近世代数结构完整体系（带符号解释）

目录

1 基础代数结构体系

1.1 半群 (Semigroup)

定义 1.1 (半群). 非空集合 S 配备一个二元运算 $\cdot : S \times S \to S$，满足：*[注：S 是任意集合，$\cdot$ 是任意运算（比如加法、乘法、矩阵乘法等），$S \times S \to S$ 表示从 S 中取两个元素运算后结果还在 S 中]*

1. **封闭性：** $\forall a, b \in S, a \cdot b \in S$ *[注：$\forall$ 读作"任意"或"所有"，$\in$ 读作"属于"，意思是：对于 S 中任意两个元素 a 和 b，它们运算后的结果 $a \cdot b$ 还在 S 中]*

2. **结合律：** $\forall a, b, c \in S, (a \cdot b) \cdot c = a \cdot (b \cdot c)$ *[注：结合律就是先算哪两个不影响结果，比如 $(1+2)+3 = 1+(2+3)$，注意顺序不能变，只是括号位置变]*

1.2 幺半群 (Monoid)

定义 1.2 (幺半群). 在**半群** $(M, \cdot)$ 的基础上增加：*[注：$(M, \cdot)$ 表示集合 M 配上运算 $\cdot$]*

1. **单位元：** $\exists e \in M, \forall a \in M, e \cdot a = a \cdot e = a$ *[注：$\exists$ 读作"存在"，意思是有一个特殊元素 e，使得 e 与任何元素 a 运算都等于 a 本身。比如加法中的 0，乘法中的 1]*

记为 $(M, \cdot, e)$。

1.3 群 (Group)

定义 1.3 (群). 在**幺半群** $(G, \cdot, e)$ 的基础上增加：

1. **逆元：** $\forall a \in G, \exists a^{-1} \in G, a \cdot a^{-1} = a^{-1} \cdot a = e$ *[注：每个元素 a 都有一个"伙伴" a^{-1}，它们运算后得到单位元 e。比如加法中 3 的逆元是 -3（因为 $3+(-3)=0$），乘法中（除了 0）2 的逆元是 $\frac{1}{2}$（因为 $2 \times \frac{1}{2} = 1$）]*

1.4 阿贝尔群/交换群 (Abelian Group)

定义 1.4 (阿贝尔群). 在群 $(G, \cdot, e)$ 的基础上增加：

1. **交换律**：$\forall a, b \in G, a \cdot b = b \cdot a$ *[注：运算顺序可以交换，比如 $2+3=3+2$，但注意矩阵乘法一般不能交换]*

2 环论体系

2.1 环 (Ring)

定义 2.1 (环). 集合 R 配备两个二元运算 $+$（加法）和 $\cdot$（乘法）满足：*[注：环有两个运算：加法 $+$ 和乘法 $\cdot$，注意这里的 $\cdot$ 不一定是我们平常的乘法，可以是任何定义的运算]*

1. $(R, +)$ 是**阿贝尔群**，其单位元记作 0 *[注：R 配上加法构成一个交换群，有零元 0。注意：这里的 0 不一定是数字 0，而是加法单位元]*
2. $(R, \cdot)$ 是**半群** *[注：R 配上乘法构成半群，但不一定有单位元或逆元]*
3. **分配律**：$\forall a, b, c \in R$，

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c$$

[注：分配律就是乘法对加法的分配，像我们熟悉的 $2 \times (3+4) = 2 \times 3 + 2 \times 4$，但这里环的乘法不一定可交换，所以有两个分配律]

记为 $(R, +, \cdot, 0)$。

2.2 幺环 (Ring with Unity)

定义 2.2 (幺环). 在环 $(R, +, \cdot, 0)$ 的基础上增加：

1. **乘法单位元**：$\exists 1 \in R, \forall a \in R, 1 \cdot a = a \cdot 1 = a$ *[注：有一个元素 1（注意不一定是数字 1）使得任何元素乘 1 都等于自己。比如整数环中 1 就是数字 1，矩阵环中 1 就是单位矩阵]*

记为 $(R, +, \cdot, 0, 1)$。

2.3 交换环 (Commutative Ring)

定义 2.3 (交换环). 在环 $(R, +, \cdot, 0)$ 的基础上，乘法满足交换律：

1. $\forall a, b \in R, a \cdot b = b \cdot a$ *[注：乘法可以交换顺序，比如整数乘法 $2 \times 3 = 3 \times 2$，但矩阵乘法一般不能交换，所以矩阵环不是交换环]*

2.4 交换幺环 (Commutative Ring with Unity)

定义 2.4 (交换幺环). 同时满足**幺环**和**交换环**的条件。*[注：既有乘法单位元 1，乘法又可交换。比如整数环 $\mathbb{Z}$，多项式环 $F[x]$ 等]*

2.5 整环 (Integral Domain)

定义 2.5 (整环). 在**交换幺环** $(R, +, \cdot, 0, 1)$ 的基础上增加：

1. **无零因子**：若 $a \cdot b = 0$，则 $a = 0$ 或 $b = 0$ *[注：零因子就是两个非零元素相乘等于零。比如在 $\mathbb{Z}_6$（模 6 的整数）中，$2 \times 3 = 6 \equiv 0$，所以 2 和 3 是零因子。整环要求没有这种零因子]*

2. $1 \neq 0$（排除平凡环）*[注：排除只有一个元素的环 $\{0\}$，这种环没意思]*

等价地，满足消去律：$a \neq 0$ 且 $a \cdot b = a \cdot c \implies b = c$。*[注：可以像平常一样消去非零因子。比如整数中 $2x = 2y$ 可以消去 2 得 $x = y$]*

2.6 域 (Field)

定义 2.6 (域). 在**交换幺环** $(F, +, \cdot, 0, 1)$ 的基础上增加：

1. **乘法逆元**：$\forall a \neq 0 \in F, \exists a^{-1} \in F, a \cdot a^{-1} = a^{-1} \cdot a = 1$ *[注：除了 0 之外，每个元素都有乘法逆元。比如有理数 $\mathbb{Q}$ 中，2 的逆元是 $\frac{1}{2}$，实数 $\mathbb{R}$ 和复数 $\mathbb{C}$ 也一样。整数 $\mathbb{Z}$ 不是域，因为 2 的逆元 $\frac{1}{2}$ 不是整数]*

2.7 有限域 (Finite Field)

定义 2.7 (有限域). 元素个数有限的**域**。*[注：比如模 p 的整数 $\mathbb{Z}_p$（p 是素数）就是一个有限域，有 p 个元素]*

定理 2.8 (有限域的性质). 有限域的阶必为 p^n（p 为素数）。对每个素数幂 p^n，存在同构意义下唯一的有限域 $GF(p^n)$。*[注：$GF(p^n)$ 表示有 p^n 个元素的有限域，p 是素数，n 是正整数。比如 $GF(2)$ 有 0,1 两个元素，$GF(4)$ 有 4 个元素]*

3 特殊环的层次结构

3.1 欧几里得整环 (Euclidean Domain, ED)

定义 3.1 (欧几里得整环). **整环** R 配备**欧几里得函数** $\varphi : R \setminus \{0\} \to \mathbb{N}_0$ 满足：*[注：$R \setminus \{0\}$ 表示 R 中除了 0 的所有元素，$\mathbb{N}_0$ 表示非负整数 $\{0, 1, 2, 3, \ldots\}$，φ 是一个函数，给每个非零元素赋一个非负整数]*

1. $\forall a, b \neq 0 \in R, \exists q, r \in R : a = bq + r$，其中 $r = 0$ 或 $\varphi(r) < \varphi(b)$ *[注：这就是”带余除法”！a 是被除数，b 是除数，q 是商，r 是余数。余数要么是 0，要么 $\varphi(r) < \varphi(b)$（用 φ 函数衡量大小）]*

2. $\forall a, b \neq 0 \in R, \varphi(a) \leq \varphi(ab)$ *[注：φ 函数满足：一个元素乘上别的元素不会变小。比如整数的绝对值：$|a| \leq |ab|$]*

3.2 主理想整环 (Principal Ideal Domain, PID)

定义 3.2 (主理想整环). **整环** R 中每个**理想**都是主理想（由单个元素生成）。*[注：理想是环的子集，可以理解为环的”倍数集合”。主理想就是由一个元素的所有倍数组成的理想。比如整数环 $\mathbb{Z}$ 中，所有偶数的集合就是由 2 生成的主理想，记作 (2)]*

3.3 唯一分解整环 (Unique Factorization Domain, UFD)

定义 3.3 (唯一分解整环). **整环** R 中每个非零非单位的元素都可唯一分解为不可约元的乘积(在相伴意义下唯一)。*[注：这就是”质因数分解”的推广！不可约元就像质数。唯一分解的意思是:除了顺序和”单位倍”(相伴元)的不同,分解是唯一的。比如整数 $6 = 2\times3 = (-2)\times(-3)$，这算唯一，因为 -2 和 2 是相伴的（差一个单位 -1）]*

定理 3.4 (层次关系).

$$\text{域} \subsetneq ED \subsetneq PID \subsetneq UFD \subsetneq \text{整环} \subsetneq \text{交换幺环} \subsetneq \text{环}$$

[注：$\subsetneq$ 读作”真包含于”，左边的结构比右边的”更特殊”。比如：每个域都是 ED，每个 ED 都是 PID，每个 PID 都是 UFD，等等。但不是反过来都成立。比如整数环 $\mathbb{Z}$ 是 UFD 但不是域]

4 群论核心概念

4.1 子群 (Subgroup)

定义 4.1 (子群). 群 $(G, \cdot, e)$ 的子集 H，在 G 的运算下也构成群。*[注：H 是 G 的一部分，并且 H 自己用同样的运算也构成群。比如整数加法群 $\mathbb{Z}$ 中，所有偶数构成的集合就是子群]*

判定： $H \neq \emptyset$，且 $\forall a, b \in H, ab^{-1} \in H$。[注：检查子群的简便方法：$H$ 非空，且对任意 $a, b \in H$，有 $ab^{-1} \in H$。注意 b^{-1} 是 b 在群 G 中的逆元]

4.2 正规子群 (Normal Subgroup)

定义 4.2 (正规子群). 子群 $N \leq G$ 满足 $\forall g \in G, gN = Ng$，记作 $N \trianglelefteq G$。*[注：$gN = \{g \cdot n \mid n \in N\}$ 是 N 的左陪集，$Ng = \{n \cdot g \mid n \in N\}$ 是右陪集。正规子群就是左右陪集相等的子群。注意 $\trianglelefteq$ 是正规子群的符号]*

4.3 商群 (Quotient Group)

定义 4.3 (商群). 对正规子群 $N \trianglelefteq G$, 定义 $G/N = \{gN \mid g \in G\}$, 运算 $(aN)(bN) = abN$。*[注：商群就是把 G 分成 N 的陪集，然后陪集之间可以运算。比如整数 $\mathbb{Z}$ 模 n 的剩余类群 $\mathbb{Z}/n\mathbb{Z}$]*

4.4 群同态与核 (Homomorphism & Kernel)

定义 4.4 (群同态). 映射 $\varphi : G \to H$ 满足 $\varphi(ab) = \varphi(a)\varphi(b)$。*[注：$\varphi$ 把 G 的元素映射到 H，并且保持运算结构。比如 G 和 H 都是加法群时，$\varphi(a+b) = \varphi(a) + \varphi(b)$]*

定义 4.5 (核与像).

- $\ker \varphi = \{g \in G \mid \varphi(g) = e_H\}$ *[注：核是映射到 H 的单位元的那些 G 中元素的集合]*
- $\operatorname{im} \varphi = \{\varphi(g) \mid g \in G\}$ *[注：像是 φ 映射得到的所有结果的集合]*

5 核心定理

5.1 拉格朗日定理 (Lagrange's Theorem)

定理 5.1 (拉格朗日定理). 有限群 G 的子群 H 的阶整除 G 的阶：

$$|G| = |H| \cdot [G : H]$$

[注：$|G|$ 读作"G 的阶"，就是 G 中有多少个元素。$[G : H]$ 读作"G 对 H 的指数"，就是 H 在 G 中的陪集个数。比如 G 有 12 个元素，H 有 3 个元素，那么 $[G : H] = 4$] 其中 $[G : H]$ 是 H 在 G 中的指数。

5.2 凯莱定理 (Cayley's Theorem)

定理 5.2 (凯莱定理). 每个群都同构于一个对称群的子群。特别地，$|G| = n \implies G \hookrightarrow S_n$。*[注：$S_n$ 是 n 个元素的对称群（所有置换构成的群）。$\hookrightarrow$ 表示"嵌入"，就是同构于某个子群。意思是任何抽象群都可以看成置换群]*

5.3 同态基本定理

定理 5.3 (同态基本定理). 设 $\varphi : G \to H$ 是群同态，则

$$G/\ker \varphi \cong \operatorname{im} \varphi$$

[注：$G/\ker \varphi$ 是商群，$\cong$ 表示同构（结构相同）。这个定理是说：商群 $G/\ker \varphi$ 与像 $\operatorname{im} \varphi$ 结构完全一样]

5.4 欧拉函数 (Euler's Totient Function)

定义 5.4 (欧拉函数). $\varphi(n) = |\{1 \le k \le n \mid \gcd(k,n) = 1\}|$ *[注：$\varphi(n)$ 是从 1 到 n 中与 n 互质的数的个数。$\gcd(k,n)$ 是 k 和 n 的最大公约数，$\gcd(k,n) = 1$ 表示互质。$|\{\cdots\}|$ 表示集合中元素的个数]*

定理 5.5 (欧拉函数的性质).

1. 若 p 为素数,则 $\varphi(p) = p-1$ *[注：质数 p 与 $1, 2, \ldots, p-1$ 都互质，所以 $\varphi(p) = p-1$]*
2. 若 $\gcd(m,n) = 1$，则 $\varphi(mn) = \varphi(m)\varphi(n)$ *[注：$\gcd(m,n) = 1$ 表示 m 和 n 互质，这时欧拉函数是乘性的]*
3. $\varphi(p^k) = p^{k-1}(p-1)$ *[注：p^k 的欧拉函数公式。比如 $\varphi(8) = \varphi(2^3) = 2^{3-1}(2-1) = 4$，确实 $1, 3, 5, 7$ 这四个数与 8 互质]*

6 重要旁支定义

6.1 理想 (Ideal)

定义 6.1 (理想). 环 R 的子集 I 满足：

1. $(I, +)$ 是 $(R, +)$ 的子群 *[注：I 配上加法是 R 的加法子群]*
2. $\forall r \in R, a \in I : ra \in I$ 且 $ar \in I$（双边理想）*[注：I 吸收乘法：R 中任何元素乘 I 中元素还在 I 中。注意如果只要求 $ra \in I$ 叫左理想，只要求 $ar \in I$ 叫右理想，两个都要求叫双边理想]*

6.2 素理想与极大理想

定义 6.2 (素理想). 环 R 的理想 $P \neq R$ 称为素理想，若 $ab \in P \implies a \in P$ 或 $b \in P$。*[注：素理想就像质数：如果乘积在理想中，那么至少有一个因子在理想中]*

定义 6.3 (极大理想). 环 R 的理想 $M \neq R$ 称为极大理想，若不存在理想 I 满足 $M \subsetneq I \subsetneq R$。*[注：极大理想就是不能再"扩大"的理想（除了扩大到整个环 R）。$\subsetneq$ 表示真包含，就是严格包含]*

定理 6.4 (理想与商结构). 设 I 是环 R 的理想，则：

1. R/I 是整环 $\iff$ I 是素理想 *[注：商环 R/I 是整环当且仅当 I 是素理想]*
2. R/I 是域 $\iff$ I 是极大理想 *[注：商环 R/I 是域当且仅当 I 是极大理想。注意：域一定是整环，所以极大理想一定是素理想]*

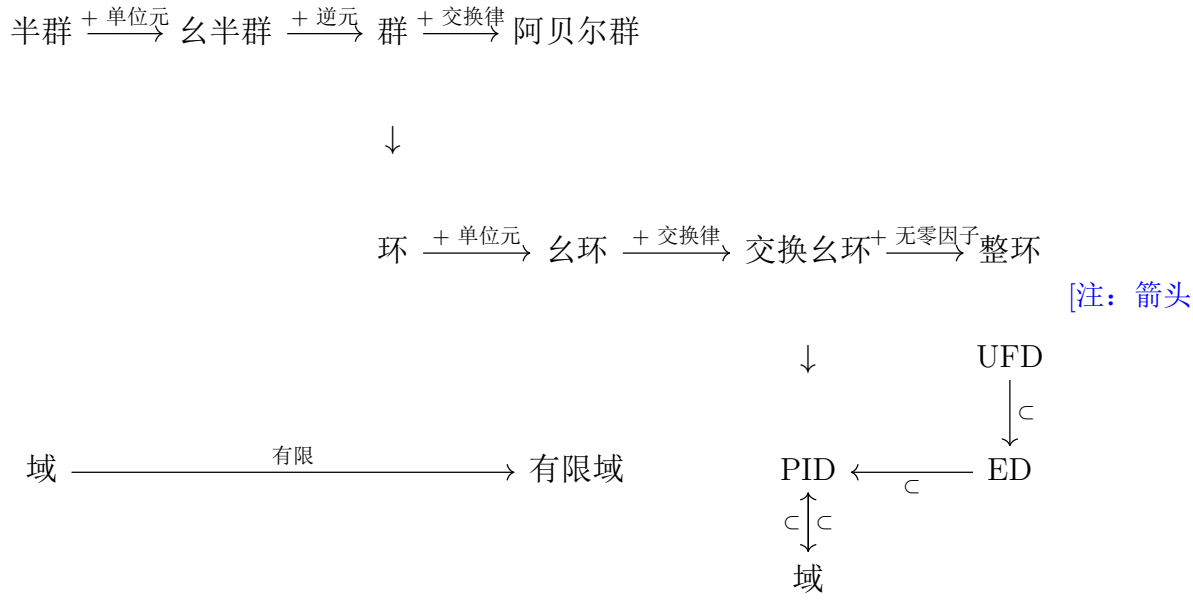
6.3 环同态基本定理

定理 6.5 (环同态基本定理). 设 $\varphi : R \to S$ 是环同态，则

$$R/\ker\varphi \cong \operatorname{im}\varphi$$

[注：和群同态基本定理类似：商环 $R/\ker\varphi$ 同构于像 $\operatorname{im}\varphi$]

7 逻辑关联图



[注：箭头表示" 增加条件得到"，$\subset$ 表示包含关系。比如：每个域都是 ED，每个 ED 都是 PID，等等]

8 常用符号速查表

- $\forall$ - 读作" 任意" 或" 所有"，英文 for all
- $\exists$ - 读作" 存在"，英文 there exists
- $\in$ - 读作" 属于"，英文 element of，如 $a \in S$ 表示 a 在集合 S 中
- $\notin$ - 读作" 不属于"
- $\subseteq$ - 读作" 包含于"（可能相等）
- $\subsetneq$ 或 $\subset$ - 读作" 真包含于"（严格包含）
- $\emptyset$ - 空集，没有元素的集合
- $\mathbb{Z}$ - 整数集 $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$
- $\mathbb{Q}$ - 有理数集（所有分数）

- $\mathbb{R}$ - 实数集
- $\mathbb{C}$ - 复数集
- $\mathbb{N}$ - 自然数集，通常是 $\{0, 1, 2, \ldots\}$ 或 $\{1, 2, 3, \ldots\}$（看定义）
- $F[x]$ - 系数在域 F 中的多项式集合
- a^{-1} - a 的逆元
- e - 单位元（群）
- 0 - 零元（环的加法单位元）
- 1 - 幺元（环的乘法单位元）
- $f : A \to B$ - 从 A 到 B 的函数/映射
- ker - 核（kernel），映射到单位元的那些元素
- im - 像（image），映射得到的所有结果
- $\cong$ - 同构，表示两个结构完全一样
- $\simeq$ - 同伦或弱等价
- $\approx$ - 近似等于
- $\neq$ - 不等于
- $\equiv$ - 恒等于或同余

9 总结规律

1. **结构扩展规律**：每个新结构都是在旧结构上增加公理条件
2. **群 $\to$ 环**：环 = 加法群 + 乘法半群 + 分配律
3. **整环 $\to$ 域**：域 = 整环 + 非零元可逆
4. **分解层次**：ED $\to$ PID $\to$ UFD 逐步放宽分解条件
5. **商结构**：需要” 正规” 条件保证运算良定义（群需正规子群，环需理想）