。还可以考虑所有 n-轮换，总共有 $(n-1)!$ 个（相当于排成环的方法数），对应到生成函数 $\widetilde{C}(x) = \sum \frac{1}{n}x^n = \log \frac{1}{1-x}$。那么，$C(x)C(x)/2$ 就相当于把 n 元置换分解成两个轮换，$C(x)C(x)C(x)/6$ 就是分解成三个。以此类推，由于所有置换总能表示成不交轮换的乘积，再规定 $S(0) = 1, C(0) = 0$，就有：

$$S(x) = 1 + C(x) + \frac{C(x)^2}{2!} + \cdots = \exp C(x)$$

根据上面的结果也能检验确实如此。

9.10 Burnside's Lemma

定义 9.3

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g|$$

♣

证明

$$|X/G| = \sum_{x\in X}\frac{1}{|Gx|} = \sum_{x\in X}\frac{Stab(x)}{|G|} \tag{9.11}$$

$$= \sum_{x\in X}\sum_{g\in Stab(x)}\frac{1}{|G|} = \sum_{(x,g)\ s.t.\ g\circ x=x}\frac{1}{|G|} \tag{9.12}$$

$$= \sum_{g\in G}\sum_{x\in X^g}\frac{1}{|G|} \tag{9.13}$$

$$= \sum_{g}\frac{|X^g|}{|G|} \tag{9.14}$$

注

$$G \times X \to X$$

$$X/G = \{Gx | x \in G\}$$

$$orbit(x) = Gx = \{g \circ x | g \in G\}$$

$$|G| = Stab(x) \cdot |Gx|$$

$$Stab_G(x) = \{g | g \circ x = x\}$$

$$X^g = \{x | g \circ x = x\}$$

这个定理对一些蕴含着对称性的计数问题很有帮助。考虑对一条由 4 个珠子组成的项链用两种颜色染色，项

链可以旋转或者翻转，问不同的染色方法数。这里，对项链的旋转或者翻转就对应于二面体群 D_4 对顶点染好色的正方形的作用。D_4 共有八个元素，假设正方形的顶点在坐标轴上，下面逐个计算它们的不动点（在相应的变换下不变的染色方法）：

- 恒等：2^4 个不动点
- 旋转 90°：2 个不动点
- 旋转 180°：2^2 个不动点
- 旋转 270°：2 个不动点
- 绕 x 轴翻转：2^3 个不动点
- 绕 y 轴翻转：2^3 个不动点
- 绕 $y = x$ 翻转：2^2 个不动点
- 绕 $y = -x$ 翻转：2^2 个不动点

于是总方法数为：

$$\frac{1}{8}(16 + 2 + 4 + 2 + 8 + 8 + 4 + 4) = 6$$

9.11 Polya Counting

Polya 计数是对以上方法的进一步发展。令 $F = \{f : X \to C\}$，集合 X 相当于待染色的点集，C 则是颜色集。考虑群作用 $G \times X \to X$（也就相当于指定映射 $G \to \mathrm{Sym}(X)$），这也就同时给出了另一个群作用 $G \times F \to F$，$g * f = f \circ g^{-1}$。用 $c(g)$ 表示 g 所对应的置换的轮换分解中所包含的轮换的个数（包括那些长度为 1 的轮换），那么自然地 $|F^g| = |C|^{c(g)}$（每个轮换所涉及的元素一定同色）。将这个结果代入 Burnside 引理，就有：

定理 9.1 (Polya 计数定理)

$$|F/G| = \frac{1}{|G|}\sum_{g\in G}|C|^{c(g)}$$

♡

下面考虑对一个长度为 n 的项链以 c 种颜色染色，仅允许旋转，不再允许翻转，也就是考虑循环群 $\mathbb{Z}_n$ 的群作用。对于某个 $g \in \mathbb{Z}_n$，它所包含的轮换的长度为 $\mathrm{lcm}(g,n)/g$，于是 $c(g) = n \cdot g/\mathrm{lcm}(g,n) = \gcd(g,n)$。代入 Polya 计数定理，就有：

$$\begin{aligned}
|F/G| &= \frac{1}{n}\sum_{g\in\mathbb{Z}_n} c^{\gcd(g,n)} \\
&= \frac{1}{n}\sum_{d|n}\sum_{\gcd(g,n)=d} c^d \\
&= \frac{1}{n}\sum_{d|n}\sum_{\gcd(\frac{g}{d},\frac{n}{d})=1} c^d \\
&= \frac{1}{n}\sum_{d|n}\varphi\left(\frac{n}{d}\right)c^d
\end{aligned}$$

Polya & GF

用 $c_l(g)$ 表示 $g : X \to X$ 中的长 l 环的个数. 于是 $\sum_l c_l(g) = c(g)$，而 $\sum_l l c_l(g) = |X|$.

我们将 Polya Counting 写成如下的形式. 其中 z_i 为一个生成函数，整个式子当然也得到一个多项式，这个多项式蕴含了一些关于计数的信息（有时被称为“轮换指数多项式”）.

$$|F/G| = \frac{1}{|G|}\sum_g Z_1^{c_1(g)}Z_2^{c_2(g)}\dots$$

回到环染色问题. 我们一个点可以染 c 种颜色，或者不染. 我们希望最终得到的生成函数的 $[z^m]$ 项为有 m 个点不染色的方案数. 则 $Z_i = c + x^i$（Z_i 对应于一个长度为 i 的轮换，轮换中的元素要么同时不染，要么同时染相同的颜色，染相同颜色共有 c 种方式）.

于是在 $n = 4$ 的二面体群作用下，染色方案的生成函数为 $\frac{1}{8}(Z_1^4 + 2Z_4 + 3Z_2^2 + 2Z_2Z_1^2)$，展开即可.

同理，我们还可以这样：我们用三种颜色对上面那个项链染色，用 x，y，z 表示那三种颜色，用多项式的 $x^iy^jz^k$ 项系数表示 i 个珠子用 x 染，j 个珠子用 y 染，k 个珠子用 z 染的方法数。现在对于 Z_i 来说，因为这 i 个珠子只能同色，于是 $Z_i = x^i + y^i + z^i$。仿照上面代入轮换指数多项式，我们同样可以得到有关总方法数的若干信息。

回到 $Z_i = c + x^i$. 如果我们想知道“有多少个方案使得偶数个点没染色”，那么只需要代 $\frac{F(1)+F(-1)}{2}$ 即可.

化学 一卤代烷计数:

解 不考虑立体异构的条件下，n 个碳原子的一卤代烷等价于 n 个点的有根树，且每个点儿子数 ≤ 3. 以 r_n 记满足条件的 n 个节点的有根树的数目，将 r_n 的生成函数记作 $R(x)$。

假如区分每个儿子，那么有 $R(x) = 1 + xR^3(x)$.

但实际上三个儿子是可交换. 于是考虑群作用 $g \in Sym(3)$.

- Z_1 对应于恒等，因此 $Z_1 = R(x)$。
- Z_2 对应于两棵子树的对换，要求这两棵子树完全一样。因此，两棵子树总共有偶数个节点，并且如果有 $2n$ 个子节点，那么每棵子树 n 个子节点，总共有 r_n 种，也就是说 Z_2 的 $2n$ 次项系数为 r_n，故 $Z_2 = r_0 + r_1x^2 + r_2x^4 + \cdots = R(x^2)$。
- 类似地，Z_3 要求三棵完全相同的子树，有 $Z_3 = R(x^3)$。

最终根据 Polya Counting，有

$$R(x) = 1 + \frac{x}{6}(Z_1^3 + 3Z_1Z_2 + 2Z_3) = 1 + \frac{x}{6}(R^3(x) + 3R(x)R(x^2) + 2R(x^3))$$

9.12 共轭类计数

考虑共轭作用 $g \cdot x \to gxg^{-1}$. 我们想关心群的共轭类数量.

$$\#\text{conjugation classes} = \frac{1}{|G|}\sum_g \{x|gxg^{-1} = x\} = \frac{1}{|G|}\sum_g C(g)$$

往年题 F 为有限域，$M_{2\times 2}(F)$ 的相似共轭类数量.

解 用上面的式子，只需要求 $\frac{1}{GL_{2\times 2}(F)}\sum_g C(g)$.

$\sum_g |C(g)| = \{(m, g)|gm = mg\}$. $m = \begin{matrix} a & b \\ c & d \end{matrix}$，$g = \begin{matrix} e & f \\ g & h \end{matrix}$.

那么需要满足条件 $cf = bg$，$ag + ch = ce + dg$，$be + df = bg + dh$，$eh \neq fg$.

推一下得到 $b(e - h) = f(a - d)$，$c(e - h) = g(a - d)$，$cf = bg$，$eh \neq fg$.

分类讨论:

- m 为对角阵或 g 为对角阵，此时方案数小用一下容斥原理得到 $|F||GL| + (|F| - 1)|F|^4 - |F|(|F| - 1)$.
- 上面所有乘积项都不为 0，那么此时只需要 $a - d : b : c = e - h : f : g$，方案数即 $(|GL| - (|F| - 1)) \times (|F| - 1)|F|$

相加得到 $|F|^2 + |F|$.

实际上，F 的标准型如下:

- $diag(\lambda_1, \lambda_2)$，$\lambda_1 \neq \lambda_2$
- $diag(\lambda, \lambda)$
- $\begin{matrix} \lambda & 1 \\ & \lambda \end{matrix}$

- $\begin{matrix} a & 1 \\ -b & \end{matrix}$，其中 x^2+ax+b 不可约.

另一种简便的方法，是用高等代数的知识，等同于有理标准型的计数。能够轻松得到 $|F|^2+|F|$ 的答案.

第十章 概率基础

10.1 概率与随机变量

下面的定义是大家所熟知的：

定义 10.1

给定集合 Ω（称为样本空间）和函数 $\mathbb{P}:\Omega\to\mathbb{R}$，如果满足：

- $\forall\omega\in\Omega,\mathbb{P}(\omega)\geq 0$;
- $\sum_{\omega\in\Omega}\mathbb{P}(\omega)=1$;

则称 $(\Omega,\mathbb{P})$ 是一个概率空间。

♣

定义 10.2

样本空间的子集 $A\subseteq\Omega$ 称为一个事件，其概率定义作 $\Pr[A]=\mathbb{P}(A)=\sum_{\omega\in A}\mathbb{P}(\omega)$。

♣

定义 10.3

给定事件 A,B，条件概率定义为 $\Pr[A|B]=\Pr[AB]/\Pr[B]$，这里 AB 为 $A\cap B$ 的简写。

♣

定理 10.1 (Bayes 公式)

$$\Pr[A|B]=\frac{\Pr[A]\Pr[B|A]}{\Pr[B]}$$

♡

定义 10.4

若 $\Pr[AB]=\Pr[A]\Pr[B]$，则称两个事件独立。等价的说法是 $\Pr[B]=\Pr[B|A]=\Pr[B|\neg A]$

♣

定义 10.5

随机变量指的是定义在样本空间上的函数 $X:\Omega\to S$，它的概率（质量）函数定义为 $P(x)=\Pr[X=x]=\Pr[X(\omega)=x]=\Pr[X^{-1}(x)]=\sum_{\omega\in\Omega,X(\omega)=x}\mathbb{P}(\omega)$。

♣

以上概率的简单定义推广到无穷集合上并不是很容易。这门课并不给出概率的严格定义，但我们还是可以考察一个例子。考虑扔可数次骰子的概率空间。严格化的，令 $\Omega=\{0,1\}^{\mathbb{N}},P:2^{\Omega}\to[0,1]$，以下性质是我们对于“概率”的朴素期待：

- $P(\varnothing)=0,P(\Omega)=1$;
- $S\subseteq T\Rightarrow P(S)\leq P(T)$;
- $\forall i,j,S_i\cap S_j=\varnothing\Rightarrow P(\bigcup_i S_i)=\sum_i P(S_i)$;
- $P(S)=P(S\oplus r)$，这里 $S\oplus r=\{s\oplus r|s\in S\}$ 是一个平移。

很遗憾，这些性质会导致矛盾。将 $a,b\in\{0,1\}^{\mathbb{N}}$ 视作无穷长字符串，定义 $a\sim b\Leftrightarrow a,b$ 在至多有限位上不同。容易看出这是一个等价关系，在每个等价类中取一个代表元组成集合 S。于是，我们有

$$\{0,1\}^{\mathbb{N}}=\bigcup_{r\in\{0,1\}^{\mathbb{N}},r\text{有有限个}1}S\oplus r$$

根据我们期望的可列可加性和平移不变性，$1=P(\Omega)=\sum_r P(S\oplus r)=\sum_r P(S)$，然而这已经导致矛盾：$P(S)$ 无论取何值都不可能使上式成立。这个例子说明我们不能够直接将概率定义在全体子集上面，这就需要来自实变的 $\sigma-$ 代数和可测的概念，在此展开则岔题太远。

10.2 期望，方差和分布

定义 10.6

给定随机变量 X, $P_X(x) = \Pr[X = x]$ 称为 X 的分布。

定义 10.7

给定两个随机变量 X 和 Y，它们的联合分布定义为 $P_{XY}(x, y) = \Pr[X = x \wedge Y = y]$。

相对地，如果已知联合分布 P_{XY}，容易证明

$$P_X(x) = \sum_y P_{XY}(x, y)$$

将其称为**边缘分布**。

定义 10.8

给定两个随机变量 X 和 Y，Y 在 X 下的条件分布（也称为 **Markov** 核）定义为

$$P_{Y|X}(y|x) = \Pr[Y = y|X = x]$$

联合分布，条件分布和边缘分布有基本的转化关系：

$$P_{Y|X}(y|x) = \frac{P_{XY}(x, y)}{P_X(x)}$$

定义 10.9

给定两个随机变量 X 和 Y，如果 $P_{XY}(x, y) = P_X(x)P_Y(y)$，就称 X 和 Y 相互独立。

定义 10.10

给定随机变量 X，其数学期望（或称为均值）定义为 $\mathbb{E}(x) = \sum_x P_X(x)x$。

期望具备基本的线性性质：

定理 10.2

- 若 $X = X_1 + \cdots + X_r$，那么 $\mathbb{E}[X] = \mathbb{E}[X_1] + \ldots \mathbb{E}[X_r]$。
- 若 X 和 Y 相互独立，那么 $\mathbb{E}[XY] = \mathbb{E}[X]\mathbb{E}[Y]$。

需要注意的是，期望的可加性需要小心地推广到无穷。考虑这样的一种游戏：从第一轮开始；到第 k 轮时，投 2^{k-1} 元，等概率地赢或输 2^k 元。如果赢了，立刻停手；否则继续第 $k+1$ 轮。以 X_n 记第 n 轮中获得的钱，那么：

$$X_n = \begin{cases} 2^{n-1}, P = \dfrac{1}{2^n} \\ -2^{n-1}, P = \dfrac{1}{2^n} \\ 0, P = 1 - \dfrac{1}{2^{n-1}} \end{cases}$$

用 X 表示游戏结束时的总钱数，那么 $X = \sum_{n=1}^{\infty} X_n = 1$，进而 $\mathbb{E}[X] = 1$。然而 $\sum_{n=1}^{\infty} \mathbb{E}[X_n] = \sum_{n=1}^{\infty} 0 = 0$，矛盾！

定义 10.11

给定随机变量 X 和事件 A，条件期望定义为：

$$\mathbb{E}[X|A] = \sum_x x \Pr[X = x|A]$$

定理 10.3 (重期望公式)

给定随机变量 X。对于某个随机变量 Y，考虑函数 $f_Y(y) = \mathbb{E}[X|Y = y]$，若引入记号 $\mathbb{E}[X|Y] = f_Y(\cdot)$（这里的 $\mathbb{E}[X|Y]$ 并不是一个“期望”，它其实是一个把随机变量映为随机变量的函数，因而也是一个随机变量），有

$$\mathbb{E}[X] = \mathbb{E}[\mathbb{E}[X|Y]]$$

定义 10.12

给定随机变量 X，其方差定义为

$$Var(X) = \mathbb{E}[(X - \mathbb{E}[X])^2] = \mathbb{E}[X^2] - (\mathbb{E}[X])^2$$

定义 10.13

给定随机变量 X 和 Y，它们的协方差定义为

$$Cov(X, Y) = \mathbb{E}[(X - \mathbb{E}[X])(Y - \mathbb{E}[Y])] = \mathbb{E}[XY] - \mathbb{E}[X]\mathbb{E}[Y]$$

方差只有在独立的条件下才具有可加性，不具有可乘性。

定理 10.4

若随机变量 X 和 Y 独立，那么 $Var(X + Y) = Var(X) + Var(Y)$。

如果 X 服从某个分布，按照分布随机取点 $x_1, \ldots, x_n$，可以由这些点去估计 X 的均值和方差：

- 估计 $\mathbb{E}[X]$：$\dfrac{\sum_i x_i}{n}$
- 估计 $Var(X)$：$\dfrac{n}{n-1}\left(\dfrac{\sum_i x_i^2}{n} - \left(\dfrac{\sum_i x_i}{n}\right)^2\right)$

10.3 概率生成函数

定义 10.14

给定随机变量 X 及其分布 $P_X(x)$。定义形式幂级数

$$G_X(z) = \mathbb{E}[z^X] = \sum_x P_X(x) z^x$$

称为 X 的概率生成函数。

简单的计算给出：

- $G_X(1) = 1$；
- $G'_X(z) = \mathbb{E}[Xz^{X-1}]$，$G'_X(1) = \mathbb{E}[X]$；
- $G''_X(z) = \mathbb{E}[X(X-1)z^{X-2}]$，$G''_X(1) + G'_X(1) = \mathbb{E}[X^2]$。

并且容易看出，如果 X 和 Y 独立，那么

$$G_{X+Y}(z) = G_X(z) G_Y(z)$$

下面的两个例子展示概率生成函数的用处。

其一，掷一颗硬币，正面朝上和反面朝上分别记作 H 和 T，正面朝上的概率为 p，连续出现两个 H 就停止，停止时抛掷的总次数为随机变量 X。如果把 H 写作 pz，T 写作 $(1-p)z$，那么，对于一个序列，例如 THTHH，就对应到一个单项式 $p^3(1-p)^2z^5$，系数是这个序列出现的概率，次数是停止时抛掷的次数。因此，生成函数 $G(z)$ 就是所有的这些项的和。

由于每次掷出 T 后相当于从 0 开始，实际上

$$\begin{aligned} G(z) &= HH + \mathrm{T}G(z) + \mathrm{HT}G(z) \\ &= p^2z^2 + (1-p)zG(z) + (1-p)pz^2G(z) \end{aligned}$$

解出 $G(z)$，我们就获得了关于 X 的很多信息。

其二，设 Y 是一个随机变量，$X_1, \ldots, X_Y$ 独立同分布，研究随机和 $X_1 + \ldots X_Y$。

$$\begin{aligned} G_{\sum X_i}(z) &= \mathbb{E}[z_1^{X_1} \ldots z_Y^{X_Y}] \\ &= \mathbb{E}[\mathbb{E}[z_1^{X_1} \ldots z_Y^{X_Y} | Y]] \\ &= \sum_y P_Y(y)\mathbb{E}[z_1^{X_1} \ldots z_Y^{X_Y} | Y = y] \\ &= \sum_y P_Y(y)\mathbb{E}[z_1^{X_1} \ldots z_y^{X_y}] \\ &= \sum_y P_Y(y)\mathbb{E}[z_1^{X_1}] \ldots \mathbb{E}[z_y^{X_y}] \\ &= \sum_y P_Y(y)\left(G_X(z)\right)^y \\ &= G_Y(G_X(z)) \end{aligned}$$

因此随机和对应的概率生成函数是两者的复合。

特别地，我们可以考虑 $G_X(\mathrm{e}^t) = \mathbb{E}[\mathrm{e}^{tX}]$，那么 $\frac{\mathrm{d}^n}{\mathrm{d}t^n}G_X(\mathrm{e}^t) = \mathbb{E}[X^n\mathrm{e}^{tX}]$，因此代入 $t=0$ 就可以得到 $\mathbb{E}[X^n]$。还可以考虑 $G_X(\mathrm{e}^{it}) = \mathbb{E}[\mathrm{e}^{itX}]$，它的好处是永远收敛。

10.4 一些常见的分布

分布	概率函数	期望	方差	概率生成函数
Bernoulli 分布 $\mathrm{Bern}(p)$	$\begin{cases} 1-p, & x=0 \\ p, & x=1 \end{cases}$	p	$p(1-p)$	$(1-p)+pz$
二项分布 $\mathrm{Binom}(n,p)$	$\binom{n}{x}p^x(1-p)^{n-x}$	np	$np(1-p)$	$(1-p+pz)^n$
均匀分布 $\mathrm{Unif}(\{1,\ldots,n\})$	$\begin{cases} \frac{1}{n}, & x \in \{1,\ldots,n\} \\ 0, & \text{其他} \end{cases}$	$\frac{n+1}{2}$	$\frac{(n+1)(n-1)}{12}$	$\frac{z}{n}\cdot\frac{z^n-1}{z-1}$
几何分布 $\mathrm{Geom}(p)$	$p(1-p)^{x-1}$	$\frac{1}{p}$	$\frac{1-p}{p^2}$	$\frac{pz}{1-(1-p)z}$
负二项分布 $\mathrm{NegBinom}(r,p)$	$\binom{r+x-1}{x}p^r(1-p)^x$	$\frac{r(1-p)}{p}$	$\frac{r(1-p)}{p^2}$	$\left(\frac{p}{1-(1-p)z}\right)^r$
Poisson 分布 $\mathrm{Poisson}(\lambda)$	$\frac{e^{-\lambda}\lambda^x}{x!}$	λ	λ	$e^{\lambda(z-1)}$

注：

- 几何分布指的是进行一系列独立 Bernoulli 试验首次成功时的试验次数，而负二项分布指的是进行一系列独立 Bernoulli 试验，成功 r 次时失败的次数。它们之间有简单的关系，如果 $X \sim \mathrm{NegBinom}(1,\mathrm{p})$，那么

$X+1 \sim \mathrm{Geom}(p)$。

- Poisson 分布可以视为二项分布在 $n \to \infty$ 时的极限。设 $X \sim \mathrm{Binom}(n, \frac{\lambda}{n})$，则

$$\binom{n}{x}\left(\frac{\lambda}{n}\right)^x\left(1-\frac{\lambda}{n}\right)^{n-x} = \frac{\lambda^x}{x!}\left(1-\frac{\lambda}{n}\right)^n \frac{n!}{(n-x)!}\left(\frac{1-\lambda/n}{n}\right)^x \to \mathrm{Poisson}(\lambda)$$

第十一章 信息论 (Information Theory)

11.1 熵 (Entropy)

定义 11.1

对于离散随机变量 X 服从分布 P_X，定义熵

$$H[X] = \sum_x P_X(x) \log \frac{1}{P_X(x)}$$

等价地，熵也可以写成期望形式

$$H[X] = \mathbb{E}_{X\sim P_X}\left[\log \frac{1}{P_X(X)}\right].$$

命题 11.1

$$0 \le H[X] \le \log |X|,$$

其中 $|X| = |\{x \mid P_X(x) > 0\}|$ 为 X 的支撑集大小。

命题 11.2

对于 $X \sim \mathrm{Bern}(p)$，其熵为

$$h(p) = H[X] = p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p}.$$

当 $p = 0.5$ 时，$H[X] = 1$ bit $= \log 2$。

命题 11.3

若 $X \sim \mathrm{Unif}(\Omega)$，则

$$H[X] = \log |\Omega|.$$

11.2 联合熵与条件熵

定义 11.2 (联合熵)

对于随机变量 (X, Y)，定义

$$H[X,Y] = \mathbb{E}_{(X,Y)\sim P_{XY}}\left[\log \frac{1}{P_{XY}(X,Y)}\right].$$

定义 11.3 (条件熵)

对于随机变量 (X, Y)，定义

$$H[Y|X] = \sum_x P_X(x) H[Y|X=x] = \mathbb{E}_{(X,Y)\sim P_{XY}}\left[\log \frac{1}{P_{Y|X}(Y|X)}\right].$$

命题 11.4 (链式法则)

$$H[X,Y] = H[X] + H[Y|X].$$

命题 11.5 (一般化)

$$H[X_1X_2\dots X_n] = H[X_1] + \sum_{i=2}^{n} H[X_i|X_1X_2\dots X_{i-1}]$$

证明 代入定义，会发现就是 $P_{XY}(x,y) = P_X(x)P_{X|Y}(x|y)$ 和 $P_X(x) = \sum_y P_{XY}(x,y)$ 的简单应用。

命题 11.6

$H[X|Y] \le H[X]$。

证明 作差，用 $P_X(x) = \sum_y P_{XY}(x,y)$ 展开 $H[X]$，有：

$$\begin{aligned} H[X] - H[X|Y] &= \sum_x P_X(x) \log \frac{1}{P_X(x)} - \sum_{x,y} P_{XY}(x,y) \log \frac{1}{P_{X|Y}(x|y)} \\ &= \sum_{x,y} P_{XY}(x,y) \log \frac{P_{X|Y}(x|y)}{P_X(x)} \\ &= \sum_{x,y} P_{XY}(x,y) \log \frac{P_{XY}(x,y)}{P_Y(y)P_X(x)} \\ &= \sum_{x,y} P_Y(y)P_X(x) \frac{P_{XY}(x,y)}{P_Y(y)P_X(x)} \log \frac{P_{XY}(x,y)}{P_Y(y)P_X(x)} \end{aligned}$$

利用 $f(x) = x\log x$ 的凸性，使用加权的 Jensen 不等式即可，留意到 $\sum_{x,y} P_{XY}(x,y) = 1$ 和 $\sum_x \sum_y P_X(x)P_Y(y) = \sum_x P_X(x) \sum_y P_Y(y) = 1$。

命题 11.7

$H[X] \ge H[f(X)]$。

证明 由于 $H[X, f(X)] = H[f(X)|X] + H[X]$，而 $f(X)$ 由 X 唯一确定，故条件熵 $H[f(X)|X] = 0$（表达式中的条件概率要么是 0 要么是 1），因此 $H[X] = H[X, f(X)]$。又因为 $H[X, f(X)] = H[f(X)] + H[X|f(X)] \ge H[f(X)]$（条件熵总是非负），所以 $H[X] \ge H[f(X)]$。

11.3 互信息 (Mutual Information)

定义 11.4

定义互信息

$$I(X;Y) = H[X] - H[X|Y] = H[X] + H[Y] - H[X,Y].$$

命题 11.8

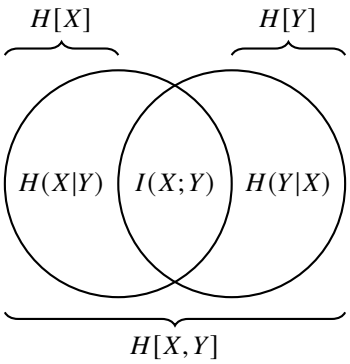
$I(X;Y) \ge 0$。

证明

$$I(X;Y) = \sum_{x,y} P_{XY}(x,y) \log \frac{P_{XY}(x,y)}{P_X(x)P_Y(y)} \ge 0.$$

其不等式成立源自 $f(x) = x\log x$ 的凸性。

以上我们定义过的量可以方便地用 Venn 图表示：



11.3.1 数据处理不等式 (Data-processing inequality)

设 $X \to Y \to Z$ 构成马尔可夫链，即 $P_{XYZ} = P_X P_{Y|X} P_{Z|Y}$。

定理 11.1 (数据处理不等式)

$$I(X;Y) \geq I(X;Z).$$

♡

证明 利用条件熵的凸性与 $P_{X|Z}$ 由 $P_{X|Y}$ 的混合得出，可得

$$H[X|Y] \leq H[X|Z].$$

遂有 $I(X;Y) = H[X] - H[X|Y] \geq H[X] - H[X|Z] = I(X;Z)$。

11.4 KL 散度

定义 11.5 (KL Divergence)

对分布 P, Q，

$$D(P\|Q) = \sum_x P(x) \log \frac{P(x)}{Q(x)} = \mathbb{E}_{x\sim P}\left[\log \frac{P(x)}{Q(x)}\right].$$

若 $\mathrm{supp}(P) \not\subseteq \mathrm{supp}(Q)$，定义 $D(P\|Q) = +\infty$。

♣

命题 11.9

$D(P\|Q) \geq 0$。

♠

证明 利用 $f(x) = x \log x$ 的凸性，Jensen 不等式给出非负性。

命题 11.10

对均匀分布 $\mathrm{Unif}(\Omega)$，

$$D(P\|\mathrm{Unif}(\Omega)) = \log|\Omega| - H(P).$$

♠

11.5 条件散度与链式法则

定义 11.6 (条件 KL 散度)

若 $P_{XY} = P_X P_{Y|X}$、$Q_{XY} = Q_X Q_{Y|X}$，

$$D(P_{XY}\|Q_{XY}) = D(P_X\|Q_X) + D(P_{Y|X}\|Q_{Y|X} \mid P_X).$$

$$D(P_{Y|X}\|Q_{Y|X} \mid P_X) = \mathbb{E}_{(X,Y)\sim P_{XY}}\left[\log \frac{P_{Y|X}(Y|X)}{Q_{Y|X}(Y|X)}\right].$$

命题 11.11 (KL 散度链式规则)

$$D(P_{X_1^n}\|Q_{X_1^n}) = \sum_{i=1}^{n} D(P_{X_i|X_1^{i-1}}\|Q_{X_i|X_1^{i-1}} \mid P_{X_1^{i-1}}).$$

命题 11.12

Bernoulli KL：

$$d(p\|q) = p\log\frac{p}{q} + (1-p)\log\frac{1-p}{1-q}.$$

命题 11.13 (KL 散度为凸函数)

任意分布 P_0, Q_0, P_1, Q_1，任意 $\lambda \in [0,1]$，满足

$$\lambda D(P_0\|Q_0) + (1-\lambda)D(P_1\|Q_1) \geq D(\lambda P_0 + (1-\lambda)P_1\|\lambda Q_0 + (1-\lambda)Q_1)$$

证明 令 $P_X = \lambda P_0 + (1-\lambda)P_1, Q_X = \lambda Q_0 + (1-\lambda)Q_1$，$P_Z = Q_Z = Bern(\lambda)$。

则有 $D(P_{XZ}\|Q_{XZ}) \geq D(P_X\|Q_X)$。

左侧等于

$$\lambda D(P_0\|Q_0) + (1-\lambda)D(P_1\|Q_1)$$

证毕。

命题 11.14

若对同一个分布 P_X，加上两个不同的条件分布 $P_{Y|X}$ 和 $Q_{Y|X}$ 得到 P_Y 和 Q_Y，则有

$$D(P_Y\|Q_Y) \leq D(P_{Y|X}\|Q_{Y|X}|P_X)$$

证明

$$D(P_{Y|X}\|Q_{Y|X}|P_X) = D(P_{XY}\|Q_{XY}) \geq D(P_Y\|Q_Y)$$

命题 11.15 (Data Processing)

两个分布 P_X 和 Q_X，过相同的数据处理 $P_{Y|X}$ 得到 P_Y 和 Q_Y，有

$$D(P_Y\|Q_Y) \leq D(P_X\|Q_X)$$

证明

$$D(P_Y\|Q_Y) \leq D(P_{XY}\|Q_{XY}) = D(P_X\|Q_X) + D(P_{Y|X}\|P_{Y|X}|P_X) = D(P_X\|Q_X)$$