COURSE NOTES Fall 2024

抽象代数 I

Abstract Algebra I

Runkun Liu

Nankai University

目录

记号约定 **ii**

第一章 群 **1**

1.1 半群与群 1
1.2 子群与陪集 4
1.3 正规子群与商群 6
1.4 群的同态与同构 8
1.5 循环群 11
1.6 对称群与交错群 12
1.7 群的扩张与 Jordan–Hölder 定理 14
1.8 可解群和幂零群 18
1.9 群在集合上的作用 21
1.10 Sylow 定理 24
1.11 本章小结 26

第二章 环 **27**

2.1 环的定义与基本性质 27
2.2 理想与商环 29
2.3 四元数体 30
2.4 环的同态 32
2.5 整环上的因子分解 34
2.6 素理想与极大理想 36
2.7 主理想整环与欧几里得环 37
2.8 环上的多项式 38
2.9 整环上的多项式环 41
2.10 对称多项式 44
2.11 本章小结 45

常用条件与结论速查 **47**

记号约定

$\mathbb{N}=\{0,1,2,\ldots\}$，$\mathbb{N}^*=\{1,2,\ldots\}$；$\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ 分别为整数、有理数、实数与复数。映射复合从右往左作用：$fg=f\circ g$。$\cong$ 表示相应代数结构的同构。

记号	含义与约定
e，1，$\{e\}$	群的幺元通常记为 e；短正合序列和群列中也用 1 表示平凡群。
$\lvert G\rvert$，$\lvert a\rvert$	群的阶，以及群元素 a 的阶。
$H<G$，$N\trianglelefteq G$	H 为子群，允许 $H=G$；N 为正规子群。真包含用 $\subsetneq$ 或文字注明。
$\langle S\rangle$，$\langle a\rangle$	由集合 S、或元素 a 生成的子群。
G/H，$[G:H]$	左陪集集合及其基数。只有 $H\trianglelefteq G$ 时，G/H 才带有自然的商群结构。
$C(G)$，$C_G(a)$	群的中心，以及元素 a 的中心化子；两者不要混淆。
C_a，$N_G(H)$	a 的共轭类，以及子群 H 的正规化子。
O_x，F_x	群作用中 x 的轨道与迷向子群。
$G^{(i)}$，G^i，$C_i(G)$	导出列、降中心列、升中心序列的项；起点分别为 $G^{(0)}=G$、$G^1=G$、$C_0(G)=1$。
$\operatorname{Ker} f$，$\operatorname{Im} f$	同态的核与像；群同态的核是 e 的原像，环同态的核是 0 的原像。
$\operatorname{Aut}(G)$，$\operatorname{Inn}(G)$	自同构群与内自同构群。
S_n，A_n，K_4	对称群、交错群、Klein 四元群。置换中右边的轮换先作用。
$U(R)$，R^*	幺环的单位群；$R^*=R\setminus\{0\}$。一般环中二者未必相同。
(S)，(a)，(a,b)，R/I	生成理想、主理想、二生成理想、商环。“理想”未加限定时指双边理想。
$a\sim b$，$\gcd(a,b)$	在整环的分解理论中分别表示相伴、最大公因子；最大公因子只在相伴意义下唯一。
$\operatorname{Ch} R$，$\mathbb{Z}_m$	无零因子环的特征；$\mathbb{Z}/m\mathbb{Z}$。后者随语境视为群或环。
$R[x_1,\ldots,x_n]$，$c(f)$	多项式环；UFD 上非零多项式的容度。零多项式的次数约定为 $-\infty$。

环不默认交换或有幺元；环同态也不默认保持幺元。整环则是非零的无零因子交换幺环。正文中“单位”指可逆元，“幺元”指乘法恒等元。$\mathrm{GL}(n,P)$ 与 $\mathrm{SL}(n,P)$ 分别表示可逆矩阵群与行列式为 1 的矩阵群。

矩阵统一作用在列向量上：$A=(a_{ij})$ 的第 j 列记录第 j 个基向量的像，第 i 行给出第 i 个坐标。若 T 把旧坐标变成新坐标，换基后矩阵为 TAT^{-1}，详见例 1.4.3。记号 $\operatorname{Hom}(G)$ 在本笔记中专指 G 的自同态全体，运算是映射复合；线性空间的自同态仍记为 $\operatorname{End} V$。

第一章

群

我们在线性代数中已经反复使用可逆矩阵：两个可逆矩阵相乘仍可逆，矩阵乘法满足结合律，单位矩阵不改变向量，而逆矩阵可以解开方程 $Ax = b$。如果暂时不关心矩阵的具体条目，只保留这些运算规则，还能证明什么？群的概念从这里开始。

本章先研究子群以及怎样把若干元素合成一个新的元素，再用同态说明这种合并与映射之间的关系。之后，我们一方面考察循环群和置换群，另一方面尝试借助正规子群逐层分解有限群。到最后，群作用会把抽象群变成集合上的置换，使我们能够用轨道计数证明 Sylow 定理，并据此寻找正规子群。

1.1 半群与群

先看两个熟悉的方程。在整数中，$a + x = b$ 总能用 $x = b - a$ 解出；在可逆矩阵中，$AX = B$ 总能用 $X = A^{-1}B$ 解出。这里的做法相似：先找到能抵消 a 或 A 的元素，再把它作用到等式两边。我们想把这种做法写成不依赖整数或矩阵的共同规则。

不过，并不是每一种运算都允许这样做。正整数的加法不能解出 $2 + x = 1$，矩阵乘法也不能约去一个不可逆矩阵。因此我们先只要求运算能进行、能连续进行，再依次加入幺元和逆元，看看它们各自解决什么问题。首先，运算两个元素后得到的结果还应属于原集合。

定义 1.1.1 (二元运算与运算律)**.** 非空集合 S 上的二元运算是映射 $S \times S \to S$，记作 $(a, b) \mapsto ab$。结合律与交换律分别指

$$(ab)c = a(bc), \qquad ab = ba \quad (a, b, c \in S).$$

若还有加法，则乘法对加法的左、右分配律为

$$a(b + c) = ab + ac, \qquad (b + c)a = ba + ca.$$

结合律只允许改变括号，并不允许交换因子的先后次序。例如矩阵乘法满足结合律，却一般没有 $AB = BA$。有了结合律，abc 就有确定含义；如果再有一个像加法中的 0、矩阵乘法中的 I 那样不改变其他元素的元素，就可以谈论下面的幺半群。

定义 1.1.2 (半群与幺半群)**.** 具有结合律的二元运算的非空集合称为半群。若 $ea = a$ 对所有 a 成立，称 e 为左幺元；若 $ae = a$，称为右幺元。兼为两者的元素称为幺元；有幺元的半群称为幺半群。运算可交换时，相应称交换半群或交换幺半群。

在有幺元的情形，我们可以问一次运算是否能被撤销。这将把可逆矩阵的想法推广到一般运算。

定义 1.1.3 (逆元). 在幺半群 S 中，若 $ba = e$，称 b 为 a 的左逆元；若 $ab = e$，称为右逆元。若两式同时成立，称 b 为 a 的逆元，并称 a 为可逆元。

左右条件一旦同时成立，幺元和逆元就不再有选择的余地；这保证了后面的记号有确定含义。

命题 1.1.4 (幺元与逆元的唯一性). 左幺元与右幺元同时存在时必相等。一个元素的左、右逆元同时存在时也必相等。因此幺元及可逆元的逆元唯一。

证明. 若 e_l, e_r 分别为左、右幺元，则 $e_l = e_l e_r = e_r$。若 $ba = e$、$ac = e$，则 $b = b(ac) = (ba)c = c$。 □

下面几类例子说明：结构取决于集合上的运算，不能只看集合本身。

例 1.1.5 (从熟悉的运算出发).

1. $\mathbb{N}^*$ 对加法是半群，对乘法是幺半群；前者没有幺元。
2. 非空集合 X 的全体变换 $M(X)$ 对复合是幺半群，幺元为 id_X；线性空间的 $\mathrm{End}\, V$ 是其中保持线性结构的例子。
3. 幂集 $\mathcal{P}(X)$ 对并、交分别是交换幺半群，幺元分别为 $\varnothing, X$。

如果所有元素都可以撤销，乘法方程就有了统一的解法。我们把这类幺半群单独提出。

定义 1.1.6 (群). 每个元素都可逆的幺半群称为群；运算可交换时称为交换群或 Abel 群。群 G 的基数 $|G|$ 称为阶；只有一个元素的群称为平凡群。逆元记为 a^{-1}。

验证群时不必分别检查左右两套条件，但同一侧的幺元和逆元必须配合使用。

定理 1.1.7 (群的单侧判别). 半群 G 是群，当且仅当存在左幺元 e，且每个 $a \in G$ 都有相对于 e 的左逆元。

证明. 必要性由群的定义得到。反过来，我们已经有 $ea = a$ 和一个左逆 b，即 $ba = e$；缺少的是 $ab = e$ 与 $ae = a$。不能直接在 $ba = e$ 两边消去，因为消去律还没有证明。

条件对每个元素都成立，所以可以再给 b 取一个左逆 c，使 $cb = e$。于是

$$a = ea = (cb)a = c(ba) = ce.$$

把这个表达式代入 ab，得到 $ab = (ce)b = c(eb) = cb = e$。这就把 b 的左逆性质变成了双侧逆性质。最后

$$ae = a(ba) = (ab)a = ea = a,$$

所以 e 也是右幺元，G 是群。 □

这里不能把条件随意换成“左幺元和右逆元”。例如在至少含两个元素的集合上定义 $ab = b$，则运算结合，每个元素都是左幺元；固定其中一个 e，又有 $ae = e$，所以每个元素都有相对于 e 的右逆元，但它不是群。

有了逆元，我们才能合法地约去等式中的因子。

引理 1.1.8 (消去律)**.** 群中 $ab = ac$ 或 $ba = ca$ 均推出 $b = c$。

证明. 分别左乘或右乘 a^{-1} 即得。 □

逆元已经给出了乘法方程的解。反过来，如果只知道两类方程总能求解，能否从这些解中构造出幺元和逆元?

命题 1.1.9 (用方程刻画群)**.** 半群 G 是群，当且仅当对任意 $a, b \in G$，方程 $ax = b$ 与 $ya = b$ 均有解。在群中，这些解唯一，分别是 $a^{-1}b$ 与 ba^{-1}。

证明. 在群中，左乘 a^{-1} 或右乘 a^{-1} 就得到所列解，消去律保证唯一性。

反过来，此时尚未给出幺元，要先从方程的可解性中找出一个。固定 $a_0 \in G$，解 $ya_0 = a_0$，把一个解记为 e。我们只知道 $ea_0 = a_0$，还需证明 e 对所有元素都起同样作用。任取 $b \in G$，由 $a_0c = b$ 可解，写成 $b = a_0c$，便有

$$eb = e(a_0c) = (ea_0)c = a_0c = b.$$

所以 e 是左幺元。再对任意 a 解 $ya = e$，便得到相对于同一个 e 的左逆元。定理 1.1.7 于是给出结论。 □

仅有消去律一般不能保证方程有解。不过，集合有限时，乘一个固定元素所给出的单射自动是满射，因而情况不同。

命题 1.1.10 (有限消去半群)**.** 非空有限半群若满足左右消去律，则是群。

证明. 固定 a，映射 $x \mapsto ax$ 和 $x \mapsto xa$ 均为有限集上的单射，因而为满射；应用命题 1.1.9。有限性不能省略，例如 $(\mathbb{N}, +)$ 满足消去律，却不是群。 □

最后回到一般幺半群。虽然其中未必每个元素都可逆，我们可以只取可逆元；要让它们组成群，关键是验证两个可逆元的乘积仍可逆。

命题 1.1.11 (可逆元群)**.** 幺半群 S 中的可逆元全体 $U(S)$ 构成群，并且

$$(ab)^{-1} = b^{-1}a^{-1}, \qquad (a^{-1})^{-1} = a.$$

证明. 先检查可逆元相乘仍可逆。对 $a, b \in U(S)$，有

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = e, \qquad (b^{-1}a^{-1})(ab) = e.$$

因此 $ab \in U(S)$，并得到逆序的求逆公式。e 属于 $U(S)$，而 a^{-1} 的逆就是 a，所以求逆也不离开 $U(S)$。结合律从 S 继承，群的条件全部满足。 □

例 1.1.12 (对称群与一般线性群)**.** $U(M(X))$ 是 X 上所有双射组成的对称群 S_X。当 $X = \{1, \dots, n\}$ 时记为 S_n。$U(\operatorname{End} V) = \mathrm{GL}(V)$；取基后得到可逆矩阵群 $\mathrm{GL}(n, P)$。此外，$(\mathbb{Z}, +)$、向量空间的加法群以及数域 P 的乘法群 $P^* = P \setminus \{0\}$ 都是群。

这样，同一个幺半群中即使有不可逆元素，我们仍能把可逆的部分取出来组成群。可逆矩阵群与对称群都是用这个办法得到的。接下来我们再问：在一个已经给定的群中，哪些更小的子集也能独立进行这些运算?

1.2 子群与陪集

在线性空间中，子空间的向量仍能相加、取负、作数乘，因此可以把子空间本身当作线性空间研究。群中也有同样的问题：取出一个子集后，乘法与求逆会不会把元素带到这个子集之外？如果不会，就不必重新证明所有群公理。

有了这样的子群 H，我们还想把只相差一个 H 中元素的群元素归在一起。例如在 $\mathbb{Z}$ 中取 $m\mathbb{Z}$，就会得到按模 m 的余数分类。本节先完成这种分类；至于这些类别之间能否继续相乘，要留到下一节检查。

定义 1.2.1 (子群与生成子群)**.** 非空子集 $H \subseteq G$ 对原运算构成群时，称 H 为 G 的子群，记为 $H < G$。$\{e\}, G$ 称平凡子群；$H \neq G$ 时称真子群。对 $S \subseteq G$，包含 S 的最小子群称为 S 生成的子群，记为 $\langle S\rangle$。有有限生成组的群称有限生成群。

子群中的结合律已由原群保证，实际需要检查的是封闭性。

定理 1.2.2 (子群判别法)**.** 对非空子集 $H \subseteq G$，以下三条件等价：$H < G$；H 对乘法和求逆封闭；对任意 $a, b \in H$ 有 $ab^{-1} \in H$。

证明. 若 H 本身是群，它的幺元 e_H 满足 $e_H h = h$。在 G 中右乘 h^{-1}，可知 $e_H = e$；再由逆元唯一性，H 中的逆元也是 G 中的逆元。因此子群必对乘法、求逆封闭，进而对 ab^{-1} 封闭。

反过来，假设第三个条件成立。非空性让我们先取 $a \in H$，从而 $e = aa^{-1} \in H$。于是对任意 $b \in H$，有 $b^{-1} = eb^{-1} \in H$；对任意 $a, b \in H$，再把 b^{-1} 放进第三个条件，得到 $ab = a(b^{-1})^{-1} \in H$。幺元、逆元和乘积都已留在 H 中，结合律则从 G 继承，所以 H 是子群。这也说明第二个条件足以保证子群性。 □

给定一些元素 S，要得到包含它们的子群，我们必须加入它们的逆元，再加入所有有限乘积。除此之外，没有必要强迫加入别的元素。另一方面，所有包含 S 的子群的交仍是子群，因为每个子群都对乘法和求逆封闭。于是可以从这两个方向写出同一个最小子群：

$$\langle S\rangle = \bigcap_{S \subseteq H < G} H = \{s_1^{\varepsilon_1} \cdots s_r^{\varepsilon_r} : r \geq 0,\ s_i \in S,\ \varepsilon_i = \pm 1\}.$$

空乘积取为 e。右边对乘法、求逆封闭，且包含在每个含 S 的子群中，这就证明了等式。

只有一个生成元时，群元素可以用整数指数记录；这也给出元素自身的大小指标。

定义 1.2.3 (元素的阶)**.** 规定 $a^0 = e$、$a^{-n} = (a^{-1})^n$，则 $a^m a^n = a^{m+n}$。$\langle a\rangle$ 的阶称为 a 的阶。若此阶有限，它等于满足 $a^n = e$ 的最小正整数 n；否则称 a 为无限阶元。

这里为什么能用最小正整数 n 表示 $\langle a\rangle$ 的大小？若 $a^n = e$，带余除法把任意整数 m 写成 $m = qn + r$，$0 \leq r < n$，所以 $a^m = a^r$。而 $e, a, \ldots, a^{n-1}$ 互不相同，否则两个相同的幂相除，就会得到更小的正整数使 $a^k = e$。若不存在这样的 n，同样的相除说明所有整数次幂互不相同，故生成的子群无限。

例 1.2.4 (矩阵子群与整数子群). 线性空间的子空间是其加法群的子群；$\mathrm{SL}(V) < \mathrm{GL}(V)$，正交群保持实内积，酉群保持复 Hermitian 内积，辛群保持非退化交错双线性型。保持同一种形式的可逆变换对复合与求逆封闭，所以它们也分别组成子群。可逆对角矩阵、可逆上三角矩阵、对角元为 1 的上三角矩阵也分别构成子群。
$\mathbb{Z}$ 的每个子群都形如 $m\mathbb{Z}$（$m \in \mathbb{N}$）：非零子群中取最小正整数 m，带余除法说明其中每个整数都是 m 的倍数。特别地，有限生成不等于有限，$\mathbb{Z} = \langle 1 \rangle$ 就是反例。

我们希望把“相差一个 H 中元素”看作同一类。由于乘法可能不交换，必须区分左右。

定义 1.2.5 (陪集). 对 $H < G$、$a \in G$，集合 $aH = \{ah : h \in H\}$ 与 $Ha = \{ha : h \in H\}$ 分别称为 H 的左、右陪集。左陪集全体记为 G/H，其基数记为 $[G : H]$，称为指数。

要把陪集当作一类对象，先要知道它们确实把 G 分开，且代表元可以更换。

引理 1.2.6 (陪集判别). $aH = bH$ 当且仅当 $a^{-1}b \in H$；两个左陪集要么相等，要么不交。每个陪集中的任一元素都可作代表元。

证明. 若 $b = ah$，则 $bH = aH$；反之 $b \in aH$ 给出 $a^{-1}b \in H$。若 $x \in aH \cap bH$，则 $aH = xH = bH$。 □

矩阵的左右乘法有不同效果，因此左右陪集也确实可能不同。

例 1.2.7 (左右陪集不必相等). 在 $\mathrm{GL}(2, \mathbb{C})$ 中，令 T 为可逆对角矩阵组成的子群，$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$。则

$$AT = \left\{ \begin{pmatrix} a & b \\ 0 & b \end{pmatrix} : a, b \in \mathbb{C}^* \right\},$$

$$TA = \left\{ \begin{pmatrix} a & a \\ 0 & b \end{pmatrix} : a, b \in \mathbb{C}^* \right\}.$$

例如 $\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$ 属于 AT，却不属于 TA，所以两者不相等。这与右乘对角矩阵缩放各列、左乘对角矩阵缩放各行的差别一致。另一方面，取逆给出左陪集与右陪集之间的双射 $gT \mapsto Tg^{-1}$，故左右陪集的个数始终相同。

陪集体现了一个更一般的构造：先规定哪些元素应视为等价，再把每一类当作一个新元素。

定义 1.2.8 (等价关系与商集合). 集合 A 上的关系是 $A \times A$ 的子集。满足反身性、对称性和传递性的关系称等价关系。$\bar{a} = \{b : b \sim a\}$ 称等价类；所有等价类组成商集合 $A/\!\sim$。映射 $\pi : A \to A/\!\sim$，$a \mapsto \bar{a}$，称自然映射。

如果已经给出互不相交且覆盖全集的若干块，只需规定同一块中的元素等价，就得到一个等价关系。反过来，等价关系也应把集合分成这样的块。下面验证这两种做法确实互相还原。

定理 1.2.9 (等价关系与分划)**.** 集合的等价关系与其分划一一对应。对群 G 的子群 H，关系 $a \sim b \iff a^{-1}b \in H$ 是等价关系，a 的等价类正是 aH。

证明. 等价类覆盖全集，且相交即相等，故给出分划。反之，规定同一块中的元素等价即可，两个构造互逆。陪集情形的反身、对称和传递性分别由 $e \in H$、求逆封闭及乘法封闭保证。 □

注意 aH 是 G 的子集，却是 G/H 的一个元素；此时 G/H 还只是集合。

有限群的所有陪集大小相同，因此陪集分划立即转化为计数公式。

定理 1.2.10 (Lagrange 定理)**.** 若 G 有限、$H < G$，则 $|G| = [G : H]|H|$。所以子群的阶及元素的阶均整除 $|G|$。

证明. $H \to aH$，$h \mapsto ah$ 是双射，而 G 是 $[G : H]$ 个左陪集的不交并。 □

推论 1.2.11 (指数的乘法公式)**.** 若 $K < H < G$ 且 G 有限，则 $[G : K] = [G : H][H : K]$。

证明. 分别用群阶之比表示三个指数即可。 □

例 1.2.12 (两个陪集分解)**.** 当 $m > 0$ 时，$\mathbb{Z} = \coprod_{r=0}^{m-1}(r + m\mathbb{Z})$，故 $[\mathbb{Z} : m\mathbb{Z}] = m$。对 $n \geq 1$，令 $D = \mathrm{diag}(-1, 1, \ldots, 1)$。正交矩阵的行列式只能为 ± 1；行列式为 -1 的矩阵 A 满足 $D^{-1}A \in SO(n)$，因此 $O(n) = SO(n) \sqcup DSO(n)$，故 $[O(n) : SO(n)] = 2$。

陪集的计数只用到了子群性，并没有要求左右陪集相同。如果我们进一步想乘两个陪集，代表元的选择就会进入计算。矩阵例 1.2.7 已经提醒我们，非交换乘法中不能随意把 H 中的因子移到另一边。

1.3 正规子群与商群

现在 G/H 只是由左陪集组成的集合。我们想沿用 G 的乘法，定义 $(aH)(bH) = abH$。写下这个公式并不困难，困难在于同一个陪集有许多代表元：如果换一组代表元，结果不能变。

取 $h_1, h_2 \in H$，将 a, b 换为 ah_1, bh_2，得到

$$(ah_1)(bh_2) = ab(b^{-1}h_1b)h_2.$$

要让它仍落在 abH 中，只需保证 $b^{-1}h_1b \in H$。这里多出来的共轭并非人为加上的技巧，它恰好来自把中间的 h_1 移到乘积的右端。因此我们要求子群在所有这样的共轭下保持不变。

定义 1.3.1 (正规子群、共轭与单群). 子群 $H < G$ 若满足 $ghg^{-1} \in H\,(g \in G, h \in H)$，称为正规子群，记为 $H \trianglelefteq G$。形如 gag^{-1} 的元素称与 a 共轭，它们的全体 C_a 称共轭类。非平凡群若仅有 $\{e\}, G$ 两个正规子群，则称单群。

共轭确实是等价关系：$a = eae^{-1}$；若 $b = gag^{-1}$，则 $a = g^{-1}bg$；接着再共轭一次，仍是共轭。因此正规子群一旦含有 a，就必须含有 a 的整个共轭类。反过来，由完整共轭类组成的子群也满足正规性。交换群中 $gag^{-1} = a$，故所有子群都正规。

若要把相同的办法用于其他代数结构，需要把“等价与运算相容”单独表述出来。

定义 1.3.2 (同余关系). 集合 A 上有二元运算 $*$。等价关系 $\sim$ 若满足

$$a \sim b,\ c \sim d \implies a * c \sim b * d,$$

则称为关于该运算的同余关系。

正规性可以改写成左右陪集相等，从而避免每次直接检查代表元。

定理 1.3.3 (正规性的等价条件). 对 $H < G$，以下条件等价：$H \trianglelefteq G$；$gH = Hg$ 对所有 g 成立；$(aH)(bH) = abH$ 作为集合乘积对所有 a, b 成立。它们也等价于 $a \sim b \iff a^{-1}b \in H$ 是乘法同余关系。

证明. 正规性对 g 和 g^{-1} 分别应用，得 $gHg^{-1} = H$，即 $gH = Hg$；于是 $(aH)(bH) = abHH = abH$。反之，取 $a = g, b = g^{-1}$，得 $ghg^{-1} \in H$。同余关系的充分性由本节开头的计算得到；必要性由 $h \sim e$ 推出 $ghg^{-1} \sim e$。 □

现在运算不再依赖代表元，群公理也就能从 G 传下来。

定理 1.3.4 (商群). 若 $H \trianglelefteq G$，则 G/H 在 $(aH)(bH) = abH$ 下构成群，幺元为 H，$(aH)^{-1} = a^{-1}H$，称为商群。

证明. 代表元无关性已经由定理 1.3.3 保证。现在检查的是陪集之间的等式，例如

$$((aH)(bH))(cH) = (ab)cH = a(bc)H = (aH)((bH)(cH)).$$

又有 $H(aH) = (aH)H = aH$，以及 $(aH)(a^{-1}H) = (a^{-1}H)(aH) = H$。所以幺元是整个陪集 H，而不是 G 中单独的元素 e；这些公式给出所需群结构。 □

例 1.3.5 (剩余类群与矩阵商群的起点). 对 $m \geq 1$，$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$ 的运算为 $\bar{a} + \bar{b} = \overline{a+b}$。此外，$\mathrm{SL}(n, \mathbb{R}) \trianglelefteq \mathrm{GL}(n, \mathbb{R})$，因为 $\det(ABA^{-1}) = \det B$；同理 $SO(n) \trianglelefteq O(n)$。

后面限制同态或比较商群时，经常需要把正规子群与任意子群相交。

引理 1.3.6 (正规子群的限制). 若 $H < G$、$N \trianglelefteq G$，则 $H \cap N \trianglelefteq H$。

证明. 交集是子群，且 hnh^{-1} 同时属于 H 和 N。 □

商群告诉我们，把 N 中的元素视为幺元后会得到什么。也可以反过来问：能否找一个子群 H，使每个 $g \in G$ 都能写成 hn，其中 $h \in H, n \in N$？如果还要求这种写法唯一，

就必须有 $H\cap N=\{e\}$：交中一个非幺元可以在两个因子之间来回移动。下一节之后，我们会从扩张的角度继续研究这种分解；这里先记下名称。

定义 1.3.7 (内半直积与内直积). 若 $N\trianglelefteq G$、$H<G$，且 $G=HN$、$H\cap N=\{e\}$，称 G 为 H 与 N 的半直积，记为 $H\ltimes N$。若 H 也正规，则称为内直积，记为 $H\times N$。

商群构造自带一个保持乘法的映射，它将引出下一节的一般概念。

定义 1.3.8 (自然同态). 对 $N\trianglelefteq G$，映射 $\pi:G\to G/N$，$g\mapsto gN$ 称自然同态；它满足 $\pi(gh)=\pi(g)\pi(h)$。

1.4 群的同态与同构

上一节的自然映射 $\pi(g)=gN$ 满足 $\pi(gh)=\pi(g)\pi(h)$：先在原群中相乘再取陪集，与先取陪集再相乘，结果相同。我们想研究的正是保持这种运算关系的映射。

有些映射只是给同一个群换一种写法，例如指数函数把实数加法变为正实数乘法；另一些映射会把不同元素送到同一个位置，例如模 m 的映射。因而接下来有两个问题：映射的像本身是什么群？哪些原元素在映射后相等？核与商群将给出这两个问题的统一答案。

定义 1.4.1 (群同态). 映射 $f:G\to G'$ 若满足 $f(ab)=f(a)f(b)$，称群同态。分别为单射、满射、双射时称单同态、满同态、同构；存在同构时记 $G\cong G'$。到自身的同态和同构分别称自同态、自同构。恒取值 e' 的同态称平凡同态。

保持乘法已经足以迫使幺元和逆元的像也相容，因此不必把这些条件另加进定义。

命题 1.4.2 (同态的基本运算). 同态满足 $f(e)=e'$、$f(a^{-1})=f(a)^{-1}$；同态的复合仍是同态，同构的逆映射仍是同构。G 的自同态全体 $\mathrm{Hom}(G)$ 是复合幺半群，自同构全体 $\mathrm{Aut}(G)$ 是群。

证明. $f(e)^2=f(e)$，消去得第一式；由 $f(a)f(a^{-1})=f(e)$ 得第二式。复合的乘法保持性直接计算；同构的逆把等式 $f(ab)=f(a)f(b)$ 反向读出即可。 □

例 1.4.3 (同一结构的不同表现). $\exp:(\mathbb{R},+)\to(\mathbb{R}^+,\cdot)$ 是同构，因为 $e^{a+b}=e^ae^b$，且对数给出逆映射。

给 n 维线性空间 V 选定有序基 $\mathcal{B}=(v_1,\dots,v_n)$，将坐标写成列向量。若线性变换 u 的矩阵为 $A=(a_{ij})$，约定

$$u(v_j)=\sum_{i=1}^{n}a_{ij}v_i,\qquad [u(v)]_{\mathcal{B}}=A[v]_{\mathcal{B}}.$$

因此第 j 列是第 j 个基向量的像的坐标，复合变换对应同序的矩阵乘法。这给出加法群 $V\cong P^n$ 以及 $\mathrm{GL}(V)\cong\mathrm{GL}(n,P)$。

若 T 将旧坐标变成新坐标，即 $[v]_{\mathcal{B}'}=T[v]_{\mathcal{B}}$，那么新矩阵为 TAT^{-1}。必须同时说明 T 的方向；若把 T 定义为反向的坐标变换，公式就会写成 $T^{-1}AT$。

换基中的共轭并不依赖矩阵；它在任意群中都给出一族自同构。

命题 1.4.4 (内自同构). 对 $a \in G$、$\varphi \in \mathrm{Aut}(G)$，$\mathrm{Ad}_a(g) = aga^{-1}$ 是自同构，且

$$\mathrm{Ad}_a \,\mathrm{Ad}_b = \mathrm{Ad}_{ab}, \qquad \varphi \,\mathrm{Ad}_a \,\varphi^{-1} = \mathrm{Ad}_{\varphi(a)}\,.$$

故 $\mathrm{Inn}(G) = \{\mathrm{Ad}_a : a \in G\} \trianglelefteq \mathrm{Aut}(G)$。商群 $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ 称外自同构群。

证明. 共轭保持乘法，逆映射为 $\mathrm{Ad}_{a^{-1}}$。两个公式逐点计算即得，第二个公式同时给出正规性。 □

也可以只左乘或右乘一个元素。这些变换未必是群自同构，却总是集合上的双射。

定义 1.4.5 (平移变换). 令 $L_a(g) = ag$、$R_a(g) = ga$，分别称左、右平移。它们满足 $L_aL_b = L_{ab}$、$R_aR_b = R_{ba}$。

左平移忠实记录了原来的乘法，因此每个抽象群都能实现为一个变换群。

定理 1.4.6 (Cayley 定理). 任意群 G 同构于 S_G 的一个子群。

证明. 映射 $a \mapsto L_a$ 是同态；若 $L_a = L_b$，在 e 处取值得 $a = b$，所以它是单同态。 □

现在回到一般同态 $f : G \to G'$。判断 a, b 是否被送到同一个元素，不必逐对比较：

$$f(a) = f(b) \iff f(a)^{-1}f(b) = e' \iff f(a^{-1}b) = e'.$$

所以只要知道哪些元素被送到 e'，就知道全部相等的像从何而来。我们把这些元素组成的集合叫作核，把所有实际取到的值组成的集合叫作像。

定义 1.4.7 (核、像与中心). 令 $\ker f = \{g : f(g) = e'\}$、$\mathrm{Im}\, f = f(G)$。群的中心记为

$$C(G) = \{a \in G : ag = ga \text{ 对所有} g \in G\}.$$

它是同态 $\mathrm{Ad} : G \to \mathrm{Inn}(G)$ 的核。

核不仅判别单射，而且准确描述哪些元素被同态合并。

引理 1.4.8 (核与像). $\mathrm{Im}\, f < G'$、$\ker f \trianglelefteq G$；且 $f(a) = f(b)$ 当且仅当 $a^{-1}b \in \ker f$。特别地，f 单射当且仅当 $\ker f = \{e\}$。更一般地，子群的像和完全原像仍是子群；正规子群的完全原像仍正规，正规子群的像在 $f(G)$ 中正规。

证明. 先看像：$f(a)f(b)^{-1} = f(ab^{-1})$ 仍在像中，故像是子群。核是子群判别法的另一个直接应用；若 $n \in \ker f$，则 $f(gng^{-1}) = f(g)e'f(g)^{-1} = e'$，故核正规。前面的等式链说明 $f(a) = f(b) \iff a^{-1}b \in \ker f$。核只含 e 时，它迫使 $a = b$；反向由单射性立即得到。

对任意子群 $H < G$，同样把子群判别法用于 $f(a), f(b)$，得到 $f(H) < G'$。对任意 $H' < G'$，若 $a, b \in f^{-1}(H')$，则 $f(ab^{-1}) \in H'$，所以 $f^{-1}(H') < G$。

正规性的区别在于共轭元素来自哪里。若 $H' \trianglelefteq G'$，则 $f(gag^{-1}) = f(g)f(a)f(g)^{-1} \in H'$，故原像在 G 中正规。若 $N \trianglelefteq G$，则对 $f(g) \in f(G)$ 有

$$f(g)f(N)f(g)^{-1} = f(gNg^{-1}) = f(N).$$

这只保证 $f(N)$ 在 $f(G)$ 中正规；陪域 G' 中未必每个元素都形如 $f(g)$。 □

推论 1.4.9 (正规子群的同态刻画)**.** $N < G$ 正规，当且仅当它是某个以 G 为定义域的同态的核。

证明. 一个方向用引理 1.4.8，另一个方向取自然同态 $G \to G/N$。 □

例 1.4.10 (寻找核)**.** $\mathbb{Z} \to G$，$m \mapsto a^m$，像为 $\langle a \rangle$，核为某个 $n\mathbb{Z}$。行列式 $\det : \mathrm{GL}(n,P) \to P^*$ 是满同态，核为 $\mathrm{SL}(n,P)$。置换 σ 作用于基向量 $e_i \mapsto e_{\sigma(i)}$ 给出 $S_n \to \mathrm{GL}(n,P)$ 的单同态；在特征 0 时再取行列式，就得到置换的符号。

令 $N = \operatorname{Ker} f$。刚才的判别说明，gN 中的元素全被送到 $f(g)$，并且凡是被送到 $f(g)$ 的元素都在 gN 中。因此可以先把每个陪集当成一个元素，再把它对应到这个共同的像。这样既不会遗漏 $f(G)$ 中的元素，也不会把两个不同陪集再次合并。

定理 1.4.11 (群的同态基本定理)**.** 对同态 $f : G \to G'$，存在同构

$$\bar{f} : G/\operatorname{Ker} f \longrightarrow \operatorname{Im} f, \qquad g \operatorname{Ker} f \longmapsto f(g).$$

证明. 定义 $\bar{f}(gN) = f(g)$，其中 $N = \operatorname{Ker} f$。若 $gN = hN$，则 $g^{-1}h \in N$，所以 $f(g) = f(h)$，公式不依赖代表元。反过来，若两个像相等，同一个判别又给出 $gN = hN$，故 $\bar{f}$ 单射。它显然取遍 $f(G)$，并且

$$\bar{f}((gN)(hN)) = f(gh) = f(g)f(h) = \bar{f}(gN)\bar{f}(hN).$$

于是 $\bar{f}$ 是同构。若把像包含进 G' 的映射记为 j，原同态就写成 $f = j\bar{f}\pi$：先取陪集，再用同构对应到像，最后看成陪域中的元素。 □

特别地，$G/C(G) \cong \mathrm{Inn}(G)$、$\mathrm{GL}(n,P)/\mathrm{SL}(n,P) \cong P^*$。

既然 G/N 与像同构，我们还想知道商群中的子群对应原群的哪些子群。由 G 走向商群用的是取像，返回则用完全原像。这里有一个限制：任何子群的完全原像都包含核，因为它必须包含幺元的全部原像。因此，能够被这两个操作互相对应的，正是原群中包含核的子群。

定理 1.4.12 (子群对应与商的商)**.** 设 $f : G \twoheadrightarrow G'$，$N = \operatorname{Ker} f$。映射 $H \mapsto f(H)$ 与 $H' \mapsto f^{-1}(H')$ 给出 G 中包含 N 的子群与 G' 的子群之间的互逆对应，并保持包含及正规性。若 $N \subseteq H \trianglelefteq G$，则

$$G/H \cong G'/f(H), \qquad (G/N)/(H/N) \cong G/H.$$

证明. 满射性保证 $f(f^{-1}(H')) = H'$。对于 $N \subseteq H < G$，显然 $H \subseteq f^{-1}(f(H))$；反过来，若 $f(g) = f(h)$、$h \in H$，则 $h^{-1}g \in N \subseteq H$，所以 $g \in H$。于是两个操作互逆。取像与原像都保持包含关系，正规性的双向保持来自引理 1.4.8 及满射性。

若 $H \trianglelefteq G$ 且包含 N，考虑具体映射 $g \mapsto f(g)f(H)$。它满射到 $G'/f(H)$，核为 $f^{-1}(f(H)) = H$。同态基本定理便给出 $G/H \cong G'/f(H)$。特别取 $G' = G/N$ 及自然映射，此时 $f(H) = H/N$，便得到商的商公式。 □

把自然同态限制到任意子群，可以比较“先限制再取商”和“先取商再取像”这两种做法。

定理 1.4.13 (子群与正规子群的乘积). 若 $H < G$、$N \trianglelefteq G$，则 $HN < G$，且对自然同态 $\pi : G \to G/N$ 有

$$HN = \pi^{-1}(\pi(H)), \qquad H/(H \cap N) \cong HN/N.$$

证明. $\pi^{-1}(\pi(H))$ 是子群；$\pi(g) = \pi(h)$ 恰指 $g \in hN$，故等于 HN。限制 $\pi|_H$ 的核为 $H \cap N$，像为 HN/N，再次应用同态基本定理。 □

以后遇到商群同构，不必先猜一个双射再反复检查。通常可以先找一个自然同态，计算它的核与像，再应用定理 1.4.11。例如下一节只需研究 $m \mapsto a^m$ 的核，就能分类所有由一个元素生成的群。

1.5 循环群

上一节已经有一个特别简单的同态：$\mathbb{Z} \to G$，$m \mapsto a^m$。它把整数加法变成幂的乘法，像恰好是 $\langle a \rangle$。因此，如果一个群的全部元素都能写成 a 的整数次幂，研究它就等于研究这个同态把哪些整数合在一起。

核是 $\mathbb{Z}$ 的子群，而例 1.2.4 已说明这种子群只能是 $n\mathbb{Z}$。这意味着分类所需的准备已经完成：只要看 a 的幂是否会回到幺元，以及第一次回到幺元要乘几次。

定义 1.5.1 (循环群). 若 $G = \langle a \rangle$，称 G 为循环群，a 为生成元。循环群必为 Abel 群。

例 1.5.2 (循环群的几种表现). $\mathbb{Z} = \langle 1 \rangle$，$\mathbb{Z}_n = \langle \bar{1} \rangle$ $(n \geq 1)$。在复数中取 $\zeta = e^{2\pi i/n}$，则 n 次单位根群 $\mu_n = \{z \in \mathbb{C} : z^n = 1\} = \{1, \zeta, \ldots, \zeta^{n-1}\}$ 也由一个元素生成。
循环置换矩阵 $J = E_{12} + \cdots + E_{n-1,n} + E_{n1}$ 依次将 e_1 送到 e_n、将 e_j 送到 $e_{j-1}$$(j > 1)$。所以 $J^n = I$，且没有更小的正幂为 I，它生成 n 阶循环群。形如 $a_0 I + a_1 J + \cdots + a_{n-1} J^{n-1}$ 的矩阵称循环矩阵；这里的线性组合全体与仅由 J 的幂组成的群要区分。
若 $|G| = p$ 为素数，任取 $a \neq e$，Lagrange 定理给出 $|a| \mid p$ 且 $|a| > 1$，故 $|a| = p$，于是 $G = \langle a \rangle$。

同态基本定理把分类问题化为寻找 $\mathbb{Z}$ 的子群，而这一点我们已经解决。

定理 1.5.3 (循环群的分类). 无限循环群同构于 $\mathbb{Z}$；n 阶循环群同构于 $\mathbb{Z}_n$。因此两个循环群同构，当且仅当它们同阶。

证明. 把 $m \mapsto a^m$ 看作到 $\langle a \rangle$ 的满同态，核形如 $n\mathbb{Z}$，其中 $n \geq 0$。若 $n = 0$，核平凡，不同整数给出不同幂，故 $\langle a \rangle \cong \mathbb{Z}$。若 $n > 0$，同态基本定理给出 $\langle a \rangle \cong \mathbb{Z}/n\mathbb{Z}$，后者恰有 n 个元素。因此群阶确定了上述两种情形及其中的 n；反过来，同构当然保持阶。 □

子群也可以继续用指数描述，关键仍然是取最小正指数再作带余除法。

引理 1.5.4 (循环群的子群). 循环群 $\langle a \rangle$ 的每个子群均为循环群，形如 $\langle a^d \rangle$。

证明. 平凡子群取 $d = 0$。非平凡子群 H 中存在正幂，令 $d = \min\{k > 0 : a^k \in H\}$。若 $a^m \in H$，写 $m = qd + r$、$0 \leq r < d$，则 $a^r \in H$，迫使 $r = 0$。因此 $H = \langle a^d \rangle$。 □

有限循环群中，每个群阶的因子都确实给出一个子群，而且只给出一个。

定理 1.5.5 (有限循环群的子群结构)**.** 设 $|a| = n$。对每个 $d \mid n$，唯一的 d 阶子群是 $\langle a^{n/d} \rangle$。此外

$$|a^k| = \frac{n}{\gcd(n,k)}, \qquad \langle a^k \rangle = \langle a \rangle \iff \gcd(n,k) = 1.$$

证明. 先算 a^k 的阶。令 $c = \gcd(n,k)$，写成 $n = cn_0, k = ck_0$，其中 $\gcd(n_0, k_0) = 1$。于是

$$(a^k)^r = e \iff n \mid kr \iff n_0 \mid k_0 r \iff n_0 \mid r.$$

最小正解为 $r = n_0$，得到阶的公式；阶等于 n 正好等价于 $c = 1$，也就等价于生成整个群。

对任意子群 H，取满足 $a^t \in H$ 的最小正整数 t；即使 $H = \{e\}$，这样的整数也存在，且此时 $t = n$。引理 1.5.4 的除法论证给出 $H = \langle a^t \rangle$。又因 $a^n = e \in H$，同一论证给出 $t \mid n$，所以 $|H| = n/t$。要使 $|H| = d$，只能有 $t = n/d$；这个取值也确实产生 d 阶子群，存在性与唯一性同时得到。 □

最后，交换群的正规子群就是所有子群，这使单群条件特别强。

定理 1.5.6 (Abel 单群)**.** 非平凡 Abel 群是单群，当且仅当它是素数阶循环群。

证明. 任取 $a \neq e$，$\langle a \rangle$ 正规，单性迫使 $G = \langle a \rangle$。无限循环群有非平凡真子群 $\langle a^2 \rangle$；合数阶循环群也有非平凡真子群。反之，素数阶群由 Lagrange 定理没有这样的子群。 □

循环群说明，Lagrange 定理的逆命题在某些群中确实成立：每个阶的因子都对应一个子群，而且这里还唯一。不过，这个结论用到了所有元素都是同一个 a 的幂。下一节的置换群中，多个轮换可以同时出现，子群的情形就丰富得多。

1.6 对称群与交错群

Cayley 定理告诉我们，每个群都能用一组置换表示。但一个置换若只写成所有元素及其像的长表，乘法、阶和共轭都不容易看清。我们先寻找更便于计算的写法。

从一个文字 i 出发，依次看 $i, \sigma(i), \sigma^2(i), \ldots$。集合有限，而且 σ 可逆，所以这条路线最终回到 i，在回去之前不会重复经过别的文字。它形成的循环就是一个轮换；把所有这样的路线找出来，就能拆开整个置换。

定义 1.6.1 (轮换)**.** $(i_1\, i_2 \cdots i_r)$ 把 $i_1 \mapsto i_2 \mapsto \cdots \mapsto i_r \mapsto i_1$，并固定其他文字，称为 r-轮换。2-轮换称对换。没有共同文字的轮换称不相交。置换乘法采用映射复合，右边先作用。

命题 1.6.2 (不相交轮换可交换)**.** 两个不相交轮换可交换。

证明. 对处于任一轮换支集中的文字，另一轮换不改变它及其像；对其他文字，两者都不改变。 □

共轭置换只是在重新标记文字。记录这个公式，便能在后面统一处理不同位置上的轮换。

命题 1.6.3 (轮换的共轭)**.** 对 $\tau \in S_n$，有

$$\tau(i_1\, i_2 \cdots i_r)\tau^{-1} = (\tau(i_1)\, \tau(i_2) \cdots \tau(i_r)).$$

证明. 左边把 $\tau(i_j)$ 送到 $\tau(i_{j+1})$，把 $\tau(i_r)$ 送到 $\tau(i_1)$，并固定其余文字。 □

沿各个文字的运动轨迹进行分组，就能把任意置换拆成互不干扰的部分。

定理 1.6.4 (不相交轮换分解)**.** 每个 $\sigma \in S_n$ 都可唯一地写成不相交轮换之积，其中不计轮换次序、轮换的循环写法及省略的 1-轮换。其阶是各轮换长度的最小公倍数。

证明. 固定 i，序列 $i, \sigma(i), \sigma^2(i), \ldots$ 第一次重复必回到 i，否则可用 σ^{-1} 得到更早的重复。把这一轨迹写成轮换，再从未使用的文字出发，有限步后用尽所有文字。每条轨迹由 σ 唯一确定，故分解唯一。σ^m 固定全部文字，当且仅当所有轮换长度都整除 m。 □

例 1.6.5 (从分解读出阶)**.** $\sigma = (274)(35)$ 的阶为 $\operatorname{lcm}(3, 2) = 6$；固定的文字 $1, 6$ 不必写出。

轮换还可以拆成对换。虽然拆法不唯一，但我们将看到一个不依赖拆法的奇偶性。

引理 1.6.6 (轮换分解成对换)**.**

$$(i_1 i_2 \cdots i_r) = (i_1 i_r)(i_1 i_{r-1}) \cdots (i_1 i_2).$$

证明. 按右边先作用的约定，i_1 先被最右边的 $(i_1 i_2)$ 送到 i_2，其余对换不再移动它。对 $2 \le j < r$，i_j 在遇到 $(i_1 i_j)$ 时先变为 i_1，再被紧接着的 $(i_1 i_{j+1})$ 送到 i_{j+1}。最后，i_r 被送到 i_1，其他文字保持不动。这与左边的轮换逐点相同。 □

命题 1.6.7 (置换的奇偶性)**.** 每个置换都是对换之积，且对换个数的奇偶性与分解无关。符号映射 $\operatorname{sgn} : S_n \to \{1, -1\}$ 是同态，r-轮换的符号为 $(-1)^{r-1}$。

证明. 轮换分解及引理 1.6.6 先保证每个置换都能写成对换之积。为了证明奇偶性不依赖写法，我们需要一个直接由置换本身确定的量。

在实数域上令 $P_\sigma e_j = e_{\sigma(j)}$。列坐标约定给出 $P_{\sigma\tau} = P_\sigma P_\tau$，而每个对换矩阵交换单位矩阵的两列，行列式为 -1。若 σ 写成 k 个对换之积，则

$$\det P_\sigma = (-1)^k.$$

左边与所选分解无关，所以右边的奇偶性也无关。定义 $\operatorname{sgn}\sigma = \det P_\sigma$，行列式的乘法公式便证明它是同态。一个 r-轮换可写成 $r-1$ 个对换之积，故符号为 $(-1)^{r-1}$。 □

偶置换对乘法和求逆封闭，因此形成一个自然的正规子群。

定义 1.6.8 (交错群)**.** 符号为 1 的置换称偶置换，为 -1 的称奇置换。$A_n = \operatorname{Ker}(\operatorname{sgn})$ 称 n 元交错群。$n \ge 2$ 时 $|A_n| = n!/2$，$A_n \trianglelefteq S_n$。

$A_3 = \langle (123) \rangle \cong \mathbb{Z}_3$。在 A_4 中，$K_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ 是子群，而且共轭只重新标记文字，仍把两个不相交对换之积送到这种形式，故 $K_4 \trianglelefteq A_4$。所以 A_4 不是单群。

从 $n = 5$ 开始，我们将证明任何非平凡正规子群都等于 A_n。直接列举所有子群并不可行，可以反过来从正规子群的一个非幺元出发，设法制造一个 3-轮换。下面先证明所有 3-轮换生成 A_n 且彼此共轭；这样，一旦得到其中一个，正规性就会给出全部生成元。

定理 1.6.9 (交错群的单性)**.** 当 $n \geq 5$ 时，A_n 是非 Abel 单群。

证明. 首先，A_n 由 3-轮换生成。把偶数个对换两两配对：相同的抵消，只有一个公共文字时乘积为 3-轮换；不相交时可用

$$(ab)(cd) = (acb)(acd).$$

其次，所有 3-轮换在 A_n 中共轭：先在 S_n 中换文字，若所用置换为奇置换，再复合一个位于目标 3-轮换之外的对换，既改变奇偶性又不影响共轭结果。

设 $\{e\} \neq N \trianglelefteq A_n$，取 $\sigma \neq e$ 属于 N。如果 σ 的轮换很多，我们不必直接取它的幂去逐个消除。可以选一个只移动少数文字的 $\tau \in A_n$，考察

$$\delta = \tau\sigma\tau^{-1}\sigma^{-1} = \tau(\sigma\tau^{-1}\sigma^{-1}).$$

正规性保证 $\delta \in N$；后一写法又让我们只需用共轭公式计算 τ 中少数文字的像，其余轮换会自动抵消。以下情形覆盖了 σ 的所有可能轮换类型，重命名文字后逐一计算。

1. 若 σ 含 $(12\cdots r)$，$r \geq 4$，则取 $\tau = (123)$，得 $\tau\sigma\tau^{-1}\sigma^{-1} = (123)(324) = (124)$。

2. 若无长于 3 的轮换但至少有两个 3-轮换，可设含 $(123)(456)$。取 $\tau = (124)$，所得乘积为 $(124)(253) = (12534)$，归结到第一种情形。

3. 若只有一个 3-轮换，其他均为对换，则 σ^2 本身是 3-轮换。

4. 若只有对换，因 σ 偶，至少有两个。设含 $(12)(34)$，取 $\tau = (123)$ 得 $\delta = (13)(24) \in N$；再取 $\tau = (135)$，得 $\tau\delta\tau^{-1}\delta^{-1} = (153) \in N$。

所以 N 含一个 3-轮换，进而含其全部共轭及它们生成的 A_n。例如 $(123)(124)$ 将 1 送到 3，而 $(124)(123)$ 将 1 送到 4，所以 A_n 非 Abel。 □

这个证明中，共轭有两个作用：它使正规子群包含某种轮换的全部重新标记，也让我们从一个复杂置换构造出只移动少数文字的元素。接下来讨论群的分解时，单群将作为不能再取非平凡正规商的末端因子出现。

1.7 群的扩张与 Jordan–Hölder 定理

已知 $N \trianglelefteq G$，我们能分别研究 N 与 G/N。反过来，如果只给出两个群 A, B，能否找到一个群 G，其中有正规子群同构于 A，并且商群同构于 B？即使找得到，这样的 G 是否唯一？

$\mathbb{Z}_4$ 中的 $\{\bar{0}, \bar{2}\}$ 和 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 中的 $\mathbb{Z}_2 \times \{0\}$ 已给出一个提醒：两次取到的正规子群与商群都同构于 $\mathbb{Z}_2$，但前一个群有 4 阶元，后一个群没有。因此，仅知道子群与商群还不能确定原群的乘法。

要比较这样的构造，还必须记住 A 怎样嵌入 G，以及 G 怎样投到 B。短正合序列把这两个映射和它们必须满足的条件放在一起。

定义 1.7.1 (正合与扩张)**.** 同态序列 $A \xrightarrow{\lambda} G \xrightarrow{\mu} B$ 在 G 处正合，指 $\operatorname{Im}\lambda = \operatorname{Ker}\mu$。若

$$1 \longrightarrow A \xrightarrow{\lambda} G \xrightarrow{\mu} B \longrightarrow 1$$

在各处正合，称为短正合序列，并称 G 是 B 过 A 的扩张。此时 λ 单、μ 满，$N = \lambda(A) \trianglelefteq G$ 称扩张核，且 $N \cong A$、$G/N \cong B$。

这里两端的 1 表示平凡群。正合性在 A 处说 $\operatorname{Ker}\lambda = 1$，所以 λ 单；在 B 处说 $\operatorname{Im}\mu = B$，所以 μ 满；在中间说被 μ 送到幺元的元素恰是嵌入的 A。因此这串箭头精确表达了开头的要求，而没有额外假定 G 由哪种乘法构成。

例 1.7.2 (相同因子，不同扩张)**.** $\mathbb{Z}_4$ 与 $K_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$ 都是 $\mathbb{Z}_2$ 过 $\mathbb{Z}_2$ 的扩张，但不同构。S_3 是 $\mathbb{Z}_2$ 过 $\mathbb{Z}_3$ 的扩张；$\mathbb{Z}$ 经由 $2\mathbb{Z}$ 是 $\mathbb{Z}_2$ 过 $\mathbb{Z}$ 的扩张；$O(n)$ 经由 $SO(n)$ 是 $\mathbb{Z}_2$ 过 $SO(n)$ 的扩张。

比较两个扩张时，我们希望 A 中同一个元素在两个群里的位置相对应，也希望对应元素投到 B 后相同。这就是图 1.1 中两个方块的交换性：从 A 到 G' 的两条路径相同，从 G 到 B 的两条路径也相同。令人方便的是，满足这些条件的群同态自动是同构。

定理 1.7.3 (扩张的等价)**.** 同构群继承原有的扩张结构。若两个 B 过 A 的扩张之间有同态 $f : G \to G'$，满足 $f\lambda = \lambda'$、$\mu' f = \mu$，则 f 必为同构；这时称两个扩张等价。

证明. 先证单射。若 $f(g) = e$，由 $\mu' f = \mu$ 得 $\mu(g) = e$，于是 $g = \lambda(a)$。再由 $f\lambda = \lambda'$ 得 $\lambda'(a) = e$；λ' 单射，故 $a = e$、$g = e$。

再证满射。给定 $g' \in G'$，先不要求在 G 中直接找到它的原像，只要求在商群 B 中对上：取 $g \in G$ 使 $\mu(g) = \mu'(g')$。此时

$$\mu'(g' f(g)^{-1}) = e,$$

所以差出的因子属于 $\operatorname{Im}\lambda'$，可写成 $g' f(g)^{-1} = \lambda'(a)$。用 $\lambda(a)$ 调整所选的 g，便有 $g' = \lambda'(a) f(g) = f(\lambda(a) g)$。故 f 满。

若只是给定群同构 $u : G \to G'$，取新的嵌入 $u\lambda$ 和新的投影 μu^{-1}，便把原短正合序列传到 G'；这是第一句的含义。 □

在线性空间中，选补空间就能给每个商向量选一个代表，而且代表的选择保持加法与数乘。群中也想这样做：对每个 $b \in B$ 选 $\iota(b) \in G$，满足 $\mu(\iota(b)) = b$，并要求 $\iota(b_1 b_2) = \iota(b_1)\iota(b_2)$。

任意选代表一般不满足后一条件。如果能满足，它们的全体就组成一个子群 H，而每个 g 与代表 $\iota(\mu(g))$ 只差一个 N 中的因子。这正好联系到前面定义的半直积。

定理 1.7.4 (扩张分裂的判别)**.** 对上述短正合序列，以下条件等价：存在 $H < G$ 使 $G = HN$、$H \cap N = \{e\}$；存在同态 $\iota : B \to G$ 使 $\mu\iota = \mathrm{id}_B$。此时 $\mu|_H : H \to B$ 为同构，且可取 $H = \iota(B)$。

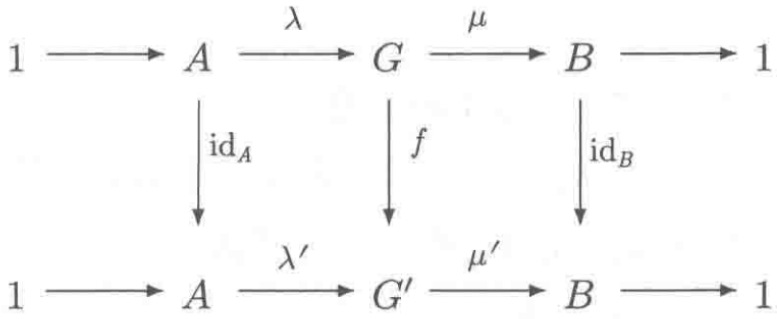


图 1.1: 保持两端及结构映射的扩张比较。交换性意味着 $f\lambda = \lambda'$、$\mu' f = \mu$。

证明. 若有 H，限制映射的核为 $H \cap N$，且由 $G = HN$ 可知满；取其逆即可。若有 ι，则 ι 单，且 $\iota(B) \cap N = \{e\}$。对 $g \in G$，$\iota(\mu(g))^{-1} g \in N$，故 $G = \iota(B)N$。 □

这些特殊的结合方式有各自的名称，后面讨论可解性和幂零性时会用到。

定义 1.7.5 (几类扩张)**.** 满足定理 1.7.4 的扩张称非本质扩张，此时 $G = H \ltimes N$。若 H 也正规，称平凡扩张，此时 $G = H \times N$。若 $N \subseteq C(G)$，称中心扩张。

例 1.7.6 (分裂与否)**.** 对 $n \geq 3$, S_n 的符号映射以 A_n 为核，子群 $H = \langle (12) \rangle$ 在符号映射下同构于 $\mathbb{Z}_2$，故给出非本质扩张。对 $n \geq 1$，$O(n)$ 中的反射 $D = \mathrm{diag}(-1, 1, \ldots, 1)$ 也给出行列式映射的补子群。
$\mathbb{Z} \to \mathbb{Z}_2$ 却不分裂：若同态右逆存在，$\bar{1}$ 必被送到一个满足 $2a = 0$ 且映到 $\bar{1}$ 的整数；$\mathbb{Z}$ 中只有 $a = 0$ 满足前式，而它的像不对。$\mathbb{Z}_{15}$ 则有 $\langle \bar{5} \rangle$、$\langle \bar{3} \rangle$ 两个子群，阶分别为 $3, 5$，交平凡且相加为全群，所以 $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$ 是平凡扩张。

要使“拼接”真正对应于有序对，需要先知道乘积分解唯一。

引理 1.7.7 (唯一分解与交换)**.** 设 $G = AB$，$A, B < G$。$A \cap B = \{e\}$、每个 $g = ab$ 的分解唯一、幺元的分解唯一三者等价。在此条件下，A, B 都正规，当且仅当它们的元素逐个交换。

证明. 由 $ab = a'b'$ 得 $a'^{-1}a = b'b^{-1} \in A \cap B$，即得唯一性。反向取 $x \in A \cap B$，用 $e = xx^{-1}$。若两者正规，$a^{-1}b^{-1}ab \in A \cap B$，故可交换；反之，写 $g = ab$ 后直接共轭验证正规性。 □

既然两部分逐个交换，有序对的逐分量乘法就能完整记录原群乘法。

定理 1.7.8 (直积的存在与唯一性)**.** 任意群 A, B 的平凡扩张在同构意义下唯一，由集合 $A \times B$ 及逐分量乘法实现。

证明. 逐分量运算满足群公理；两坐标子群正规、交平凡且乘积为全群。任何内直积分解中，映射 $(a, b) \mapsto ab$ 由上个引理是双射且保持乘法。 □

现在把取正规子群和商群这一步继续做下去。若 $G_1 \trianglelefteq G$，再取 $G_2 \trianglelefteq G_1$，就得到 G/G_1 与 G_1/G_2 两个因子。需要注意，G_2 未必正规于整个 G，但这不妨碍第二个商群

存在。因而逐层分解时，要区分只要求在前一项中正规，以及要求所有项都在 G 中正规。

定义 1.7.9 (次正规序列与合成序列)**.** 有限序列 $G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_r = \{e\}$ 若满足 $G_{i+1} \trianglelefteq G_i$，称次正规序列，$G_i/G_{i+1}$ 称因子。在其中插入子群且仍满足相应条件，称为加细。
若每项均正规于 G，称正规序列。若每个因子为单群，称合成序列，因子称合成因子。
不能再插入新的 G 的正规子群的正规序列称主序列；它要求因子在相应的 G/G_{i+1} 中没有更小的非平凡正规子群，未要求因子本身为单群。

有限群反复选极大真正规子群，必在有限步停止，所以有合成序列；$\mathbb{Z}$ 没有合成序列，因为它的非零子群仍是无限循环群。两个次正规序列若因子能在重排后逐个同构，称同构的序列。

合成序列相当于把每一层继续分解到不能再插入次正规项。不同选择可能先取不同的正规子群，因子的顺序也可能变化。Jordan–Hölder 定理要证明的，正是无论怎样选择，最后出现的单群种类与次数相同。

证明的办法不是直接把两条序列逐项配对，因为它们的项通常没有包含关系。我们先利用交集给两边同时插入更多项，构造能配对的加细；最后再用原因子的单性说明，这种加细没有产生新的非平凡因子。

定理 1.7.10 (Jordan–Hölder 定理)**.** 若群有合成序列，则任意两个合成序列具有相同长度，合成因子在重排及同构意义下相同。

证明. 设两个合成序列为 $(G_i)_{i=0}^{r}$ 与 $(H_j)_{j=0}^{s}$。固定 i，在 $G_i \supseteq G_{i+1}$ 之间插入

$$A_{ij} = G_{i+1}(G_i \cap H_j) \qquad (0 \le j \le s).$$

首项是 G_i，末项是 G_{i+1}。对另一条序列对称地设 $B_{ji} = H_{j+1}(H_j \cap G_i)$。我们将说明相邻项确实正规，且两边按 (i, j) 配对的因子同构。

令

$$K = G_i \cap H_j, \quad K_1 = G_{i+1} \cap H_j, \quad K_2 = G_i \cap H_{j+1}, \quad D = K_1 K_2.$$

由于 $G_{i+1} \trianglelefteq G_i$、$H_{j+1} \trianglelefteq H_j$，$K_1, K_2$ 都正规于 K，从而 $D \trianglelefteq K$。在 G_i/G_{i+1} 中取自然映射 q，则 $q(K_2) \trianglelefteq q(K)$，而

$$A_{ij} = q^{-1}(q(K)), \qquad A_{i,j+1} = q^{-1}(q(K_2)).$$

因此 $A_{i,j+1} \trianglelefteq A_{ij}$。对 B 的论证相同，所以确实得到两条次正规加细。

再将 K 映到 $A_{ij}/A_{i,j+1}$。这是满同态，因为 $A_{ij} = G_{i+1}K$，而 G_{i+1} 已包含在分母中。若 $x \in K$ 落在核内，就能写成 $x = uy$，其中 $u \in G_{i+1}$、$y \in K_2$。此时 $u = xy^{-1} \in H_j$，故 $u \in K_1$，从而 $x \in D$；反向包含也由乘积形式得到。故核恰为 D。对称地处理另一边，同态基本定理给出

$$\frac{A_{ij}}{A_{i,j+1}} \cong K/D \cong \frac{B_{ji}}{B_{j,i+1}}.$$

这就把两条加细的全部因子配成对。

最后用原序列的合成性。G_i/G_{i+1} 是单群，而刚构造的各项在这个区间内形成次正规链。单群的次正规链除重复项外只能从全群直接到 1：第一个真下降的项若非平凡，就

会成为全群的非平凡真正规子群。因此每个原区间的加细中恰有一个非平凡因子，仍同构于 G_i/G_{i+1}，其余因子都平凡。另一边也一样。删去重复项后，非平凡因子的配对便给出相同长度及所需同构。 □

例 1.7.11 (合成因子不决定群). $S_4 \supset A_4 \supset K_4 \supset \langle (12)(34)\rangle \supset \{e\}$ 是合成序列，因子依次为 $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_2$。但它不是正规序列：共轭可以把 $(12)(34)$ 变成 $(13)(24)$，所以那个 2 阶子群并不正规于 S_4。
相反，$S_4 \supset A_4 \supset K_4 \supset \{e\}$ 是主序列。前两段的因子阶为素数，不能再加细；K_4 的三个非幺元在 S_4 的共轭下互相变换，所以其内部没有可插入的非平凡 S_4 正规子群。这里的因子 K_4 本身并不是单群，正说明主序列与合成序列的要求不同。
$\mathbb{Z}_{15}$ 可以先取 3 阶或 5 阶子群，得到顺序相反的 $\mathbb{Z}_3, \mathbb{Z}_5$ 两个因子。$\mathbb{Z}_4$ 与 K_4 的合成因子又都为两个 $\mathbb{Z}_2$，却仍不同构。Jordan–Hölder 定理确定的是这些因子及其出现次数，并没有确定将它们组成原群的扩张方式。

1.8 可解群和幂零群

上一节把群逐层分解成商群，现在我们再对这些因子提出要求：如果每一层的乘法都是交换的，原群会有什么性质？先从一个商群 G/N 看起。要使 gN 与 hN 交换，就是要求

$$(gN)(hN) = (hN)(gN) \iff g^{-1}h^{-1}gh \in N.$$

所以，要让所有陪集交换，N 必须包含所有这种形式的元素，以及它们生成的子群。这个计算引出换位子，也给出了寻找交换商群的直接办法。

定义 1.8.1 (换位子). $[g,h] = g^{-1}h^{-1}gh$ 称换位子。对 $H, K < G$，令

$$[H,K] = \langle [h,k] : h \in H, k \in K\rangle.$$

特别地，$[G,G]$ 称 G 的换位子群。这里必须取生成子群，不能直接把换位子全体当成子群。

先记录换位子在同态和共轭下的行为，随后才能反复使用这个构造。

引理 1.8.2 (换位子的基本性质). $[g,h]^{-1} = [h,g]$，且 $[g,h] = e \iff gh = hg$。同态 f 满足 $f([g,h]) = [f(g), f(h)]$。若 $H, K \trianglelefteq G$，则 $[H,K] \trianglelefteq G$ 且 $[H,K] \subseteq H \cap K$。

证明. 前几式直接计算。共轭把 $[h,k]$ 送到 $[ghg^{-1}, gkg^{-1}]$，所以保留生成子群；正规性还给出 $h^{-1}k^{-1}hk \in H \cap K$。 □

在商群中要求所有换位子都变成幺元，就把交换性转化成一个包含关系。

引理 1.8.3 (交换商群的判别). 若 $N \trianglelefteq G$, 则 G/N 为 Abel 群, 当且仅当 $[G,G] \subseteq N$。因此 $G/[G,G]$ 是 Abel 群。

证明. 在自然投影下，gN, hN 交换当且仅当 $[g,h] \in N$。 □

$G/[G,G]$ 已经交换，但 $[G,G]$ 本身未必交换。可以对它再取一次换位子群，继续检查还剩下哪些不交换的元素。这给出导出列。

另一种更强的要求是：下一项要包含当前项的元素与整个 G 中元素的换位子，而不只是当前项内部的换位子。这样每个相邻商都会处于相应商群的中心。它给出降中心列。两种列的第二项相同，都是 $[G,G]$，从第三项开始才可能分开。

定义 1.8.4 (导出列与降中心列)**.** 递归定义

$$G^{(0)}=G,\quad G^{(i+1)}=[G^{(i)},G^{(i)}],$$
$$G^{1}=G,\quad\ G^{i+1}=[G,G^{i}].$$

它们分别称导出列与降中心列。若某个 $G^{(r)}=\{e\}$，称 G 可解；若某个 $G^{r}=\{e\}$，称 G 幂零。

自同构将 $[a,b]$ 送到相应像的换位子，所以归纳可知两种列的各项在所有自同构下都不变，特别在内自同构下不变，因而正规于 G。各列也是降链：当前项正规，故与 G 或自身取换位子仍留在当前项中。

从 $G^{(0)}=G^{1}$ 开始归纳，若 $G^{(i)}\subseteq G^{i+1}$，则

$$G^{(i+1)}=[G^{(i)},G^{(i)}]\subseteq[G,G^{i+1}]=G^{i+2}.$$

因此降中心列若到达 1，导出列也会到达 1，即幂零蕴含可解。反向是否成立，需要另看例子。

若已经知道 N 与 G/N 可解，我们希望据此判断 G。关键是把两次终止接起来：商群的导出列先让 G 的某一项落入 N，随后 N 的导出列再让它到达 1。

引理 1.8.5 (可解性的传递)**.** 可解群的子群、商群均可解。若 $N\trianglelefteq G$，则 G 可解当且仅当 N 与 G/N 都可解。

证明. 对 $H<G$，换位子的定义给出 $H^{(i)}\subseteq G^{(i)}$，所以 G 的导出列到达 1 时，H 的也到达 1。对满同态 f，每个像中的换位子都有原像中的换位子作为原像，故归纳得 $f(G^{(i)})=f(G)^{(i)}$；商群的可解性由此得到。

反过来，设 $(G/N)^{(r)}=1$。对自然投影应用刚才的等式，得到 $G^{(r)}\subseteq N$。若又有 $N^{(s)}=1$，则连续 s 次取换位子群给出

$$G^{(r+s)}=(G^{(r)})^{(s)}\subseteq N^{(s)}=1.$$

所以 G 可解。必要性已经包含在子群、商群的结论中。 □

有限情形下，可解性完全由合成因子的类型决定。

定理 1.8.6 (有限可解群的刻画)**.** 有限群 G 可解，当且仅当它有因子均为 Abel 群的正规序列；等价地，有因子均为 Abel 群的次正规序列；又等价于其合成因子均为素数阶循环群。

证明. 若 G 可解，导出列到达 1。各项正规于 G，且相邻因子由引理 1.8.3 为 Abel 群；删去重复项便得到所需正规序列。正规序列当然也是次正规序列。

若已有 Abel 因子的次正规序列，由有限性可在每个因子中取合成序列，再沿商映射取原像插回原链。这些更细的因子仍是 Abel 群，因为交换群的子群与商群都交换；它们又是单群，由定理 1.5.6 必为素数阶循环群。

反过来，若合成因子都是素数阶循环群，它们都可解。从最底部的平凡群开始，对每一层用引理 1.8.5，依次得到上一项可解，最后得到 G 可解。定理 1.7.10 又保证某一条合成序列满足这个因子条件时，所有合成序列都满足。 □

例 1.8.7 (可解与幂零的区别). 令 $s=(12)$、$r=(123)$。$S_3/A_3\cong\mathbb{Z}_2$ 交换，所以 $[S_3,S_3]\subseteq A_3$；另一方面，$srs=r^{-1}$ 给出

$$[s,r]=s^{-1}r^{-1}sr=r^2\neq e.$$

它生成 A_3，因此 $S_3^{(1)}=A_3$。A_3 交换，故 $S_3^{(2)}=1$，S_3 可解。
同一计算还说明 $[S_3,A_3]=A_3$：包含关系来自 A_3 的正规性，反向由 $[s,r]$ 生成 A_3 得到。于是降中心列从第二项起一直等于 A_3，不能到达 1，所以 S_3 不幂零。
当 $n\geq 5$ 时，A_n 非交换，故其换位子群非平凡；它又正规，单性便迫使 $[A_n,A_n]=A_n$。因此 A_n 不可解，包含它的 S_n 也不可能可解。

幂零性也能传到子群和商群，但在扩张时需要更强的条件。

引理 1.8.8 (幂零性的传递). 幂零群的子群、商群都幂零。若 $N\subseteq C(G)$ 且 G/N 幂零，则 G 幂零。

证明. 限制或投影降中心列即得第一句。若 $(G/N)^r=1$，则 $G^r\subseteq N\subseteq C(G)$，所以 $G^{r+1}=1$。S_3 的例子说明任意幂零群的扩张未必幂零。 □

降中心列从 G 往下取子群。还可以反过来从中心开始：先取所有与 G 中每个元素交换的元素；商去它们之后，再取商群的中心，并把这些陪集的全部原像取回来。

例如第二步加入的 g 未必在原群中与每个 h 交换，但 $gC(G)$ 与 $hC(G)$ 交换，也就是说 $[g,h]\in C(G)$。以后每一步都用前一项作为允许出现的换位子范围，这就得到升中心序列。

定义 1.8.9 (升中心序列). 令 $C_0(G)=\{e\}$，$\pi_i:G\to G/C_i(G)$ 为自然投影，并定义

$$C_{i+1}(G)=\pi_i^{-1}\big(C(G/C_i(G))\big).$$

所得升链称升中心序列，特别地 $C_1(G)=C(G)$。

要比较两种中心序列，不能只凭一个上升、一个下降就断言它们等价。我们需要检验中心条件 $G_i'/G_{i+1}'\subseteq C(G/G_{i+1}')$：它恰好说 $[G,G_i']\subseteq G_{i+1}'$。有了这一步，就能把任意满足此条件的序列与升中心序列逐项比较。

定理 1.8.10 (幂零群的刻画). 以下条件等价：

1. G 幂零；
2. 存在正规序列 $G=G_1'\supseteq\cdots\supseteq G_t'=1$，满足 $[G,G_i']\subseteq G_{i+1}'$；
3. 存在这样的正规序列，满足 $G_i'/G_{i+1}'\subseteq C(G/G_{i+1}')$；
4. 存在 r 使 $C_r(G)=G$。

证明. 降中心列给出第二个条件，而第二、三个条件由商群中的换位子直接等价。由第三个条件，我们从 $G'_t = 1 = C_0(G)$ 开始归纳。设 $G'_{t-k} \subseteq C_k(G)$，则图 1.2 中的商映射 μ 存在且满。满同态把中心送入中心，所以

$$\mu\big(G'_{t-k-1}/G'_{t-k}\big) \subseteq \mu\big(C(G/G'_{t-k})\big) \subseteq C(G/C_k(G)).$$

具体地，图中 $\sigma(g) = gG'_{t-k}$，$\pi(g) = gC_k(G)$，$\mu(gG'_{t-k}) = gC_k(G)$；包含关系保证 μ 良定义，且 $\pi = \mu\sigma$。上面的中心包含说明每个 $g \in G'_{t-k-1}$ 都满足 $\pi(g) \in C(G/C_k(G))$，即 $g \in C_{k+1}(G)$。所以 $G'_{t-k-1} \subseteq C_{k+1}(G)$。因此 $G = G'_1 \subseteq C_{t-1}(G)$，得到第四个条件。

反之，若 $C_r(G) = G$，则 $G/C_{r-1}(G)$ 为 Abel 群；再依次应用引理 1.8.8 于中心扩张，得到 $G/C_{r-2}(G), \dots, G$ 均幂零。 □

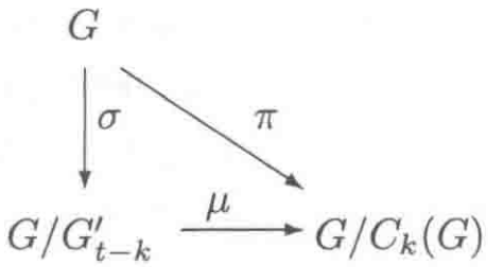


图 1.2: 中心序列与升中心序列的比较。σ, π 为自然投影，$\pi = \mu\sigma$。

因此非平凡幂零群必有非平凡中心：取降中心列最后一个非平凡项，它包含在 $C(G)$ 中。

1.9 群在集合上的作用

我们已经用左平移将一个群实现为置换群。现在不必把群作用的对象限制为群本身：矩阵可以移动向量，正交矩阵可以移动球面上的点，群元素也可以移动某个子群的陪集。

这些例子都有共同规律：先用 h 移动，再用 g 移动，应该与一次使用 gh 相同；幺元应保持每个点不动。把规律写清之后，我们就能反过来利用点的运动研究群。例如，一个点能够到达多少位置，取决于有多少群元素把它留在原处；那些把所有点都留在原处的元素，又组成一个正规子群。

定义 1.9.1 (群作用). 群 G 在非空集合 X 上的作用是映射 $G \times X \to X$，记为 $(g, x) \mapsto gx$，满足

$$ex = x, \qquad (gh)x = g(hx).$$

定理 1.9.2 (作用与置换同态). G 在 X 上的作用，与同态 $\rho : G \to S_X$ 一一对应，关系为 $\rho(g)(x) = gx$。

证明. 作用中 $x \mapsto gx$ 的逆为 $x \mapsto g^{-1}x$，故确为置换；结合条件正是 $\rho(gh) = \rho(g)\rho(h)$。反向定义同样满足两个公理。 □

例 1.9.3 (常见作用). G 在自身上有三种常见作用：左平移 $g\cdot x=gx$，右侧平移 $g\cdot x=xg^{-1}$，以及伴随作用 $g\cdot x=gxg^{-1}$。右侧平移中的逆不能去掉，因为

$$g\cdot(h\cdot x)=(xh^{-1})g^{-1}=x(gh)^{-1}=(gh)\cdot x.$$

若直接写 xg，复合次序就反过来。对任意 $H<G$，公式 $g\cdot(xH)=(gx)H$ 给出陪集作用：换 x 为 xh 只把 gx 换成同一陪集的代表，不要求 H 正规。
矩阵群对列向量的自然作用是 $v\mapsto Tv$。对矩阵本身，相似的左作用为 $A\mapsto TAT^{-1}$；若写合同的左作用，可取 $A\mapsto TAT^{\mathsf{T}}$，因为连续用 S,T 后得到 $(TS)A(TS)^{\mathsf{T}}$。通常的 $T^{\mathsf{T}}AT$ 也描述相同的合同等价类，但按这个参数写法直接复合会反序。这里的作用保持对称矩阵和反对称矩阵的集合。

先区分整个集合能否互相到达，以及不同群元素是否真的产生不同变换。

定义 1.9.4 (可递、有效与平凡作用). 若任意 $x,y\in X$ 存在 g 使 $gx=y$，称作用可递，X 称齐性空间。若固定所有点的 g 只能是 e，称作用有效；若每个 g 都固定所有点，称作用平凡。

有效与平凡分别等价于 ρ 单射与 ρ 为平凡同态。一般作用未必可递，但可以按“互相能到达”分块。

定义 1.9.5 (轨道与迷向子群). x 的轨道为 $O_x=\{gx:g\in G\}$，迷向子群为 $F_x=\{g:gx=x\}$。若 $O_x=\{x\}$，称 x 为不动点。

命题 1.9.6 (轨道分解). 轨道构成 X 的分划；G 在每条轨道上的作用可递。$F_x<G$，且若 $y=gx$，则 $F_y=gF_xg^{-1}$。

证明. 关系 $y=gx$ 自反、对称、传递，故轨道是等价类。由 $hx=x$、$kx=x$ 得 $hk^{-1}x=x$，故 F_x 为子群。$hy=y\iff g^{-1}hgx=x$ 给出共轭公式。 □

不同集合上的作用也可能描述同一种结构，比较时应要求双射尊重作用。

定义 1.9.7 (作用等价). 两个 G-集合 X,X' 若有双射 $\varphi:X\to X'$ 满足 $\varphi(gx)=g\varphi(x)$，称其作用等价。

固定 x，$g\mapsto gx$ 当然取遍轨道；但不同的 g 可能到达同一点。直接比较可得 $gx=hx\iff h^{-1}gx=x$，也就是 $h^{-1}g\in F_x$。这与陪集判别完全相同，所以要去掉这种重复，应该把 G 中同一个 F_x 左陪集的元素视为一个元素。

定理 1.9.8 (轨道与陪集). 映射 $G/F_x\to O_x$，$gF_x\mapsto gx$ 是作用等价。因而

$$|O_x|=[G:F_x];\qquad |G|=|O_x||F_x|\quad (G\text{ 有限}).$$

特别地，每个可递作用都等价于某个陪集作用。

证明. $gx=hx\iff h^{-1}g\in F_x\iff gF_x=hF_x$，所以映射良定义且双射。$\varphi(sgF_x)=sgx=s\varphi(gF_x)$ 给出作用相容性。 □

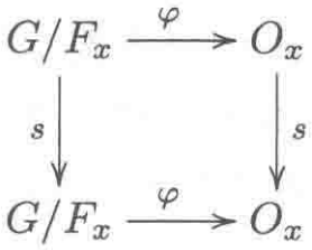


图 1.3: 陪集与轨道的对应尊重群作用：先作用 s 再取像，与先取像再作用 s 相同。

图 1.3 将最后一个等式画成交换方块。左竖箭头把 gF_x 送到 sgF_x，右竖箭头把 gx 送到 $s(gx)$，两条路径都得到 sgx。因此这个双射不仅让两边的元素个数相同，还逐一对应了 G 中每个元素对它们的作用。下面把轨道与迷向子群具体写出，看看这个对应怎样解释熟悉的几何和矩阵分类。

例 1.9.9 (从轨道看熟悉的分类).

1. $SO(2)$ 绕固定轴作用在球面 S^2，轨道为纬线，两极为不动点。
2. $\mathrm{GL}(n,\mathbb{R})$ 在 $\mathbb{R}^n$ 上有 $\{0\}$、$\mathbb{R}^n\setminus\{0\}$ 两条轨道。将任意非零向量补成一组基，就能构造可逆矩阵把它送到另一个非零向量。e_1 的迷向子群则要求矩阵第一列恰为 e_1，故是形如 $\begin{pmatrix}1 & v\\ 0 & A\end{pmatrix}$（$A$ 可逆）的矩阵；$n=1$ 时它就是 $\{1\}$。
3. $n\geq 2$ 时，$SO(n)$ 保持长度，同一长度的非零向量又可由一个保持定向的正交变换互相送到，因此轨道为各个同心球面及原点。固定一个非零向量后，变换在其正交补上的限制恰可任取 $SO(n-1)$ 的元素，所以迷向子群同构于 $SO(n-1)$。
4. 在复数域上，矩阵的相似轨道可用 Jordan 标准形代表。实对称矩阵的合同轨道由 $\mathrm{diag}(I_p,-I_q,0)$ 代表。

共轭作用把已有的共轭类纳入同一套计数方法。

定义 1.9.10 (中心化子与正规化子). 令 $C_G(a)=\{g : ga=ag\}$，$N_G(H)=\{g : gHg^{-1}=H\}$。它们分别是共轭作用在元素 a、子群 H 处的迷向子群。

由定理 1.9.8，$|C_a|=[G:C_G(a)]$，H 的共轭子群个数为 $[G:N_G(H)]$。伴随作用的核是 $C(G)$。在有限群中，把非中心共轭类逐一相加，还得到类方程

$$|G|=|C(G)|+\sum_i [G:C_G(a_i)],$$

其中 a_i 每个非中心共轭类取一个代表。

类方程的每一项都来自一条轨道。特别是当群阶为素数幂时，轨道大小也是素数幂；除单点轨道以外，每一项都会被这个素数整除。下一节将反复利用这一个观察，寻找不动点，再把不动点翻译成子群之间的关系。

1.10 Sylow 定理

Lagrange 定理说子群的阶必须整除群阶，但它没有告诉我们这些因子是否真的对应子群。本节先回答一个较小的问题：若素数 p 整除 $|G|$，能否找到 p 阶元？再逐步把它推广为 p^k 阶子群的存在、Sylow 子群的共轭性与个数限制。

前一节的轨道计数是这里的主要办法。我们会按目标选择作用的集合：为了寻找满足 $a^p = e$ 的元素，先让它们成为某个循环作用的不动点；为了扩大或比较子群，再让子群作用于陪集集合。选择集合以后，最重要的一步始终是写清“不动”究竟对应哪个代数条件。

定理 1.10.1 (Cauchy 定理)**.** 设 G 有限，素数 $p \mid |G|$，则 G 中有 p 阶元。

证明. 直接数 $a^p = e$ 的解不容易，因为乘方一般不是群同态。我们把它们放进一个较容易计数的集合：

$$X = \{(a_1, \dots, a_p) : a_1 \cdots a_p = e\}.$$

前 $p-1$ 个元素可以任取，最后一个由它们唯一决定，所以 $|X| = |G|^{p-1}$，被 p 整除。循环移位保持 X，因为 $a_2 \cdots a_p a_1 = a_1^{-1}(a_1 \cdots a_p)a_1 = e$；移位 p 次恢复原位，因此得到 p 阶循环群的作用。

每条轨道的大小只能为 1 或 p，故单点轨道的个数与 $|X|$ 模 p 同余。不动的元组恰为 $(a, \dots, a)$ 且 $a^p = e$，所以这种解的个数被 p 整除。已知 $a = e$ 是一个解，就至少还有一个非幺元解。它的阶整除素数 p 且不等于 1，因而为 p。 □

素数幂阶的群作用时，所有非单点轨道都贡献 p 的倍数，这会反复出现。

定义 1.10.2 (p-群)**.** 阶为 p^r（$r \geq 0$，p 为素数）的有限群称 p-群。

命题 1.10.3 (p-群作用的计数)**.** p-群 P 作用于有限集 X，设不动点集为 X_0，则 $|X| \equiv |X_0| \pmod{p}$。若 $p \nmid |X|$，则存在不动点。

证明. 非单点轨道的大小是 $|P|$ 的非平凡因子，故被 p 整除。 □

共轭作用的不动点正是中心，因此上述计数立即给出 p-群的一个结构限制。

推论 1.10.4 (p-群的中心与幂零性)**.** 非平凡有限 p-群有非平凡中心；所有有限 p-群均幂零。

证明. 取共轭作用得 $p \mid |C(P)|$，而中心含 e，故 $|C(P)| \geq p$。对 $|P|$ 归纳：商 $P/C(P)$ 更小且幂零，再应用中心扩张引理 1.8.8。 □

从一个 p-子群出发，若它还不够大，就考察它在陪集上的作用；不动点会指出扩大它的位置。

定理 1.10.5 (Sylow 第一定理)**.** 设 $|G| = p^r m$，$p \nmid m$。对每个 $0 \leq k \leq r$，G 有 p^k 阶子群。

证明. 从 $H=\{e\}$ 开始，只需证明：一个 p^k 阶子群在 $k<r$ 时总能扩大为 p^{k+1} 阶子群。要在包含 H 的群中取商，先考虑它的正规化子 $N_G(H)$，因为 $H \trianglelefteq N_G(H)$。我们希望证明这个商还有因子 p。

让 H 左作用于 G/H。陪集 gH 被所有 $h\in H$ 固定，当且仅当

$$hgH=gH\ (h\in H) \iff g^{-1}Hg\subseteq H.$$

有限性保证右边两个子群同阶，所以包含即相等。于是固定陪集恰好由 $g\in N_G(H)$ 给出，不动点数就是 $[N_G(H):H]$。

由于 $k<r$，$p\mid[G:H]$。命题 1.10.3 因而给出 $p\mid[N_G(H):H]$；这个数又不为零，因为陪集 H 本身固定。对群 $N_G(H)/H$ 应用 Cauchy 定理，取其中一个 p 阶子群，再取自然映射下的完全原像。原像由 p 个 H 的陪集组成，故阶为 $p|H|=p^{k+1}$。重复这一步，就得到全部所需阶数。 □

把所有能被 p 整除的部分都包含进去，就得到研究结构时最有用的子群。

定义 1.10.6 (Sylow 子群). 若 $|G|=p^rm$、$p\nmid m$，称 G 的 p^r 阶子群为 Sylow p-子群，其个数记为 n_p。

存在性证明通过 $p\mid[G:H]$ 找到扩大子群的空间。若 P 已是 Sylow 子群，情况恰好反过来：$[G:P]=m$ 不被 p 整除。让任意 p-子群 H 作用于 G/P，计数会强迫出现固定陪集，而固定条件正好把 H 放入 P 的一个共轭中。

定理 1.10.7 (Sylow 第二定理). 设 P 为 Sylow p-子群、H 为任意 p-子群，则存在 $g\in G$ 使 $H\subseteq gPg^{-1}$。特别地，所有 Sylow p-子群彼此共轭。

证明. H 作用于 G/P，而 $p\nmid[G:P]$，故存在固定陪集 gP。于是 $hgP=gP$ 对所有 $h\in H$ 成立，即 $g^{-1}Hg\subseteq P$。若两者均为 Sylow 子群，由同阶得相等。 □

共轭性把计数问题转化为一个可递作用，也就能利用轨道大小公式。

引理 1.10.8 (Sylow 子群的个数). $n_p=[G:N_G(P)]$。

证明. 共轭作用在 Sylow 子群集合上可递，P 的迷向子群恰为 $N_G(P)$。 □

轨道公式给出整除限制，再让一个 Sylow 子群作用于全部 Sylow 子群，就能补上模 p 的限制。

定理 1.10.9 (Sylow 第三定理). 在上述记号下，$n_p\mid m$、$n_p\equiv 1\pmod p$。Sylow p-子群正规，当且仅当 $n_p=1$。

证明. 由 $P\subseteq N_G(P)$ 及指数公式，

$$m=[G:P]=[G:N_G(P)]\,[N_G(P):P]=n_p[N_G(P):P],$$

所以 $n_p\mid m$。又因所有 Sylow 子群彼此共轭，P 正规等价于其共轭轨道只有一个元素，亦即 $n_p=1$。

为得到同余条件，令 P 共轭作用于全部 Sylow p-子群的集合。P 本身是不动点；还需证明没有别的不动点。若 Q 固定，则 $P\subseteq N_G(Q)$。P,Q 都有 p^r 个元素，所以也是

$N_G(Q)$ 的 Sylow 子群；但 Q 正规于这个正规化子，其在其中的共轭都等于自己。Sylow 第二定理在 $N_G(Q)$ 中便迫使 $P = Q$。

因此这个作用恰有一个不动点，其余轨道大小都是 p 的倍数，命题 1.10.3 给出 $n_p \equiv 1 \pmod{p}$。 □

下面两个应用分别使用元素计数与作用的核，体现寻找正规子群的不同办法。

例 1.10.10 (12 阶群)**.** 若 $n_3 \neq 1$，则 $n_3 = 4$。四个 3 阶子群两两只交于 e，共有 8 个 3 阶元。任何 4 阶 Sylow 子群只能由余下的四个元素组成，故唯一而正规。因此 12 阶群至少有一个正规 Sylow 子群。

例 1.10.11 (224 阶群非单)**.** $224 = 2^5 \cdot 7$，Sylow 第三定理给出 $n_2 \mid 7$ 且 n_2 为奇数，所以 $n_2 = 1$ 或 7。若为 1，唯一的 32 阶 Sylow 子群已经是非平凡真正规子群。
若为 7，让 G 共轭作用于这七个子群，得到同态 $\rho : G \to S_7$。作用可递且集合不止一个元素，所以 ρ 不是平凡同态，核不等于 G。另一方面，7! 中的因子 2 只有 2^4，而 $|G|$ 含 2^5，所以 $224 \nmid 7!$。若 ρ 单射，Lagrange 定理就会与此矛盾。因此核又非平凡，G 不是单群。

1.11 本章小结

本章先从“能否解开乘法方程”走到群，再从“取出的元素能否独立运算”走到子群。陪集把子群用来给整个群分类，但要使类别之间也能相乘，还必须检查正规性。计算 $(ah_1)(bh_2)$ 时出现的共轭，正是这个附加条件的来源。

同态让商群不再只是一个孤立构造。由 $f(a) = f(b) \iff a^{-1}b \in \operatorname{Ker} f$，每个相同像的原像集合恰好是核的一个陪集，于是得到 $G/\operatorname{Ker} f \cong f(G)$。计算循环群、矩阵商群或比较子群时，都可以先写出映射，再分别求核与像。不能只写两个对象“显然同构”，而不说明元素怎样对应。

沿正规子群逐层取商会得到合成序列。Jordan–Hölder 定理保证合成因子在重排及同构意义下不变；$\mathbb{Z}_4$ 与 K_4 则提醒我们，相同因子仍可组成不同的群。可解性要求分解为交换因子，幂零性还要求相邻因子落在相应商群的中心；S_3 的两种换位子列给出了这一差别的具体计算。

群作用提供了另一条研究路线。明确集合 X 与作用公式后，固定一点的迷向子群决定轨道大小，固定所有点的元素组成作用核。前者用于计数，后者用于找正规子群，两者不能混为一谈。Sylow 定理就是把这种方法用于陪集及子群集合，再结合素数幂的整除性质。以后从一个有限群的阶出发，可以先列出 n_p 的整除、同余限制；若还不能得到唯一性，再像例 1.10.10、例 1.10.11 那样考虑元素数目或作用的核。

下一章加入第二种运算。加法群仍允许我们形成陪集，但商上的乘法必须另外检查。与本章从代表元的改变推出正规性相似，我们将从乘积代表元的改变推出理想条件。

第二章

环

整数、矩阵与多项式不仅能相加，还能相乘。加法使它们成为交换群，乘法却可能不交换，非零元素也未必可逆。我们要研究的环保留这两种运算及其分配律，从而能同时讨论同余、方程和因式分解。

本章沿两个问题展开。首先，怎样把环中的元素按某种同余关系合为一类，同时让加法、乘法都有意义？这引出理想、商环与环同态。其次，整数中熟悉的素因子分解能推广到哪些环？我们会区分不可约与素，分别检查分解能否结束、结果是否唯一，最后把这些方法用于多项式环和对称多项式。

2.1 环的定义与基本性质

群论把一次运算及其逆运算作为研究对象。但在整数中，我们还会比较 $a(b+c)$ 与 $ab+ac$；在矩阵中，也同时使用加法与乘法。这时只分别研究两个运算是不够的，还必须保留它们通过分配律发生的联系。

加法仍按熟悉的交换群处理，因而可以取差；乘法先只要求结合，不要求每个非零元都有逆，也不要求交换。例如整数中的 2 没有整数乘法逆，而矩阵一般不能交换次序，这两类重要例子都应包括进来。

定义 2.1.1 (环)**.** 非空集合 R 有加法和乘法，若 $(R,+)$ 是 Abel 群，乘法满足结合律，并满足

$$a(b+c)=ab+ac,\qquad (a+b)c=ac+bc,$$

则称 R 为环。乘法有幺元时称幺环，乘法可交换时称交换环。只含 0 的环称零环。

本章不默认环有幺元，也不默认交换。加法的逆元记为 $-a$。由分配律及加法消去律，

$$a0=0a=0,\qquad (-a)b=a(-b)=-ab,$$
$$(-a)(-b)=ab,\qquad (ma)(nb)=(mn)(ab)\quad (m,n\in\mathbb{Z}).$$

例如 $a0=a(0+0)=a0+a0$，在加法群中消去一个 $a0$，得到 $a0=0$。再由 $ab+a(-b)=a(b-b)=0$ 得到 $a(-b)=-ab$；另一侧同理，继续取负便得到 $(-a)(-b)=ab$。对整数倍先对正整数反复使用分配律，再借助负元处理负整数，就得到 $(ma)(nb)=(mn)(ab)$。有限和的展开也是同样的归纳，并没有使用乘法交换律。

例 2.1.2 (数、矩阵、多项式与函数)**.** $\mathbb{Z}$、$\mathbb{Z}[\sqrt{d}]=\{a+b\sqrt{d}:a,b\in\mathbb{Z}\}$、数域 P、$P[x]$ 及矩阵环 $P^{n\times n}$ 都是环。$\mathbb{Z}[\sqrt{-1}]$ 称 Gauss 整数环。连续函数环 $C(X)$ 和光滑函数环 $C^{\infty}(\mathbb{R}^n)$ 的加法、乘法逐点定义。

在整数中，两个非零元素的积不为零；矩阵和函数却未必如此。这个差别直接决定乘法能否消去。

定义 2.1.3 (零因子). 若 $a, b \neq 0$ 且 $ab = 0$，称 a 为左零因子、b 为右零因子。非零环若没有零因子，称无零因子环。

命题 2.1.4 (消去与零因子). 环没有零因子，当且仅当非零元素满足左右消去律。

证明. $ax = ay$ 等价于 $a(x-y) = 0$。无零因子且 $a \neq 0$ 时得到 $x = y$；反向取 $y = 0$。右边同理。 □

例 2.1.5 (不能任意消去). 在 $n \geq 2$ 的矩阵环中，E_{11}, E_{22} 都非零，却有 $E_{11}E_{22} = 0$，因此从 $E_{11}E_{22} = E_{11}0$ 不能约去 E_{11}。
在 $C([0,1])$ 中，令 $f(x) = \max(0, \frac{1}{2} - x)$、$g(x) = \max(0, x - \frac{1}{2})$。$f$ 只可能在左半区间非零，g 只可能在右半区间非零，所以每一点处至少有一个因子为零，$fg = 0$；但两个函数本身都不是零函数。

无零因子还会限制加法。例如假设某个非零 a 满足 $na = 0$，想知道另一个 b 是否也满足 $nb = 0$。分配律给出 $a(nb) = (na)b = 0$，于是便能通过约去非零的 a，把一个元素的加法关系传到其他元素。

命题 2.1.6 (非零元的加法阶). 无零因子环的非零元素具有相同的加法阶；这个共同阶若有限，则为素数。

证明. 若 $a \neq 0$ 且正整数 n 满足 $na = 0$，则任意 b 都满足 $a(nb) = (na)b = 0$，无零因子性推出 $nb = 0$。所以任意两个非零元素被同一批正整数消成零：若有有限阶，彼此的阶互相整除，从而相同；若没有这样的正整数，就全为无限阶。

设共同的有限阶 n 是合数，写成 $n = rs$，其中 $1 < r, s < n$。对任意非零 a，由阶的最小性知 ra, sa 均非零，但

$$(ra)(sa) = rs\,a^2 = (na)a = 0,$$

与无零因子矛盾。因此 n 只能是素数。 □

现在可以用一个数记录这种共同的加法行为。

定义 2.1.7 (特征). 无零因子环中非零元素的加法阶无限时，记 $\operatorname{Ch} R = 0$；共同阶为素数 p 时，记 $\operatorname{Ch} R = p$。

命题 2.1.8 (特征 p 的幂公式). 若 R 为特征 p 的无零因子交换环，则对 $r \geq 0$ 有

$$(a+b)^{p^r} = a^{p^r} + b^{p^r}, \qquad (a-b)^{p^r} = a^{p^r} - b^{p^r}.$$

证明. $p \mid \binom{p}{k}$ $(0 < k < p)$，故交换性允许使用的二项式展开中，所有中间项均为零。迭代得到 p^r 次幂情形。减法公式由加法公式及负元的唯一性得到。 □

特征 p 的幂公式之所以能成立，既用到了中间二项式系数被 p 整除，也用到了乘法交换，从而可以合并展开中的同类项。进入一般环以后，熟悉的整数或多项式计算仍可使用，但需要逐次确认原计算究竟在哪一步用了交换、消去或可逆。

2.2 理想与商环

上一章已经知道怎样给群取子群和商群。环的加法是交换群，所以任意加法子群 I 都允许形成加法陪集 $a+I$，也能定义陪集加法。我们想进一步让它们相乘：$(a+I)(b+I)=ab+I$。问题又落在代表元的改变上。

在做这个检查之前，先分清两类子集。子环只要求选出的元素彼此运算后仍在其中；为了取商，稍后还会要求它们乘上原环中任意元素后仍留在其中。后一要求比子环性强，这正是理想与子环的区别。

定义 2.2.1 (子环)**.** 非空子集 $S\subseteq R$ 若对原加法、乘法构成环，称为子环；不要求它包含原环的幺元。

命题 2.2.2 (子环判别)**.** S 为子环，当且仅当对所有 $a,b\in S$ 有 $a-b,ab\in S$。

证明. 差封闭保证加法子群，乘积封闭保证乘法半群，其余公理由 R 继承。 □

$\mathbb{Z}$ 的子环为 $m\mathbb{Z}$；$\mathbb{Z}^{n\times n}$ 是 $P^{n\times n}$ 的子环；$C^{\infty}(\mathbb{R}^n)$ 是 $C(\mathbb{R}^n)$ 的子环。

尝试定义 $(a+I)(b+I)=ab+I$ 时，若 $a-a',b-b'\in I$，则

$$ab-a'b'=a(b-b')+(a-a')b'.$$

所以 I 不仅要对内部乘法封闭，还要能吸收任意外部因子的乘法。

定义 2.2.3 (理想)**.** 子环 $I\subseteq R$ 若 $RI\subseteq I$，称左理想；若 $IR\subseteq I$，称右理想；两者兼具称双边理想，简称理想。$0,R$ 称平凡理想。

命题 2.2.4 (理想判别与生成)**.** 非空 $I\subseteq R$ 是理想，当且仅当它对差及左右乘任意 R 中元素封闭。任意族理想的交仍是理想；包含子集 S 的所有理想之交为包含 S 的最小理想，记为 (S)。

证明. 判别法由定义立即得到；逐项检查差与吸收性即得交仍是理想。交包含 S 且包含于每个候选理想中，故为最小者。 □

单个元素生成的理想经常足以控制商环，我们给它一个名称并写出具体形式。

定义 2.2.5 (主理想)**.** 形如 (a) 的理想称主理想。在交换幺环中，(S) 由有限和 $\sum r_is_i$ 组成，特别地 $(a)=Ra$。在交换但未必有幺元的环中，$(a)=Ra+\mathbb{Z}a$；一般幺环中，(a) 由有限和 $\sum r_ias_i$ 组成。

这些公式可以用“必须加入什么”来理解。在交换幺环中，包含 a 的理想必须包含每个 ra；反过来，Ra 对差和乘任意环元素都封闭，且 $a=1a$ 在其中，故 $(a)=Ra$。若没有幺元，就不能用 $1a$ 保证包含 a，因此必须另外加入它的整数倍，得到 $Ra+\mathbb{Z}a$。

一般幺环中乘法可能不交换，一个包含 a 的双边理想必须同时容许左右乘，因而包含所有有限和 $\sum r_i a s_i$。这些和本身构成理想并包含 $a = 1a1$，故恰为 (a)。多个生成元的公式也按同一方法验证。

例 2.2.6 (函数环中的理想). $\{f \in C(\mathbb{R}) : f(x_0) = 0\}$ 是理想。在 $C^\infty(\mathbb{R}^n)$ 中，O_x 表示在 x 的某个邻域内恒为零的光滑函数全体，也是理想：两个这样的邻域可取交，乘任意光滑函数仍在该邻域消失。

吸收性正好消除了代表元的影响，现在可以完成商环构造。

定理 2.2.7 (商环). 若 I 为 R 的理想，则加法商群 R/I 配上乘法 $(a+I)(b+I) = ab+I$ 构成环。交换性与幺元均可传到商环，幺元为 $1 + I$。

证明. 加法商群已经构造好。若 $a - a', b - b' \in I$，则

$$ab - a'b' = a(b - b') + (a - a')b' \in I,$$

所以 $ab+I = a'b'+I$，乘法与代表元无关。结合律如 $((a+I)(b+I))(c+I) = (ab)c+I = a(bc) + I$，分配律也从 R 中的等式得到。若 R 交换，陪集乘法也交换；若 R 有幺元，$1 + I$ 乘任意陪集保持其不变。

若 $I = R$，商为零环；它仍满足这些环公理。因此若之后希望商成为整环或域，必须另外要求 I 是真理想。 □

例 2.2.8 (剩余类与函数芽). 对 $m \geq 1$，$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$ 的加法、乘法均按模 m 计算：先用整数代表计算，再取余数，换代表不改变结果。
$C^\infty(\mathbb{R}^n)/O_x$ 中两个函数的陪集相同，当且仅当差在 x 的某个邻域恒为零，也就是两个函数在某个邻域内一致。其元素称函数芽。这里并非只比较 x 这一个点的函数值：例如在 $\mathbb{R}$ 上，零函数与 $t \mapsto t$ 在 0 的值相同，但在任何 0 的邻域都不一致，所以它们在 0 的函数芽不同。

下面按可逆性区分几种环。注意“单位”指可逆元，“幺元”仅指 1。

定义 2.2.9 (整环、除环与域). 非零幺环的可逆元全体构成单位群 $U(R)$。无零因子的交换幺环称整环；非零幺环若每个非零元均可逆，称除环；交换的除环称域。

例 2.2.10 (有限域的第一个例子). p 为素数时，$\mathbb{Z}_p$ 是域：对 $\bar{a} \neq 0$，$\gcd(a, p) = 1$，故存在 $u, v \in \mathbb{Z}$ 使 $ua + vp = 1$，于是 $\bar{u}\bar{a} = 1$。合数 m 的 $\mathbb{Z}_m$ 则有零因子。

$\mathbb{Z}_p$ 的例子把两个原先不同的问题连起来了：商环来自理想 (p)，而非零陪集可逆又依赖 p 是素数。稍后我们会问，什么样的理想让商环成为整环或域。此前先看一个非交换的除环，明确“非零元都可逆”并不强迫乘法交换。

2.3 四元数体

复数把一个实数扩为两个实坐标，并且每个非零元素仍可逆。是否还能找到由四个实坐标表示、每个非零元均可逆的对象？本节构造四元数，它将说明除环可以不交换。

如果直接在 $\mathbb{R}^4$ 上列一张乘法表，我们还得逐项检验结合律。更方便的办法是在一个已知结合的矩阵环中找子环：只要对加减乘封闭，结合律就自动继承。我们取下面这种由两个复数决定的 2×2 矩阵，再检查它的逆是否仍有同样形式。

例 2.3.1 (四元数的矩阵实现). 令

$$\mathbb{H}=\left\{A(\alpha,\beta)=\begin{pmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{pmatrix}:\alpha,\beta\in\mathbb{C}\right\}.$$

直接相乘得

$$A(\alpha,\beta)A(\gamma,\delta)=A(\alpha\gamma-\beta\bar{\delta},\ \alpha\delta+\beta\bar{\gamma}).$$

故 $\mathbb{H}$ 对加减乘封闭且包含单位矩阵，是 $\mathbb{C}^{2\times 2}$ 的幺子环。若 $(\alpha,\beta)\neq(0,0)$，则

$$A(\alpha,\beta)^{-1}=\frac{1}{|\alpha|^2+|\beta|^2}\begin{pmatrix}\bar{\alpha} & -\beta\\ \bar{\beta} & \alpha\end{pmatrix}\in\mathbb{H}.$$

因此 $\mathbb{H}$ 是除环。

矩阵构造已经保证了结合律与可逆性，但还没直接展示四个实坐标各自如何相乘。写 $\alpha=a+bi$、$\beta=c+di$，矩阵便唯一拆成单位矩阵与下面三个矩阵的实线性组合。把它们依次记作 $\mathbf{i},\mathbf{j},\mathbf{k}$，就得到通常的四元数写法。

定义 2.3.2 (四元数). 令

$$\mathbf{i}=\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix},\quad \mathbf{j}=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\quad \mathbf{k}=\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}.$$

$\mathbb{H}$ 的元素唯一写为 $a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$ $(a,b,c,d\in\mathbb{R})$，称四元数；$\mathbb{H}$ 称四元数体。乘法由分配律及

$$\mathbf{i}^2=\mathbf{j}^2=\mathbf{k}^2=-1,$$
$$\mathbf{ij}=\mathbf{k}=-\mathbf{ji},\quad \mathbf{jk}=\mathbf{i}=-\mathbf{kj},\quad \mathbf{ki}=\mathbf{j}=-\mathbf{ik}$$

决定，所以它不是交换环。

对 $q=a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$，记 $\bar{q}=a-b\mathbf{i}-c\mathbf{j}-d\mathbf{k}$，则

$$q\bar{q}=\bar{q}q=a^2+b^2+c^2+d^2,\qquad q^{-1}=\frac{\bar{q}}{a^2+b^2+c^2+d^2}\quad(q\neq 0).$$

也可把 $a+b\mathbf{i}$ 视为复数 α，把 $c+d\mathbf{i}$ 视为复数 β，写成 $q=\alpha+\beta\mathbf{j}$。由于 $\mathbf{ji}=-\mathbf{ij}$，有 $\mathbf{j}\alpha=\bar{\alpha}\mathbf{j}$。于是

$$(\alpha+\beta\mathbf{j})(\gamma+\delta\mathbf{j})=(\alpha\gamma-\beta\bar{\delta})+(\alpha\delta+\beta\bar{\gamma})\mathbf{j},$$

恰好回到矩阵乘法的公式。共轭来自把复系数移过 $\mathbf{j}$ 时的反交换关系；它不是额外附加的运算规则。虽然名称叫“四元数体”，这里得到的是除环，不能当作交换域使用。

2.4 环的同态

自然映射 $R \to R/I$ 同时保持加法与乘法；函数取值也是如此，先相加或相乘再取值，与先取值再计算结果相同。因此，环之间合适的比较映射应当同时保留这两种运算。

群论的核与商的证明仍能提供主要步骤，因为环同态首先是加法群同态。不过，加法子群还不够成为理想，我们要另外验证它对环中乘法的吸收性。同样，最后得到的双射还必须保持乘法，才能称为环同构。

定义 2.4.1 (环同态). 映射 $f : R \to S$ 若满足 $f(a+b) = f(a)+f(b)$、$f(ab) = f(a)f(b)$，称环同态。单同态、满同态、同构按映射的单、满、双射定义。本定义不默认 $f(1) = 1$；需要保持幺元时会明确说明。

同态保持 0、负元；复合仍为同态，同构的逆仍为同构。核 $\operatorname{Ker} f = f^{-1}(0)$ 为理想，因为 $f(ra) = f(r)f(a) = 0$，右乘同理。像为子环，而非一般意义下陪域的理想。

例 2.4.2 (几个基本同态). 自然投影 $R \to R/I$、取值映射 $C^\infty(\mathbb{R}^n) \to \mathbb{R}$，$f \mapsto f(x_0)$，均为满同态。选定基后，$\operatorname{End} V \to P^{n\times n}$ 是环同构。零映射也是环同态。

对环同态，$f(a) = f(b) \iff f(a-b) = 0$，所以相同像的原像集合恰是 $\operatorname{Ker} f$ 的加法陪集。这已经说明应该定义 $a + \operatorname{Ker} f \mapsto f(a)$。接下来只需检查陪集乘法与像中的乘法相符，就能把加法群同构加强为环同构。

定理 2.4.3 (环的同态基本定理与对应). 同态 $f : R \to S$ 诱导环同构 $R/\operatorname{Ker} f \cong f(R)$，$a + \operatorname{Ker} f \mapsto f(a)$。若 f 满，则 R 中含 $\operatorname{Ker} f$ 的子环与 S 的子环一一对应，理想对应于理想；若 $I \supseteq \operatorname{Ker} f$ 是理想，则 $R/I \cong S/f(I)$。

证明. 令 $K = \operatorname{Ker} f$。加法群的同态基本定理给出良定义的加法群同构 $\bar f : R/K \to f(R)$；再算

$$\bar f((a+K)(b+K)) = f(ab) = f(a)f(b) = \bar f(a+K)\bar f(b+K),$$

便得到环同构。

满射时，取像与完全原像对含核的加法子群已经互逆；乘法封闭性也沿着这两个操作传递，所以子环互相对应。对于理想，原像的吸收性由 $f(ra) = f(r)f(a)$ 直接得到；像的吸收性则要用满射。具体说，若 $a \in I$、$s \in S$，选 $r \in R$ 使 $f(r) = s$，便有 $sf(a) = f(ra) \in f(I)$，右乘同理。这说明为什么这里不能省去满射条件。

最后，复合同态 $R \to S \to S/f(I)$ 的核为 $f^{-1}(f(I)) = I$，像为整个 $S/f(I)$，应用刚证明的基本定理即可。 □

图 2.1 画的是 f 为满射的情形。沿斜箭头，a 直接到 $f(a)$；沿上方再向下，先到 $a+K$，再由 $\bar f$ 到 $f(a)$，所以 $f = \bar f\pi$。一般同态只需把右下角的陪域改为 $f(R)$，最后再接入 S。复合商映射与限制商映射，分别给出下面两个常用的同构。

推论 2.4.4 (商的商与理想的和). 若 $I \subseteq J$ 为理想，则 $(R/I)/(J/I) \cong R/J$。一般地，$I + J = \{a + b : a \in I, b \in J\}$ 是理想，且

$$(I+J)/I \cong J/(I \cap J).$$

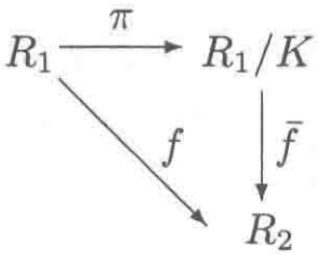


图 2.1: 满同态的分解。图中 $R_1 = R$、$R_2 = S$、$K = \operatorname{Ker} f$，且 $f = \bar{f}\pi$。

证明. 第一式应用对应定理；第二式限制自然同态于 J，其核为 $I \cap J$，像为 $(I+J)/I$。 □

有些自然映射会颠倒乘法顺序，转置就是一个例子。我们把这一情形单独记录。

定义 2.4.5 (反同态与半同态)**.** 加法群同态 $\varphi : R \to S$ 若满足 $\varphi(ab) = \varphi(b)\varphi(a)$，称反同态；双射的反同态称反同构。若对每对 a, b，至少有

$$\varphi(ab) = \varphi(a)\varphi(b) \quad \text{或} \quad \varphi(ab) = \varphi(b)\varphi(a)$$

之一成立，称半同态。

矩阵转置与四元数共轭都是反同构。令 R^{op} 与 R 有相同加法，而乘法 $a \circ b = ba$，则恒等映射 $R \to R^{\mathrm{op}}$ 为反同构。

半同态允许一对元素按原顺序相乘，另一对元素按反顺序相乘，看起来比同态或反同态宽松很多。但这些选择必须同时与加法相容，不能任意切换。证明将用一个简单观察：一个群若等于两个子群的并，其中必有一个已经是全群。先固定第一个因子使用一次，再对第一个因子整体使用一次，就能让次序在全环统一。

定理 2.4.6 (华罗庚半同态定理)**.** 任意环的半同态必为同态或反同态。

证明. 先说明所用的子群事实。若两个子群之一包含另一个，则它们的并就是较大的一个；若互不包含，取 $x \in H \setminus K$、$y \in K \setminus H$，则 xy 既不在 H 也不在 K，否则用逆元便会推出 $y \in H$ 或 $x \in K$。所以两个真子群的并不可能是全群。

固定 $a \in R$，令

$$L_a = \{b : \varphi(ab) = \varphi(a)\varphi(b)\}, \qquad R_a = \{b : \varphi(ab) = \varphi(b)\varphi(a)\}.$$

加法性与分配律使这两个集合都对差封闭。例如 $b, c \in L_a$ 时，$\varphi(a(b-c)) = \varphi(a)(\varphi(b) - \varphi(c))$，故 $b - c \in L_a$。它们都包含 0，所以是加法子群。半同态条件又给出 $L_a \cup R_a = R$。由刚才的事实，固定这个 a 后，至少有一种顺序对所有 b 都成立。

再令 $L = \{a : L_a = R\}$、$T = \{a : R_a = R\}$。这次条件中的“对所有 b”也允许相减：若 $a_1, a_2 \in L$，则对每个 b，

$$\varphi((a_1 - a_2)b) = \big(\varphi(a_1) - \varphi(a_2)\big)\varphi(b) = \varphi(a_1 - a_2)\varphi(b).$$

因此 L 是加法子群，T 同理。前一步给出 $L \cup T = R$，再用一次子群并集事实，得到 $L = R$ 或 $T = R$，即 φ 为同态或反同态。 □

2.5 整环上的因子分解

在整数中，$12 = 2\cdot 2\cdot 3$；如果把某个因子换成它的负数，并同时调整另一个因子的符号，分解仍表示同一个整数。所以谈唯一分解时，必须容许单位倍数和因子的次序改变。

推广到整环还有两个独立的问题。第一，一个非零非单位元素能不能一直分下去，永远到不了不可约元素？第二，即使分解已经结束，两种分解的因子能否逐个对应？前者要控制分解过程的终止，后者则需要一种整除乘积的规则。我们先把这些条件分开，再讨论它们怎样共同给出唯一分解。

定义 2.5.1 (整除、相伴与真因子)**.** 在整环 R 中，$b \mid a$ 指 $a = bc$ 对某个 $c \in R$ 成立。若 $a = ub$，$u \in U(R)$，称 a, b 相伴，记为 $a \sim b$。对非零 a，单位与 a 的相伴元称平凡因子；若 $b \mid a$ 而 $a \nmid b$，称 b 为真因子。

相伴是等价关系；对非零元素，互相整除等价于相伴，因为 $a = bc, b = ad$ 推出 $cd = 1$。

“不能再分”与“整除乘积就整除一个因子”在整数中等价，在一般整环中却要区分。

定义 2.5.2 (不可约元素与素元素)**.** 设 $p \neq 0$ 且 $p \notin U(R)$。若 $p = ab$ 必有 a 或 b 为单位，称 p 不可约；若 $p \mid ab$ 必有 $p \mid a$ 或 $p \mid b$，称 p 为素元素。

乘积的整除性质比不能继续分解更强；先证明这一方向，再看反向失败的例子。

引理 2.5.3 (素元素不可约)**.** 整环中每个素元素都不可约。

证明. 若 $p = ab$，则 $p \mid a$ 或 $p \mid b$。设 $a = pc$，消去非零 p 得 $cb = 1$，故 b 为单位。 □

例 2.5.4 ($\mathbb{Z}[\sqrt{5}]$ 中的区别)**.** 令 $N(a + b\sqrt{5}) = |a^2 - 5b^2|$。对非零元素，这个范数是正整数，且共轭相乘的公式给出 $N(uv) = N(u)N(v)$。若 u 可逆，$N(u)N(u^{-1}) = 1$，所以 $N(u) = 1$；反过来，范数为 1 时，$u^{-1} = \pm\bar{u}$ 仍在 $\mathbb{Z}[\sqrt{5}]$ 中。

现在检验 2 是否不可约。它的范数为 4，若分成两个非单位，两个范数都必须为 2。但 $|a^2 - 5b^2| = 2$ 会给出 $a^2 \equiv 2$ 或 $3 \pmod 5$，而模 5 的平方只能为 $0, 1, 4$，矛盾。因此 2 不可约。

它却不是素元素，因为

$$2 \mid (1 + \sqrt{5})(1 - \sqrt{5}) = -4.$$

若 2 整除 $1 + \sqrt{5}$ 或 $1 - \sqrt{5}$，比较 $1, \sqrt{5}$ 的整数系数，会要求奇数系数被 2 整除，这是不可能的。此例把“自己不能再分”与“整除乘积时能落到某个因子”明确区分开来。

现在研究分解是否会无止境地继续。沿着一次不断细分的过程追踪一个因子，就得到下降链。

定义 2.5.5 (有限分解与因子链)**.** 若每个非零非单位元素，无论怎样继续分成两个非单位因子，都在有限步后结束，称满足有限分解条件。若不存在无限序列 $a_1, a_2, \ldots$ 使 a_{i+1} 始终为 a_i 的真因子，称满足因子链条件。

真因子链只沿一个因子往下走，而一次反复分解可以同时在许多因子上继续进行。要证明两种终止条件等价，必须把这种分支也考虑进去。关键在于每次只把一个元素分为两个非单位因子：如果整个分解一直不结束，就能不断选出仍会继续分裂的一支。

定理 2.5.6 (分解终止的判别)**.** 整环的有限分解条件与因子链条件等价。

证明. 无限真因子链直接给出一种不终止的分解。反之，若一次分解过程不终止，把分解记录为二叉树；每个节点只有两个子节点。在具有无穷多个后继的节点处，总有一个子节点仍有无穷多个后继，沿此选择得到无限真因子链。 □

当分解已经存在，就可以提出唯一性；也可以用素性或最大公因子来检验它。

定义 2.5.7 (唯一分解整环与公因子条件)**.** 满足有限分解条件，且不可约分解在次序、相伴意义下唯一的整环称唯一分解整环（UFD）。每个不可约元都是素元，称满足素条件。元素 d 若整除 $a_1,\dots,a_n$，且被它们的每个公因子整除，称为最大公因子。每对元素均有最大公因子，称满足公因子条件。

最大公因子按整除关系定义，并不是比较数值大小。例如多项式也能谈最大公因子。若 d,d' 都满足定义，则二者互相整除，因而在相伴意义下唯一。以下统一写 $\gcd(a,b)$；(a,b) 保留表示由 a,b 生成的理想，避免把元素与理想混写。

下面的三个条件分别从唯一性、整除规律和公因子三个角度刻画同一件事。

定理 2.5.8 (唯一分解的判别)**.** 对整环 R，以下条件等价：R 是 UFD；R 满足因子链条件和素条件；R 满足因子链条件和公因子条件。

证明. 若已有唯一分解，以非零元素不可约因子的个数定义长度 $\ell(a)$，单位长度为 0。若 b 是 a 的真因子，写 $a=bc$，则 c 非单位，故 $\ell(a)=\ell(b)+\ell(c)>\ell(b)$。长度是非负整数，因此不存在无限真因子链。若不可约 $p\mid ab$，且 a,b 均非零，比较 ab 与 pc 的不可约分解，p 必与 a 或 b 的某个因子相伴，故为素元素；零因子的情形直接成立。

反过来，因子链条件保证分解终止，从而存在不可约分解。若不可约元素都是素元素，对 $p_1\cdots p_r=q_1\cdots q_s$，$p_1$ 必整除某个 q_j。由 q_j 不可约，二者相伴；调整一个单位并消去这一对因子，再归纳即可得到全部因子的对应。由此得到 UFD。在 UFD 中取各不可约因子的最小指数，又能构造最大公因子；涉及 0 时取 $\gcd(a,0)\sim a$。

还剩下公因子条件如何给出素条件。先证两个只依赖公因子定义的公式：

$$\gcd(ca,cb)\sim c\gcd(a,b),\qquad \gcd(a,\gcd(b,c))\sim\gcd(\gcd(a,b),c).$$

第二式的两边都恰好代表 a,b,c 的公因子中被所有公因子整除的元素。对第一式，零的情形直接验证；否则令 $d=\gcd(a,b)$、$e=\gcd(ca,cb)$。因为 cd 是 ca,cb 的公因子，有 $e=cdu$。再由 $e\mid ca,cb$ 消去非零 c，得到 $du\mid a,b$，从而 $du\mid d$，迫使 u 为单位。这就证明第一式，未使用待证的素性。

若 $\gcd(a,b)\sim\gcd(a,c)\sim 1$，则

$$\begin{aligned}\gcd(a,bc)&\sim\gcd(\gcd(a,ab),bc)\\&\sim\gcd(a,\gcd(ab,bc))\\&\sim\gcd(a,b\gcd(a,c))\sim 1.\end{aligned}$$

现在取不可约元素 p。若 p 都不整除 a, b，它与二者的最大公因子只能是单位，否则不可约性会迫使该公因子与 p 相伴。上式于是给出 $\gcd(p, ab) \sim 1$，所以 p 也不整除 ab。取逆否命题，便得到 p 为素元素。再结合因子链条件及前面的论证，完成等价性。 □

2.6 素理想与极大理想

商环把 I 中的元素变为零，因此它可能消除原来的一些障碍，也可能使原先非零的乘积变为零。例如 $\mathbb{Z}$ 无零因子，但 $\mathbb{Z}/4\mathbb{Z}$ 中有 $\bar{2}^2 = 0$。我们现在想直接用理想的条件判断，商环何时是整环，何时又是域。

以下除明确说明外，均在交换幺环中讨论。先看无零因子：商中 $(a+I)(b+I) = 0$ 恰好等价于 $ab \in I$。要让至少一个因子在商中为零，就必须从这个条件推出 $a \in I$ 或 $b \in I$。

定义 2.6.1 (素理想). 真理想 $I \neq R$ 若满足 $ab \in I \Rightarrow a \in I$ 或 $b \in I$，称素理想。

定理 2.6.2 (素理想与整环). 交换幺环 R 的真理想 I 为素理想，当且仅当 R/I 是整环。特别地，R 为整环当且仅当 (0) 为素理想。

证明. $(a+I)(b+I) = 0+I \iff ab \in I$，而 $a+I = 0+I \iff a \in I$。真理想条件保证商环非零。 □

例 2.6.3 (整数与剩余类环). $\mathbb{Z}$ 的素理想为 (0) 和 (p)（p 素数）。$\mathbb{Z}_4$ 的理想 $\{0, \bar{2}\}$ 是素理想，零理想则不是，因为 $\bar{2}^2 = 0$。

素性既可以随商同态传递，也可以改写成对两个理想乘积的条件，便于整体操作理想。

定理 2.6.4 (素理想的对应与乘积判别). 满同态 $f : R \twoheadrightarrow S$ 将包含核的素理想对应到素理想。真理想 I 为素理想，当且仅当对任意理想 A, B，$AB \subseteq I$ 蕴含 $A \subseteq I$ 或 $B \subseteq I$；这里 AB 由有限和 $\sum a_i b_i$ 组成。

证明. 第一句由 $R/I \cong S/f(I)$ 及定理 2.6.2 得到。若 I 素而 A, B 均不包含于 I，取 $a \in A \setminus I, b \in B \setminus I$，则 $ab \notin I$，矛盾。反向对 $ab \in I$ 取 $A = (a), B = (b)$，有 $AB = (ab) \subseteq I$，即得所需结论。 □

要让 R/I 成为域，对每个 $a \notin I$ 还必须找到 r，使 $(r+I)(a+I) = 1+I$，即 $1 - ra \in I$。换句话说，1 应属于 $I + (a)$。一个理想包含 1 就是全环，所以要求正是：向 I 加入任何原先不在其中的元素，所生成的理想立即变成 R。这引出极大理想。

定义 2.6.5 (极大理想). 真理想 $M \subsetneq R$ 若没有满足 $M \subsetneq I \subsetneq R$ 的理想 I，称极大理想。

定理 2.6.6 (极大理想与域). R 的理想 M 极大，当且仅当 R/M 是域。因此极大理想必为素理想。

证明. 若 M 极大，取 $a \notin M$，则 $M + (a) = R$，故 $1 = m + ra$，其中 $m \in M$。于是 $(r + M)(a + M) = 1 + M$。反之，域的非零理想含非零元及其乘法逆，因此含 1，只能是全域；利用理想对应，M 极大。 □

例 2.6.7 (素不一定极大). $\mathbb{Z}$ 的极大理想为 (p)，而 (0) 是素理想但非极大理想。域 F 的 (0) 是极大理想。一般地，$F[x, y]$ 中 (x) 是素理想，因为商为 $F[y]$；它非极大，因为 $F[y]$ 不是域。

因此，判别商环时可以依次问两个具体问题：$ab \in I$ 是否迫使一个因子落入 I？每个 $a \notin I$ 是否都能与 I 一起生成 1？前者判别素性，后者判别极大性。在下一节的主理想整环中，理想可以由单个元素生成，这些问题就能直接转回元素的整除与不可约性。

2.7 主理想整环与欧几里得环

上一节用理想判断商环，本节反过来用理想研究因子。在交换幺环中，$a \mid b$ 等价于 $(b) \subseteq (a)$：越能整除别人的元素，生成的理想反而越大。因此，如果每个理想都由一个元素生成，理想的包含关系就能直接用整除关系描述。

我们将先证明这种主理想整环一定具有唯一分解，再解释为何带余除法能保证每个理想都是主理想。这样，整数与域上多项式中熟悉的除法算法就会成为唯一分解的一个充分理由。

定义 2.7.1 (主理想环). 每个理想均为主理想的交换幺环称主理想环；若又是整环，称主理想整环（PID）。

$\mathbb{Z}$ 的理想都是 $m\mathbb{Z} = (m)$，所以它是 PID。$\mathbb{Z}[x]$ 却不是。若 $(3, x) = (g)$，则 $g \mid 3$，次数说明 g 是非零整数；又因 $g \mid x$，比较 x 的系数得 $g = \pm 1$。于是 (g) 应为全环。但 $(3, x)$ 中的多项式都形如 $3u(x) + xv(x)$，常数项被 3 整除，不可能等于 1，矛盾。

先用一个简单的并集观察把无限上升链控制住。

引理 2.7.2 (理想升链的并). 若 $I_1 \subseteq I_2 \subseteq \cdots$ 为理想，则 $\bigcup I_i$ 是理想。

证明. 有限多个指定元素总同时处于某个 I_k 中，故差封闭；任意环元素的左右乘也不离开该项。 □

理想升链的并仍由一个元素生成，就迫使升链停止；不可约元素生成的理想又会给出素性。

定理 2.7.3 (PID 蕴含 UFD). 每个主理想整环都是唯一分解整环。

证明. 按定理 2.5.8，分别证明因子链条件与素条件。

若有无限真因子链，就会得到严格上升的主理想链 $(a_1) \subsetneq (a_2) \subsetneq \cdots$。其并 I 由引理 2.7.2 是理想，PID 条件使它形如 (d)。因为 $d \in I$，必在某一项 (a_k) 中，于是 $(d) \subseteq (a_k) \subseteq I = (d)$，该项已经等于全部的并，之后不可能再严格上升。故因子链条件成立。

再取不可约元素 p。任何包含 (p) 的理想都形如 (a)，而 $(p)\subseteq(a)$ 意味着 $p=ab$。由不可约性，或者 a 是单位，此时 $(a)=R$；或者 b 是单位，此时 $(a)=(p)$。所以 (p) 为极大理想，进而为素理想。

最后把理想的素性译回元素：$p\mid uv$ 即 $uv\in(p)$，因此 $u\in(p)$ 或 $v\in(p)$，即 $p\mid u$ 或 $p\mid v$。素条件成立，故 R 为 UFD。 □

主理想条件还能把最大公因子写成原元素的线性组合，这是随后计算时比唯一分解更直接的工具。

定理 2.7.4 (最大公因子的线性表示)**.** 在 PID 中，若 d 是 a,b 的最大公因子，则存在 $u,v\in R$ 使 $d=ua+vb$，而 $(a,b)=(d)$。

证明. 设理想 $(a,b)=(d_0)$，则 d_0 整除 a,b，且任意公因子都整除 $d_0=ua+vb$，故 $d_0\sim d$；乘上相应单位即得。 □

这比 UFD 的公因子条件更强。例如 $3,x$ 在 $\mathbb{Z}[x]$ 中互素，却不能线性组合成 1。

如何实际证明一个环是 PID? 整数中的办法是选理想里最小的正整数 b，再把任意 a 除以 b。余数仍在理想里，又比 b 小，因此只能是 0，于是每个 a 都是 b 的倍数。

对一般整环未必有大小次序，但可以用一个取非负整数值的函数 δ 代替。我们只要求带余除法能使非零余数的 δ 严格下降，并不要求它真是数值大小或总能唯一确定余数。

定义 2.7.5 (欧几里得环)**.** 整环 R 若有映射 $\delta:R\setminus\{0\}\to\mathbb{N}$，使任意 $a,b\in R$、$b\neq0$ 都可写成 $a=qb+r$，且 $r=0$ 或 $\delta(r)<\delta(b)$，称欧几里得环。

定理 2.7.6 (欧几里得环蕴含 PID)**.** 欧几里得环是主理想整环，因而是 UFD。

证明. 非零理想 I 中选使 $\delta(b)$ 最小的非零元 b。对 $a\in I$ 带余除，余式 $r=a-qb\in I$，由最小性只能为零，故 $I=(b)$。零理想为 (0)。 □

例 2.7.7 (三个欧几里得环)**.** $\mathbb{Z}$ 可取 $\delta(a)=|a|$，域上 $F[x]$ 可取次数。Gauss 整数环 $\mathbb{Z}[i]$ 可取 $\delta(a+bi)=a^2+b^2$：对 $\alpha/\beta=s+ti$，各取最近整数 m,n，令 $q=m+ni$、$r=\alpha-q\beta$，则

$$\delta(r)=\delta(\beta)\big((s-m)^2+(t-n)^2\big)\le\tfrac12\delta(\beta)<\delta(\beta).$$

在 Gauss 整数的例子中，实部与虚部分别取最近整数，使两个方向的误差都不超过 $1/2$，于是平方和不超过 $1/2$；这就是余数范数严格变小的具体原因。域上多项式的次数也有同样作用，后面定理 2.9.3 会在更一般的整环上把除法过程写清。

2.8 环上的多项式

到目前为止，我们经常把 $\mathbb{Z}[x]$、$F[x]$ 当作熟悉的例子。现在要把多项式推广到一般环，并说明它的定义究竟依赖什么。

如果只把多项式理解为“代入一个数后得到的函数”，会在有限域上遇到问题：不同的系数表达式可能处处取相同值。因此，我们先让两个多项式相等的意思严格地等于

“每一项系数相等”，而把代入放在构造之后讨论。一个多项式只含有限个非零系数，故可以从有限支撑的系数序列出发；乘法则按熟悉的逐项展开来定义。

定义 2.8.1 (形式多项式)**.** 对环 R，令 $R[x]$ 为有限支撑序列 $(a_0, a_1, \dots)$ 的集合，加法逐项进行，乘法由卷积

$$(ab)_k = \sum_{i+j=k} a_i b_j$$

定义。若 R 有幺元，令 $x = (0, 1, 0, \dots)$，则每个元素唯一表示为 $\sum_{i=0}^{n} a_i x^i$。非零多项式的最高非零指数称次数，零多项式约定次数为 $-\infty$；首项系数为 1 时称首一。

这个定义的乘法为什么仍结合？两次相乘后，第 m 项系数无论先乘哪两个序列，都是有限和

$$\sum_{i+j+k=m} (a_i b_j) c_k = \sum_{i+j+k=m} a_i (b_j c_k).$$

我们只改了括号，没有交换系数次序，因而对非交换环也成立。分配律同样逐项得到。有限支撑保证乘积仍只有有限个非零项。

常数序列给出嵌入 $a \mapsto (a, 0, \dots)$，我们据此把 R 看作 $R[x]$ 的子环。若 R 有幺元，$x = (0, 1, 0, \dots)$ 乘任何常数 a 都只是把 a 移到一次项，因此 $xa = ax$。这是不定元与系数交换的约定，并没有要求系数之间交换。若没有幺元，系数序列的构造仍有效，但不能照此取出含系数 1 的元素 x。

命题 2.8.2 (次数规则)**.** 对非零多项式 f, g，有 $\deg(f+g) \le \max(\deg f, \deg g)$、$\deg(fg) \le \deg f + \deg g$；后者取等号当且仅当首项系数的积非零。因而整环 R 上的 $R[x]$ 仍为整环，且 $U(R[x]) = U(R)$。

证明. 设 f 的最高项为 ax^m、g 的最高项为 bx^n。相加只能抵消最高项，不会产生更高项，所以有加法不等式。相乘时没有次数高于 $m+n$ 的项，而 x^{m+n} 的系数恰为 ab；它非零时次数才等于 $m+n$，否则次数下降，甚至乘积为零。

若 R 为整环，非零的 a, b 保证 $ab \neq 0$，因此两个非零多项式之积非零；加上继承的交换性与幺元，$R[x]$ 仍为整环。若 $fg = 1$，次数公式给出 $\deg f + \deg g = 0$，故二者都是常数，并且互为 R 中的逆元。反过来 R 的单位当然也是 $R[x]$ 的单位，所以 $U(R[x]) = U(R)$。 □

把指数从一个非负整数改成一组非负整数，即可同时处理多个不定元。

定义 2.8.3 (多元多项式)**.** $R[x_1, \dots, x_n]$ 由有限支撑映射 $\mathbb{N}^n \to R$ 构成，乘法按多重指标卷积定义。幺环情形的元素写为有限和 $\sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$。非零单项式的总次数为 $i_1 + \cdots + i_n$；非零多项式的总次数为其各项总次数的最大值；所有项总次数相同的多项式称齐次多项式。

按 x_n 的幂收集系数，得到自然同构

$$R[x_1, \dots, x_n] \cong \big(R[x_1, \dots, x_{n-1}]\big)[x_n].$$

这也是把一元结论推广到多元的基本归纳方法。

形式构造完成后，才来讨论代入。以下讨论交换幺环及包含它的交换幺环，且要求包含保持幺元。给定扩环中的 a，可把 $\sum r_i x^i$ 送到 $\sum r_i a^i$。分配律与交换律保证这是取值同态，它的像正好包含所有用 a 和 R 中系数作有限次加法、乘法得到的元素。

取值是否会把不同表达式合并，取决于是否存在非零多项式 f 满足 $f(a)=0$。这种等式就是 a 与系数环之间的一条代数关系，下面据此区分代数元与超越元。

定义 2.8.4 (添加元素与代数关系)**.** 记 $R[a]=\{\sum r_i a^i\}$，类似定义 $R[a_1,\dots,a_n]$。若存在非零 $f\in R[x]$ 使 $f(a)=0$，称 a 为 R 上代数元，否则称超越元。若存在非零 $f\in R[x_1,\dots,x_n]$ 使 $f(a_1,\dots,a_n)=0$，称这些元素代数相关；否则称代数无关。

例 2.8.5 (多项式与函数不同)**.** 在 $\mathbb{Z}_p$ 上，x^p-x 是非零的形式多项式，因为它的一次项与 p 次项系数非零。但对每个 $a\in\mathbb{Z}_p$ 都有 $a^p=a$：非零时可在 $p-1$ 阶乘法群中用 Lagrange 定理，$a=0$ 时直接成立。因此 x^p-x 与零多项式在 $\mathbb{Z}_p$ 上给出同一个函数。

这里的区别是：形式多项式比较系数，多项式函数比较所有允许输入处的值。系数不同，并不总能从当前系数环的输入值中看出来。

要让不同的多项式作为函数也不同，不一定要改变系数，只需把允许取值的环扩大。

引理 2.8.6 (扩环后区分多项式)**.** 对交换幺环 R，存在含 R 的交换幺环 S，使 $R[x]$ 中任意两个不同多项式在 S 上定义的函数不同。

证明. 取一个新的不定元 t，令 $S=R[t]$。对 $f(x)=\sum a_i x^i$，在 S 的元素 t 处取值就是 $f(t)=\sum a_i t^i$。若 f,g 系数不同，它们在 t 处的值也有不同系数，因此 $f(t)\neq g(t)$。所以只需把这个形式元素 t 加入允许输入的环，就能区分所有不同的 f,g。这里换用字母 t，是为了区分作为输入的元素与写函数公式时的变量 x。 □

没有代数关系，就意味着每个元素的多项式表达式唯一，这给出不依赖具体序列模型的定义。

定义 2.8.7 (抽象的多项式环)**.** 若 $a_1,\dots,a_n$ 在 R 上代数无关，称 $R[a_1,\dots,a_n]$ 为 R 上的一个 n 元多项式环，$\{a_1,\dots,a_n\}$ 称一组多项式生成元。取值同态给出 $R[x_1,\dots,x_n]\cong R[a_1,\dots,a_n]$。

这里取值映射显然满；其核为所有多项式关系，所以代数无关恰好保证它单射。

特别地，$a_1,\dots,a_n$ 代数无关，当且仅当前 $n-1$ 个元素代数无关，且 a_n 对 $R[a_1,\dots,a_{n-1}]$ 超越。事实上，把关系式写成 $\sum_j f_j(a_1,\dots,a_{n-1})a_n^j=0$：超越性先迫使每个系数为零，前 $n-1$ 个元素的代数无关性再迫使每个 $f_j=0$。反方向则把任何一步的非零关系看成全部变量的关系即可。

还有一种办法描述多项式环：我们可以任意指定各个不定元的像，然后按加法、乘法把这个指定延伸到整个环。因为形式变量之间没有非零多项式关系，任意指定不会与既有关系冲突。

这也解释了为什么代数元不能任意指定像。例如 α 若满足 $\alpha^2+1=0$，保持系数的同态就必须把它送到一个也满足 $b^2+1=0$ 的元素。多项式环没有这种限制，下面的泛性质正是将这个差别写成关于同态的陈述。

定理 2.8.8 (多项式环的泛性质)**.** 设 R, S 为交换幺环，$\sigma : R \to S$ 为保持幺元的同态，$b_1, \dots, b_n \in S$。存在唯一保持幺元的同态

$$\widetilde{\sigma} : R[x_1, \dots, x_n] \to S, \qquad \widetilde{\sigma}|_R = \sigma, \quad \widetilde{\sigma}(x_i) = b_i,$$

其公式为 $\widetilde{\sigma}(\sum r_\nu x^\nu) = \sum \sigma(r_\nu) b^\nu$。反过来，$R[a_1, \dots, a_n]$ 若具有这样的任意指定像的性质，则 a_i 代数无关。

证明. 系数表达式唯一，保证公式良定义；卷积公式保证保持乘法；任何满足要求的同态都必须按此公式取值，故唯一。反向取 $S = R[x_1, \dots, x_n]$、σ 为常数嵌入、$b_i = x_i$；若非零关系 $f(a_1, \dots, a_n) = 0$ 存在，扩充同态会给出 $f(x_1, \dots, x_n) = 0$，矛盾。 □

这里明确要求系数同态保持幺元，是因为变量满足 $x_i = 1x_i$。若允许一般环同态，指定的 b_i 至少必须满足 $\sigma(1)b_i = b_i$，否则这个等式的像已不相容。例如系数上的零同态不能把变量送到一个非零元素。这一条件不能在使用泛性质时悄悄省去。

推论 2.8.9 (多项式环的唯一性与变量置换)**.** 同一个 R 上、指定了同样个数生成元的多项式环之间，存在唯一逐个对应生成元的 R-同构。任意置换生成元都给出唯一的 R-自同构。
若 $\sigma : R \twoheadrightarrow F$ 为保持幺元的满同态，则其扩充满射到 $F[b_1, \dots, b_n]$；此扩充为同构，当且仅当 σ 为同构且 b_i 在 F 上代数无关。

证明. 双向应用泛性质，复合固定系数及所有生成元，因唯一性就是恒等映射。最后一句中满射性来自像的生成性；单射性恰是系数无核且没有新的多项式关系。 □

于是我们有了两种互相配合的看法。系数序列保证多项式环真的存在，代数无关保证表达式唯一，泛性质则让我们构造同态时只需指定系数和变量的像。下一节进一步假定系数环为整环，用次数判断哪些变量替换可逆，以及因式分解能否继续保持唯一。

2.9 整环上的多项式环

在一般环中，相乘的最高项系数可能变成零；整环排除了这个问题，因而次数满足 $\deg(fg) = \deg f + \deg g$。我们将围绕这个公式解决三个问题。

首先，把 x 换为另一个多项式 $g(x)$ 后，还能否用新元素表示原来的 x？其次，除式首项系数不可逆时，怎样修改普通带余除法？最后，如果系数环已有唯一分解，怎样把系数中的常数因子与多项式的非常数因子分开处理？这三步会依次用到次数、首项消去与容度。

定理 2.9.1 (一元多项式环的生成元)**.** 设 R 为整环、$S = R[a]$ 为多项式环。若 $b = g(a)$ 非常数，$\deg g = n > 0$，$f \neq 0$ 且 $\deg f = m$，则 $\deg_a f(b) = mn$。元素 b 是 S 的多项式生成元，当且仅当 $b = ua + v$，其中 $u \in U(R)$、$v \in R$。

证明. 设 f 的首项为 cx^m，g 的首项为 dx^n。代入后最高项为 $cd^m a^{mn}$；整环性保证它非零，而其他项的次数都更低，故 $\deg_a f(b) = mn$。

若 b 是多项式生成元，就有 $a=h(b)$。b 不可能是常数，否则 $h(b)$ 仍为常数；同样 h 非常数。因此次数公式给出 $1=\deg g\deg h$，两者只能都是一次。写 $b=ua+v$、$a=sb+t$，比较 a 的系数得 $su=1$，故 u 可逆。

反过来，若 $b=ua+v$ 且 u 为单位，则 $a=u^{-1}(b-v)$，所以 $R[a]=R[b]$；任何非零 f 代入 b 后仍由次数公式给出非零结果，故 b 也超越，确为多项式生成元。注意次数乘法公式要求 b 非常数；常数代入可能使整个多项式为零。 □

推论 2.9.2 (一元多项式环的自同构)**.** $R[x]$ 的 R-自同构恰为 $x\mapsto ux+v$，$u\in U(R)$、$v\in R$。

证明. 一个固定 R 的自同构由 x 的像唯一决定；它满射时，像元素必须生成整个 $R[x]$，故由定理 2.9.1 形如 $ux+v$。反过来，泛性质给出这类替换同态，替换 $x\mapsto u^{-1}(x-v)$ 是其逆，所以它确为自同构。 □

普通长除法的第一步，是用被除式的首项系数除以除式的首项系数。在 $\mathbb{Z}[x]$ 中，想用 $2x+1$ 除 x，就不能把商直接写成 $1/2$。但先把被除式乘以 2，便有 $2x=(2x+1)-1$。

一般地，若除式首项为 ax^n，当前余式首项为 bx^d，不能计算 b/a 时，可改做 $a\cdot$余式 $-bx^{d-n}g$。最高项仍会消掉，代价只是多乘一次 a。反复进行，就得到下面的带余除法。

定理 2.9.3 (整环上的带余除法)**.** 设 $f,g\neq 0$，$\deg f=m$、$\deg g=n$，a 为 g 的首项系数，$k=\max(m-n+1,0)$。存在唯一 $q,r\in R[x]$ 使

$$a^k f=qg+r,\qquad \deg r<n.$$

若 a 是单位，则普通带余除法成立。特别地，域上 $F[x]$ 是欧几里得环。

证明. 当 $m<n$ 时，$k=0$，直接取 $q=0,r=f$。设 $m\geq n$，从 $f=0\cdot g+f$ 开始，在第 j 步保持

$$a^j f=q_j g+r_j.$$

若 $r_j=0$ 或 $\deg r_j<n$，便停止。否则令 r_j 的首项为 bx^d，取

$$q_{j+1}=aq_j+bx^{d-n},\qquad r_{j+1}=ar_j-bx^{d-n}g.$$

两式仍满足 $a^{j+1}f=q_{j+1}g+r_{j+1}$，而余式的最高项已经抵消，次数至少下降一。因此至多 $m-n+1=k$ 步就得到所需低次余式。若实际只用了 $t<k$ 步，把等式整体再乘 a^{k-t}，便得到指定幂次 a^k 的存在性。

若有两组商余式，则 $(q-q')g=r'-r$。当左边非零时，整环中的次数公式使它次数至少为 n，右边却小于 n，矛盾。因此 $q=q'$，进而 $r=r'$。若 a 为单位，再将等式除以 a^k，即可得到普通带余除法；域的非零首项系数总可逆，所以 $F[x]$ 以次数为欧几里得函数。 □

特别地，以首一的 $x-c$ 作除法，余式是常数；代入 c 后得到该常数为 $f(c)$，所以 $f=(x-c)q+f(c)$。因此 c 是根当且仅当 $x-c$ 整除 f。

若 $b\neq c$ 是另一个根，从 $f=(x-c)q$ 得 $0=(b-c)q(b)$；整环性保证 $b-c$ 可消去，所以 $q(b)=0$。这样每除掉一个不同的根，次数下降一，其余根仍是商的根。归纳可知非零 n 次多项式至多有 n 个根。这里消去 $b-c$ 的一步说明了整环假设的用途。

因式分解时，常数因子与非常数因子应分开。系数的最大公因子恰好记录常数部分。

定义 2.9.4 (容度与本原多项式)**.** 设 R 是 UFD。非零 $f \in R[x]$ 的系数的最大公因子称容度，记为 $c(f)$，按相伴意义取值。若 $c(f)$ 为单位，称 f 本原。总能写 $f = c(f)f_0$，其中 f_0 本原。

本原部分相乘是否仍然本原，决定了常数因子能否与非常数因子分开处理。

引理 2.9.5 (Gauss 引理)**.** 在相伴意义下 $c(fg) \sim c(f)c(g)$；特别地，本原多项式的乘积本原。

证明. 先把 f, g 分别写成容度乘本原部分。只要证明两个本原多项式的乘积仍本原，再提出 $c(f)c(g)$，就得到一般公式。

设 $f = \sum a_i x^i$、$g = \sum b_j x^j$ 本原。若乘积的全部系数有非单位公因子，在 UFD 中就能取这个公因子的一个素因子 p。由于 f, g 本原，分别存在不被 p 整除的系数；取其中下标最小的 a_i, b_j。

看乘积中 x^{i+j} 的系数 $\sum_{u+v=i+j} a_u b_v$。除 $a_i b_j$ 外，每项要么 $u < i$，要么 $v < j$，因此都被 p 整除。整个系数也被 p 整除，就会推出 $p \mid a_i b_j$。但 p 为素元，而 a_i, b_j 都不被它整除，矛盾。故乘积本原。 □

若除式没有公共的常数因子，那么在被除式前补乘常数，并不能创造新的整除关系。

引理 2.9.6 (消去常数因子)**.** 若 g 本原、$0 \neq b \in R$，且 $g \mid bf$，则 $g \mid f$。

证明. 写 $bf = gh$。Gauss 引理给出 $c(h) \sim bc(f)$，故 b 整除 h 的所有系数。写 $h = bh_1$ 并消去 b，得 $f = gh_1$。 □

这些工具足以把 R 的唯一分解性质传到多项式环。

定理 2.9.7 (多项式环中的唯一分解)**.** 若 R 为 UFD，则 $R[x]$ 也为 UFD，因而 $R[x_1, \ldots, x_n]$ 也为 UFD。

证明. 仍按定理 2.5.8 分别证明终止性与素条件。先令 $\ell_R(c)$ 为非零 $c \in R$ 的不可约因子个数，并设

$$L(f) = \deg f + \ell_R(c(f)) \qquad (f \neq 0).$$

次数公式与 Gauss 引理使 $L(fg) = L(f) + L(g)$，而 $L(f) = 0$ 恰好表示 f 是常数单位。因此真因子链中 L 严格下降，分解必终止。只用次数不够，因为还可能继续分解常数；加上容度的因子个数正好补上这一点。

再取 $R[x]$ 的不可约元素。若它是常数 p，则 p 在 R 中不可约，因而是素元。若 $p \mid fg$，则 $p \mid c(fg) \sim c(f)c(g)$，故 $p \mid c(f)$ 或 $p \mid c(g)$，也就是 $p \mid f$ 或 $p \mid g$。

设不可约 $p(x)$ 次数大于零。它必须本原，否则 $p = c(p)p_0$ 会给出两个非单位因子。我们要证明 $p \mid fg$ 且 $p \nmid f$ 时必有 $p \mid g$。在域上通常会寻找 $up + vf = 1$；这里系数环未必为域，不一定能得到 1，但只需得到某个非零常数 b，就可以用引理 2.9.6 消去它。

为此，在理想 (p, f) 中选次数最小的非零 h，将 p, f 分别用 h 作带余除法。两次余式都仍在 (p, f) 中，若非零就比 h 次数低，因此只能为零。设 a 为 h 的首项系数，于

是对适当的非负整数 k, l 有

$$h \mid a^k p, \qquad h \mid a^l f.$$

写 $h = c(h)h_0$，其中 h_0 本原。用引理 2.9.6 分别消去非零常数 a^k, a^l，得到 $h_0 \mid p, f$。由 p 不可约，h_0 或为单位，或与 p 相伴；后一情形会推出 $p \mid f$，不合假设。因此 h_0 为单位，h 本身就是非零常数 b。

因为 $b \in (p, f)$，可写 $b = up + vf$。若 $p \mid fg$，则由 $bg = upg + vfg$ 得 $p \mid bg$；p 本原，再消去常数 b，得到 $p \mid g$。于是所有不可约元素都为素元素，$R[x]$ 为 UFD。最后按变量逐个添加，利用 $R[x_1, \dots, x_n] = (R[x_1, \dots, x_{n-1}])[x_n]$ 归纳，得到多元结论。 □

2.10 对称多项式

前面可以任意置换多项式的变量，得到环的自同构。现在反过来问：哪些多项式在所有这种置换下都不改变？例如 $x_1 + x_2 + x_3$、$x_1x_2 + x_1x_3 + x_2x_3$ 和 $x_1x_2x_3$ 都不依赖三个变量的次序。

这个问题与根和系数的关系直接相连。展开

$$(t - x_1) \cdots (t - x_n) = t^n - p_1 t^{n-1} + p_2 t^{n-2} - \cdots + (-1)^n p_n,$$

其中 p_k 是所有不同的 k 个变量相乘再相加。因此不必给根排序，也能从系数知道这些对称式。我们接下来要证明，任意对称多项式都能用这些 p_k 表示，而且表示唯一。

定义 2.10.1 (对称多项式). 设 R 为交换幺环。若 $f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = f(x_1, \dots, x_n)$ 对所有 $\sigma \in S_n$ 成立，称 f 对称。令

$$p_k = \sum_{1 \le i_1 < \cdots < i_k \le n} x_{i_1} \cdots x_{i_k} \quad (1 \le k \le n),$$

称为初等对称多项式；对称多项式全体记为 $S[x_1, \dots, x_n]$。

对称多项式对加、减、乘都封闭，故构成子环，而每个 p_k 都在其中。问题是怎样从一个给定的对称式找出它关于 $p_1, \dots, p_n$ 的表达式。

我们仍采用前一节反复消去最高项的想法，不过多元多项式先需要约定“最高”的意思。按指数向量的字典序比较：从左到右找第一个不同的指数，该指数大的单项式在前。于是 p_k 的最高项是 $x_1 \cdots x_k$，系数为 1。几个这样的最高项相乘，可以精确配出任何指数递降的最高项。

最高项的指数决定了应该减去怎样的 p_i 的乘积，这既给出存在证明，也给出计算算法。

定理 2.10.2 (对称多项式基本定理). $p_1, \dots, p_n$ 在 R 上代数无关，且

$$S[x_1, \dots, x_n] = R[p_1, \dots, p_n].$$

因此每个对称多项式都唯一表示为初等对称多项式的多项式。

证明. 先证存在性。置换变量不改变总次数，所以对称多项式的各个齐次部分仍对称，可以分别处理。设某一非零齐次部分的最高项为 $a x_1^{k_1} \cdots x_n^{k_n}$。必有 $k_1 \ge \cdots \ge k_n$：若前

面的某个指数较小，交换这两个变量，由对称性会出现系数仍为 $a \neq 0$ 的更高项，与最高性矛盾。

由于 p_j 的最高项为 $x_1 \cdots x_j$，要配出这个指数向量，最后一个变量需要 k_n 次 p_n，倒数第二个还需要 $k_{n-1} - k_n$ 次 p_{n-1}，依此向前。于是

$$a p_1^{k_1-k_2} p_2^{k_2-k_3} \cdots p_{n-1}^{k_{n-1}-k_n} p_n^{k_n}$$

具有完全相同的最高项。减去它后，仍是对称的同次多项式，而最高项严格降低。固定总次数的单项式只有有限个，所以重复此操作必终止，得到所求表示。这里没有除以任何系数，因此不要求 R 为域或整环。

再证唯一性，也就是 $p_1, \ldots, p_n$ 代数无关。单项式 $p_1^{d_1} \cdots p_n^{d_n}$ 的最高项系数为 1，指数向量为

$$(d_1 + \cdots + d_n,\ d_2 + \cdots + d_n,\ \ldots,\ d_n).$$

相邻坐标作差就能找回 $d_1, \ldots, d_n$，所以不同的 d 产生不同最高项。若有关于 p_i 的非零多项式关系，在其有限个非零项中选择代入后最高项最大的一个。其他项的所有单项式都比它小，不能抵消它的非零系数，矛盾。因此没有非零关系，表示唯一。 □

例 2.10.3 (三次幂和)**.** 对三个不定元，设 $f = x_1^3 + x_2^3 + x_3^3$。最高项为 x_1^3，先减 p_1^3。展开得

$$p_1^3 = f + 3\sum_{i \neq j} x_i^2 x_j + 6p_3, \qquad p_1 p_2 = \sum_{i \neq j} x_i^2 x_j + 3p_3.$$

所以再加 $3p_1p_2$，就消去混合项，留下 $3p_3$。最终

$$f = p_1^3 - 3p_1p_2 + 3p_3.$$

这展示了逐项消去的算法；也可先利用总次数为 3，写成 $Ap_1^3 + Bp_1p_2 + Cp_3$，再比较 $x_1^3, x_1^2x_2, x_1x_2x_3$ 的系数，依次得 $A = 1, B = -3, C = 3$。
这里按原变量次数计算，p_k 的权为 k，所以 p_1^3, p_1p_2, p_3 都有权 3。若把每个 p_k 都当作权为 1 的新变量，就会漏掉正确候选项。等式的整数系数在任意交换幺环中解释，特征为 3 时相应系数自动成为零。

2.11 本章小结

从群到环，多出的一种乘法改变了取商的条件。加法陪集已经存在，代表元改变时还要求乘积陪集不变；展开差 $ab - a'b'$ 便引出理想的左右吸收性。随后，$f(a) = f(b) \iff a - b \in \operatorname{Ker} f$ 又给出环的同态基本定理。素理想与极大理想分别把商中“没有零因子”与“非零元都有逆”译回原环的条件。

研究分解时，不能把整数中的全部直觉一次带入一般整环。$\mathbb{Z}[\sqrt{5}]$ 中的 2 不可约却不素；这说明不能再分与整除乘积的规则是两件事。要得到 UFD，我们分别控制分解的终止和唯一性。主理想条件使理想升链停住，又使不可约元素生成极大理想；欧几里得除法则通过最小余数证明理想为主理想。因此得到

$$\text{欧几里得环} \implies \text{PID} \implies \text{UFD} \implies \text{整环}.$$

$\mathbb{Z}[x]$ 是 UFD，却不是 PID。特别地，存在最大公因子并不保证它能写成原元素的线性组合；$\gcd(3, x) = 1$ 与 $1 \notin (3, x)$ 可以同时成立。

多项式先按系数构造，再讨论取值，才不会把形式多项式与多项式函数混淆。泛性质将构造同态化为指定系数和变量的像；若添加的是代数元，则已有的多项式关系会限制这种指定。整环中，次数确保最高项不消失；UFD 中，容度与 Gauss 引理又把常数因子从非常数因子中分开，使唯一分解能逐次传到多元多项式环。

最后，对称多项式的证明再次使用最高项消去，但这次减去的是初等对称多项式的乘积。存在性来自可执行且会终止的消去过程，唯一性来自不同乘积具有不同最高项。读这些构造时，可以始终分别检查：要消去哪一项，选择的对象为什么恰好消掉它，以及这一步反复进行后为什么能停下来。

常用条件与结论速查

群：子群、同态与作用

目标	条件与结论	正文
判定群	半群中存在左幺元，且每个元素均有相对于它的左逆元，则为群。左右条件不可随意混搭。	1.1.7
判定子群	非空 $H \subseteq G$：$H < G \iff ab^{-1} \in H$ 对一切 $a, b \in H$ 成立。	1.2.2
比较陪集	$aH = bH \iff a^{-1}b \in H$；两个左陪集相等或不交。	1.2.6
计算指数	G 有限时，$\lvert G\rvert = [G : H]\lvert H\rvert$。若 $K < H < G$，则 $[G : K] = [G : H][H : K]$。	1.2.10、1.2.11
判定正规	$N \trianglelefteq G \iff gNg^{-1} = N$ 对所有 $g \in G$ 成立；亦等价于所有 $gN = Ng$。	1.3.3
由同态求商	$f : G \to G'$ 为同态，则 $G/\operatorname{Ker} f \cong \operatorname{Im} f$。单射等价于核平凡。	1.4.11
商中找子群	对 $N \trianglelefteq G$，G/N 的子群对应于 G 中含 N 的子群，且保持正规性。若 $N \subseteq H \trianglelefteq G$，则 $(G/N)/(H/N) \cong G/H$。	1.4.12
限制自然同态	$H < G$、$N \trianglelefteq G$ 时，$HN < G$，且 $H/(H \cap N) \cong HN/N$。	1.4.13
计算轨道	$\lvert O_x\rvert = [G : F_x]$。有限群中 $\lvert G\rvert = \lvert O_x\rvert\lvert F_x\rvert$；共轭类大小为 $[G : C_G(a)]$。	1.9.8
寻找作用核	群作用等价于同态 $G \to S_X$；固定全部点的元素组成核，作用有效当且仅当该核平凡。	1.9.2、1.9.4

计算商群前先检查正规性；利用作用时先明确集合 X 与作用公式，再分别计算迷向子群和作用核。前者控制一条轨道，后者控制整个作用。

群：结构与素数幂

目标	条件与结论	正文
循环群的子群	$G=\langle a\rangle$、$\lvert G\rvert=n$：每个 $d\mid n$ 有唯一的 d 阶子群 $\langle a^{n/d}\rangle$，且 $\lvert a^k\rvert=n/\gcd(n,k)$。	1.5.5
置换的阶与符号	不相交轮换分解唯一；阶为轮换长度的最小公倍数。r-轮换的符号为 $(-1)^{r-1}$。	1.6.4、1.6.7
判断单性	Abel 单群恰为素数阶循环群；$n\geq 5$ 时 A_n 是非 Abel 单群。	1.5.6、1.6.9
判断扩张分裂	$1\to A\to G\xrightarrow{\mu} B\to 1$ 正合：存在 $\iota: B\to G$ 使 $\mu\iota=\mathrm{id}_B$，等价于扩张核有补子群。	1.7.4
比较合成因子	群有合成序列时，各合成序列的长度相同，因子在重排与同构意义下相同；因子不决定扩张方式。	1.7.10
判断可解	有限群可解，当且仅当合成因子均为素数阶循环群。一般地，$N\trianglelefteq G$ 时，G 可解当且仅当 $N, G/N$ 都可解。	1.8.6、1.8.5
判断幂零	降中心列到达 1，等价于升中心列到达 G。若 $N\subseteq C(G)$ 且 G/N 幂零，则 G 幂零。	1.8.10、1.8.8
利用 p-群	p-群作用于有限集时，$\lvert X\rvert\equiv\lvert X_0\rvert \pmod p$。非平凡有限 p-群中心非平凡，且所有有限 p-群都幂零。	1.10.3、1.10.4
Sylow 三定理	写 $\lvert G\rvert=p^r m$、$p\nmid m$：有 p^r 阶子群；每个 p-子群包含于其某个共轭；$n_p\mid m$ 且 $n_p\equiv 1 \pmod p$。正规等价于 $n_p=1$。	1.10.5、1.10.7、1.10.9

从群阶出发时，先列出 n_p 的整除与同余限制；若未能得到唯一性，再考虑元素计数或对 Sylow 子群集合的共轭作用。可解与幂零不可混用：S_3 可解而不幂零。

环：商结构与因子分解

目标	条件与结论	正文
判定子环	非空 $S \subseteq R$：对任意 $a, b \in S$ 有 $a - b, ab \in S$。不默认含原环的幺元。	2.2.2
判定理想	非空 $I \subseteq R$：对差封闭，并对左右乘任意 R 中元素封闭。理想保证商乘法良定义。	2.2.4、2.2.7
由同态求商	环同态 $f : R \to S$ 满足 $R/\operatorname{Ker} f \cong f(R)$；满同态下含核理想与陪域理想一一对应。	2.4.3
交换商与限制	理想 $I \subseteq J$ 时，$(R/I)/(J/I) \cong R/J$。任意两个理想满足 $(I + J)/I \cong J/(I \cap J)$。	2.4.4
判定素理想	R 为交换幺环、I 为真理想：I 素 $\iff$ R/I 为整环 $\iff$ $ab \in I$ 蕴含 $a \in I$ 或 $b \in I$。	2.6.2
判定极大理想	R 为交换幺环：M 极大 $\iff$ R/M 为域。极大理想必素，反向一般不成立。	2.6.6
区分素与不可约	在整环中，素元素必不可约；UFD 中二者等价。$\mathbb{Z}[\sqrt{5}]$ 的 2 不可约却不素。	2.5.3、2.5.4
判断 UFD	整环为 UFD，等价于因子链条件与素条件同时成立，也等价于因子链条件与公因子条件同时成立。	2.5.8
使用 Bézout 式	在 PID 中，若 $d = \gcd(a, b)$，则 $d = ua + vb$，且理想 $(a, b) = (d)$。一般 UFD 不保证这种线性表示。	2.7.4
比较三类整环	欧几里得环 $\Rightarrow$ PID $\Rightarrow$ UFD。$\mathbb{Z}[x]$ 是 UFD，却不是 PID。	2.7.6、2.7.3

素理想控制商环的零因子，极大理想控制商环的可逆性；“不可约元素”是分解条件，不能在任意整环中直接替换成“素元素”。

多项式：构造、次数与分解

目标	条件与结论	正文
使用次数公式	R 为整环、$f,g\neq 0$：$\deg(fg)=\deg f+\deg g$，且 $U(R[x])=U(R)$。有零因子时次数可能下降。	2.8.2
识别多项式环	$a_1,\dots,a_n$ 在 R 上代数无关，等价于取值映射 $R[x_1,\dots,x_n]\to R[a_1,\dots,a_n]$ 为同构。	2.8.7
扩充系数同态	R,S 为交换幺环，$\sigma:R\to S$ 保持幺元。任给 $b_i\in S$，有唯一扩充同态把 x_i 送到 b_i，公式为逐项取系数像并代入。	2.8.8
更换一元生成元	整环 R 上，$R[x]$ 的多项式生成元恰为 $ux+v$，其中 $u\in U(R),v\in R$；它们恰给出所有 R-自同构。	2.9.1、2.9.2
作带余除法	R 为整环，$f,g\neq 0$，次数为 m,n，g 首项系数为 a。令 $k=\max(m-n+1,0)$，则唯一地有 $a^kf=qg+r$，$\deg r<n$。	2.9.3
分离常数因子	R 为 UFD：$c(fg)\sim c(f)c(g)$，本原多项式的乘积本原。若 g 本原、$0\neq b\in R$，则 $g\mid bf\Rightarrow g\mid f$。	2.9.5、2.9.6
逐次添加变量	R 为 UFD，则任意有限个不定元的 $R[x_1,\dots,x_n]$ 都为 UFD。PID 性质没有同样的保持结论。	2.9.7
化简对称式	R 为交换幺环：每个对称多项式唯一写成初等对称多项式 $p_1,\dots,p_n$ 的多项式；处理齐次式时给 p_k 赋权 k。	2.10.2

整环上的普通带余除法需要除式首项系数为单位；否则先补乘首项系数的幂。多项式和多项式函数也要区分：在有限域上，非零多项式可以处处取零值。